Editor’s Note

Innovation Driving Digital Transformation and Preparing for GDPR

Baker McKenzie is pleased to provide you with complimentary access to the 2018 edition of our Global Privacy and Information Management Handbook, which covers over 50 jurisdictions and is currently available online at tmt.bakermckenzie.com and in hardcopy for our clients (app format coming soon).

Three intricately linked themes dominated the news this past year:

• the profound transformation of business and organizational activities, processes, competencies and models to fully leverage the changes and opportunities of a mix of digital technologies (including artificial intelligence and machine learning) and their accelerating impact across society (e.g., internet of things and autonomous cars);

• the increasingly weighty challenge of managing and protecting the growing amounts and richness of data (e.g., big data) being collected, used and processed in connection with the pursuit of digital transformation; and

• the heightened global compliance obligations that are emerging to protect the rights of individuals impacted by the digital transformation underway, as most clearly represented by the implementation of the General Data Protection Regulation (GDPR).

If 2017 was largely about coming to terms with the impact of a world undergoing a digital transformation, for all businesses and organizations, the focus in 2018 will be around preparedness, action and managing risk.

Some of the most notable privacy trends and developments across the globe, include:

• **A more active role and enforcement by regulators due to an increase in cyber attacks and data breaches.** In Denmark, the Danish regulator has placed heavy focus on pursuing data breaches. In Australia, mandatory data breach notification is now law. In Hong Kong, the Securities and Futures Commission (SFC) issued new sector-based proposals in May 2017 to reduce and mitigate hacking risks associated with Internet trading.

• **Employee monitoring.** In Norway, the regulator released a guide for businesses implementing surveillance measures at the workplace. In Germany, the Federal Labour Court held that the use of key logger
software to secretly monitor employees violates employee privacy. In Hungary, the regulator issued guidance on data processing in the employment context.

- **Digital economy.** In Hungary, the DPA has issued guidance on website and online shop operations explaining the basic requirements around the use of cookies and applicable notice and user consent requirements. In Italy, the regulator has been fairly active in issuing orders and guidelines on the digital economy discussing a range of issues around the use of mobile applications, cyberbullying, privacy issues in school, risks of phishing attacks, data processing for credit claim purposes, and the use of smartphones and social media platforms.

- **GDPR.** In the EU, all eyes are on the GDPR, which will start to apply from 25 May 2018. National legislators have been busy consulting and drafting national legislation that will supplement the GDPR. Regulators are issuing guidance on key topics while still coming to terms with their redefined roles. Businesses are seeking to understand the numerous stringent obligations that GDPR will impose on them.

- **Sector-specific cybersecurity requirements.** In China, the China Food and Drug Administration (CFDA) issued guidelines implementing China’s Cybersecurity Law in the administration of medical devices with medical device companies required to register their networked medical devices with the CFDA. Hong Kong’s SFC issued a consultation paper on Proposals to Reduce and Mitigate Hacking Risks associated with Internet trading, which includes new baseline security requirements for Internet traders.

For more in-depth coverage of these trends and developments, we invite you to check out and subscribe to our expanding series of related digital resources:

- **Global TMT Hub** (at tmt.bakermckenzie.com), our online portal of publications and resources that help you stay on top of developments in the TMT space, where you find among others:
  - 2018 GDPR National Legislation Survey
  - EU GDPR Game Changers
  - Global Data Breach Notification Guide
  - Global Data Protection Enforcement Report
  - 2017 Global Surveillance Law Comparison Guide
  - 2018 Global Outsourcing Employment Handbook
• **bINFORM** ([www.bakerinform.com](http://www.bakerinform.com)), our online magazine that focuses on legal insights relating to data and technology trends

If you are interested in exploring ways in which technology can be leveraged to address data privacy compliance, contact your local BM partner and ask about our various award winning information governance solutions.

We also invite you to explore **Whitespace Legal Collab**, the first global legal innovation hub devoted to multidisciplinary collaboration and winner of the **Financial Times North America Innovative Lawyers 2017 Award** for “Innovation in the Business of Law: Strategy and Changing Behaviors”. The Collab draws on strategic relationships with tech firms, universities, not-for-profits and others to help solve tough client problems at the intersection of business, law, technology and other disciplines. Many collaborations center on innovations related to data privacy, smart cities, and other challenges related to data governance, compliance, and monetization. In addition, the Collab is striving to find optimal uses for AI, machine learning, data analytics in the context of legal services delivery and business model development.


**Theo Ling**  
Chair, Baker McKenzie Global Privacy & Information Management Working Group
Baker McKenzie’s Global Privacy Leadership Team

Theo Ling  
Lead Partner, Toronto  
Tel: +(416) 865-6954  
theodore.ling@bakermckenzie.com

Anne-Marie Allgrove  
Partner, Sydney  
Tel: +61 2 8922 5274  
anne-marie.allgrove@bakermckenzie.com

Ken Chia  
Partner, Singapore  
Tel: +65 6434 2558  
ken.chia@bakermckenzie.com

Lothar Determann  
Partner, Palo Alto  
Tel: +1 (650) 856-5533  
lothar.determann@bakermckenzie.com

Brian Hengesbaugh  
Partner, Chicago  
Tel: +1 312 861 3077  
brian.hengesbaugh@bakermckenzie.com

Francesca Gaudino  
Partner, Milan  
Tel: +39 02 76231-452  
francesca.gaudino@bakermckenzie.com
Contributing Lawyers

**Argentina**

Guillermo Cervio  
Buenos Aires  
Tel: +54 11 4310 2223  
guillermo.cervio@bakermckenzie.com

Roberto Grané  
Buenos Aires  
Tel: +54 11 4310 2214  
roberto.grane@bakermckenzie.com

**Australia**

Anne-Marie Allgrove  
Sydney  
Tel: +61 2 8922 5274  
ann-marie.allgrove@bakermckenzie.com

Patrick Fair  
Sydney  
Tel: +61 2 8922 5534  
patrick.fair@bakermckenzie.com

Adrian Lawrence  
Sydney  
Tel: +61 2 8922 5204  
adrian.lawrence@bakermckenzie.com

Toby Patten  
Melbourne  
Tel: +61 3 9617 4456  
toby.patten@bakermckenzie.com

**Austria**

Dr. Lukas Feiler, SSCP, CIPP/E  
Vienna  
Tel: +43 1 2 4250 450  
lukas.feiler@bakermckenzie.com

Marisa Elisa Schlacher  
Vienna  
Tel: +43 1 2 4250 278  
marisa.schlacher@bakermckenzie.com

**Azerbaijan**

Jamil Alizada  
Baku  
Tel: +994 12 4971 801  
jamil.alizada@bakermckenzie.com

Gunduz Karimov  
Baku  
Tel: +994 12 4971 801  
gunduz.karimov@bakermckenzie.com

**Belgium**

Elisabeth Dehareng  
Brussels  
Tel: +32 2 639 36 11  
elisabeth.dehareng@bakermckenzie.com

Daniel Fesler  
Brussels  
Tel: +32 2 639 36 11  
daniel.fesler@bakermckenzie.com

**Brazil**

Flavia Rebello  
Sao Paulo  
Tel: +55 11 3048 6851  
flavia.rebello@trenchrossi.com

Gabriela Paiva Morette  
Sao Paulo  
Tel: +55 11 3048 6785  
gabriela.paiva-morette@trenchrossi.com

**Canada**

Theodore Ling  
Toronto  
Tel: +416 865 6954  
theodore.ling@bakermckenzie.com

Arlan Gates  
Toronto  
Tel: +416 865 6978  
arlan.gates@bakermckenzie.com
Indonesia

Mark Innis
Jakarta
Tel: +62 21 2960 8618
mark.innis@bakernet.com

Adhika P.S. Wiyoso
Jakarta
Tel: +62 21 2960 8507
adhika.wiyoso@bakernet.com

Denny Ngadimin
Jakarta
Tel: +62 21 2960 8641
denny.ngadimin@bakernet.com

Ireland

John Cahir
Dublin
Tel: +353 1 649 2000
jcahir@algoodbody.com

Alison Quinn
Dublin
Tel: +353 1 649 2461
alquinn@algoodbody.com

Israel

Nurit Dagan
Tel Aviv
Tel: +972 3 692 7424
dagan@hfn.co.il

Ohad Elkeslassy
Tel Aviv
Tel: +972 3 692 7424
elkeslassyo@hfn.co.il

Italy

Francesca Gaudino
Milan
Tel: +39 02 76231 452
francesca.gaudino@bakermckenzie.com

Japan

Daisuke Tatsuno
Tokyo
Tel: +813 6271 9479
daisuke.tatsuno@bakermckenzie.com

Kensaku Takase
Tokyo
Tel: +813 6271 9752
kensaku.takase@bakermckenzie.com

Luxembourg

Sybille Briand
Luxembourg
Tel: +352 26 18 44 261
sybille.briand@bakermckenzie.com

Malaysia

Brian Chia
Kuala Lumpur
Tel: +603 2298 7999
brian.chia@wongpartners.com

Shameen Mohd. Haaziq Pillay
Kuala Lumpur
Tel: +603 2298 7943
shameen.mohd.haaziqpillay
@wongpartners.com

Mexico

Sergio Legorreta-Gonzalez
Mexico City
Tel: +52 55 5279 2954
sergio.legorreta-gonzalez
@bakermckenzie.com

Carlos Vela-Treviño
Mexico City
Tel: +52 55 5279 2911
carlos.vela-trevino@bakermckenzie.com
Netherlands

Remke Scheepstra
Amsterdam
Tel: +31 20 5517 831
remke.scheepstra@bakermckenzie.com

Wouter Seinen
Amsterdam
Tel: +31 20 5517 161
wouter.seinen@bakermckenzie.com

Nathalja Doing
Amsterdam
Tel: +31 20 5517 128
nathalja.doing@bakermckenzie.com

Andre Walter
Amsterdam
Tel: +31 20 5517 941
andre.walter@bakermckenzie.com

Norway

Espen Sandvik
Oslo
Tel: +47 98 29 45 41
esa@adeb.no

Emilie Veggeland Knudsen
Oslo
Tel: +47 99 15 47 74
evk@adeb.no

Paraguay

Nestor Loizaga
Asuncion
Tel: +595 21 318 3000 Ext. 2533
nloizaga@ferrere.com

Peru

Javier Tovar
Lima
Tel: +51 1 618 8500 Ext. 8550
javier.tovar@bakermckenzie.com

Teresa Tovar
Lima
Tel: +51 1 618 8500 Ext. 8552
teresa.tovar@bakermckenzie.com

Viviana Chavez
Lima
Tel: +51 1 618 8500 Ext. 8535
viviana.chavez@bakermckenzie.com

Eileen Infantas
Lima
Tel: +51 1 618 8500 Ext. 8536
eileen.infantas@bakermckenzie.com

Philippines

Bienvenido Marquez
Manila
Tel: +63 2 819 4936
bienvenido.marquez@quisumbingtorres.com

Divina Ilas-Panganiban
Manila
Tel: +63 2 819 4961
divina.ilaspanganiban@quisumbingtorres.com

Neonette Pascual
Manila
Tel: +63 2 819 4908
neonette.pascual@quisumbingtorres.com

Poland

Magdalena Kogut-Czarkowska
Warsaw
Tel: +48 22 445 3452
magdalena.kogut-czarkowska@bakermckenzie.com

Radoslaw Nozykowski
Warsaw
Tel: +48 22 445 3210
radoslaw.nozykowski@bakermckenzie.com

Jakub Falkowski
Warsaw
Tel: +48 22 445 3294
jakub.falkowski@bakermckenzie.com
Spain

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com

Patricia Pérez
Madrid
Tel: +34 91 436 6627
patricia.perez@bakermckenzie.com

Candelaria Canaro
Barcelona
Tel: +34 93 206 0820
cande.canaro@bakermckenzie.com

Sweden

Sten Bauer
Stockholm
Tel: +46 8 566 177 16
sten.bauer@bakermckenzie.com

Peder Oxhammar
Stockholm
Tel: +46 8 566 177 25
peder.oxhammar@bakermckenzie.com

Switzerland

Alessandro Celli
Zurich
Tel: +41 44 384 13 66
alessandro.celli@bakermckenzie.com

Muriel Binder
Zurich
Tel: +41 44 384 14 27
muriel.binder@bakermckenzie.com

Markus Winkler
Zurich
Tel: +41 44 384 13 01
markus.winkler@bakermckenzie.com

Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang@bakermckenzie.com

Chris Tsai
Taipei
Tel: +886 2 2715 7310
chris.tsai@bakermckenzie.com

Louis Hsieh
Taipei
Tel: +886 2 2715 7308
louis.hsieh@bakermckenzie.com

Thailand

Dhiraphol Suwanprateep
Bangkok
Tel: +66 02 636 2000 Ext. 4950
dhiraphol.suwanprateep
@bakermckenzie.com

Pattaraphan Paiboon
Bangkok
Tel: +66 02 636 2000 Ext. 4568
pattaraphan.paiboon
@bakermckenzie.com

Kritiyanee Buranatrevedhya
Bangkok
Tel: +66 02 636 2000 Ext. 4592
kritiyanee.buranatrevedhya
@bakermckenzie.com

Turkey

Can Sozer
Istanbul
Tel: +90 212 376 64 43
can.sozer@esin.av.tr

Hilal Temel
Istanbul
Tel: +90 212 376 64 17
hilal.temel@bakermckenzie.com
Ukraine

Oleksiy Stolyarenko
Kyiv
Tel: +380 44 590 0101
oleksiy.stolyarenko@bakermckenzie.com

United Kingdom

Robbie Downing
London
Tel: +44 20 7919 1161
robbie.downing@bakermckenzie.com

Harry Small
London
Tel: +44 (0)20 7919 1914
harry.small@bakermckenzie.com

Ian Walden
London
Tel: +44 20 7919 1247
ian.walden@bakermckenzie.com

Benjamin Slinn
London
Tel: +44 20 7919 1783
benjamin.slinn@bakermckenzie.com

Brian Hengesbaugh
Chicago
Tel: +1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

United States

Amy de La Lama
Chicago
Tel: +1 312 861 2923
amy.delalama@bakermckenzie.com

Lothar Determann
Palo Alto
Tel: +1 650 856 5533
lothar.determann@bakermckenzie.com

Michael Egan
Washington, D.C.
Tel: +1 202 452 7022
michael.egan@bakermckenzie.com

Martin Pesce
Montevideo
Tel: +598 2900 1000 ext. 1431
mpesce@ferrere.com

Stephania Bresque
Montevideo
Tel: +598 2900 1000 ext. 1450
sbresque@ferrere.com

Venezuela

Maria Eugenia Salazar
Caracas
Tel: +58 212 276 5161
mariaeugenia.salazar@bakermckenzie.com

Hector Martinez
Caracas
Tel: +58 212 276 5056
hector.martinez@bakermckenzie.com

Heather Mantegna Fitzwater
Chicago
Tel: +1 312 861 8808
heather.mantegna@bakermckenzie.com

Lindsay Martin
Chicago
Tel: +1 312 861 2949
lindsay.martin@bakermckenzie.com

Brandon Moseberry
Chicago
Tel: +1 312 861 8265
brandon.moseberry@bakermckenzie.com

Michael Stoker
Chicago
Tel: +1 312 861 2870
michael.stoker@bakermckenzie.com

Harry Valetk
New York
Tel: +1 212 626 4285
harry.valetk@bakermckenzie.com

Heather Mantegna Fitzwater
Chicago
Tel: +1 312 861 8808
heather.mantegna@bakermckenzie.com
Vietnam

Manh Hung Tran
Hanoi
Tel: +84 24 3936 9398
tmh@bmvn.com.vn

Thanh Son Dang
Hanoi
Tel: +84 24 3936 9607
thanhson.dang@bakermckenzie.com

Yee Chung Seck
Ho Chi Minh City
Tel: +84 28 3520 2633
yeechung.seck@bakermckenzie.com

Mai Phuong Nguyen
Ho Chi Minh City
Tel: +84 28 3520 2630
maiphuong.nguyen@bakermckenzie.com

*This list includes just some of our global Privacy practitioners. To find a Baker McKenzie lawyer or other professional, please visit www.bakermckenzie.com.
# Table of Contents

Editor’s Note ........................................................................................................................................ i
Baker McKenzie’s Global Privacy Leadership Team ............................................................................. v
Contributing Lawyers .............................................................................................................................. vii
The Game Changer in the Privacy World: the EU General Data Protection Regulation ............................ xxi
Argentina ................................................................................................................................................ 1
Australia ................................................................................................................................................. 17
Austria .................................................................................................................................................. 31
Azerbaijan ............................................................................................................................................. 43
Belgium ................................................................................................................................................. 49
Brazil .................................................................................................................................................... 67
Canada .................................................................................................................................................. 79
Alberta, Canada ................................................................................................................................. 91
British Columbia, Canada ................................................................................................................... 102
Manitoba, Canada .............................................................................................................................. 111
Ontario, Canada ................................................................................................................................... 122
Quebec, Canada .................................................................................................................................. 131
Chile .................................................................................................................................................... 139
China .................................................................................................................................................... 145
Colombia ............................................................................................................................................. 159
Czech Republic ................................................................................................................................... 177
Denmark ............................................................................................................................................... 193
Finland .................................................................................................................................................. 213
France .................................................................................................................................................. 233
Germany .............................................................................................................................................. 257
Greece .................................................................................................................................................. 279
Hong Kong .......................................................................................................................................... 299
Hungary ................................................................................................................................................ 313
Iceland .................................................................................................................................................. 335
India .................................................................................................................................................... 353
Indonesia ............................................................................................................................................. 365
Ireland .................................................................................................................................................. 381
Israel .................................................................................................................................................... 401
Italy ...................................................................................................................................................... 425
Japan .................................................................................................................................................... 439
Luxembourg .......................................................................................................................................... 453
Malaysia ................................................................................................................................................ 465
Mexico .................................................................................................................................................. 477
Netherlands ......................................................................................................................................... 487
Norway ................................................................................................................................................ 501
Paraguay ............................................................................................................................................... 513
Peru ...................................................................................................................................................... 523
Philippines ........................................................................................................................................... 533
Poland .................................................................................................................................................. 549
Portugal ................................................................................................................................................ 565
Russia .................................................................................................................................................. 593
Saudi Arabia ........................................................................................................................................ 605
Singapore ............................................................................................................................................ 617
South Africa .......................................................................................................................................... 633
South Korea ......................................................................................................................................... 649
Spain ..................................................................................................................................................... 661
Sweden ................................................................................................................................................ 681
Switzerland .......................................................................................................................................... 695
Taiwan .................................................................................................................................................. 705
Thailand ............................................................................................................................................... 715
Turkey ................................................................................................................................................... 725
Ukraine ................................................................................................................................................. 739
United Kingdom ................................................................................................................................. 751
United States ............................................................... 771
United States California Privacy Laws ............................... 776
United States Children’s Online Privacy Protection Act (“COPPA”) .... 784
United States Gramm-Leach-Bliley Act and Fair Credit Reporting Act .... 791
United States Health Insurance Portability and Accountability Act .... 801
United States State Data Security Laws ................................ 815
United States State Security Breach Notification Laws .................. 821
EU-US Privacy Shield .......................................................... 827
Uruguay ............................................................................. 829
Venezuela ............................................................................ 845
Vietnam .............................................................................. 855
Baker McKenzie Offices Worldwide ........................................... 873
The Game Changer in the Privacy World: the EU General Data Protection Regulation

Francesca Gaudino
Milan
Tel: +39 (02) 76231-452
francesca.gaudino@bakermckenzie.com

Anna von Dietze
Dusseldorf
Tel: +49 211 3 11 16 300
anna.vondietze@bakermckenzie.com

The GDPR, which will start to apply on 25 May 2018 after a two-year transition period since its formal adoption in 2016, is clearly the big Game Changer in the privacy world this year (and decade). In the EU (and beyond) all eyes are on the GDPR. During the two-year transition period, regulators, legislators as well as private and public sector organizations have devoted significant time and resources in order to get GDPR-ready. Despite all these efforts, it appears that across the spectrum, the bulk of the work is yet to be done.

In this Chapter, we:

• provide an overview as to where countries stand in terms of national legislation supplementing GDPR;

• offer a brief opinion on what to expect from national privacy regulators in the year to come;

• highlight some of the major changes that the GDPR will bring about for businesses; and

• briefly divert to the ePrivacy Regulation – “the other” key European privacy legislation on the horizon.

1. National legislation supplementing GDPR

National legislators have been, and continue to be, busy consulting on, and drafting, national legislation that will supplement the GDPR. Even though the GDPR will be directly applicable in all EU Member States, due to its numerous opening clauses, there is ample room for Member States to enact local data protection legislation to fill the gaps deliberately left by the GDPR. From a
From a compliance perspective, this poses serious challenges: businesses will not only need to comply with the GDPR (which is complex in itself) but also with a myriad of varying local supplementing laws which will lay down the rules for important topics such as processing of employee data and the appointment of data protection officers.

So, where are national legislators at? With not much time to spare until the GDPR will start to apply, by now, one would expect most national laws supplementing GDPR to be in place. However, as our GDPR National Legislation Survey reveals, as of January 2018, only two EU Member States (Germany and Austria) have enacted such legislation, while 13 countries have proposed a Bill and the remainder are even further behind. This is an important space to watch over the next year.

Overview over the 27 countries in scope (Cyprus excluded):

- Two countries have passed Acts which will come into force from 25 May 2018: Austria and Germany.
- Thirteen countries have published a Bill, including a Bill that is sitting with Parliament: Czech Republic, Denmark, France, Hungary, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Slovakia, Slovenia, Spain and the United Kingdom.
- Seven countries are planning to draft a Bill which has not yet been made public: Belgium, Croatia, Estonia, Finland, Ireland, Italy and Sweden.
- Five countries have not published a Bill or have limited publicly available information on how they will implement the GDPR: Bulgaria, Greece, Malta, Portugal and Romania.
2. **Regulator Radar – What to expect from national regulators from May 2018 onwards?**

Many are wondering what to expect from local regulators once the GDPR starts to apply. Will they come knocking on our door? Will they make use of their powers to impose huge fines?

We do not expect a dramatic change in course from regulators as of 25 May 2018. Firstly, most regulators are still coming to terms with their redefined roles and responsibilities and are busy getting their own house in order. Secondly, many regulators see much of their role in helping businesses understand, and achieve compliance with, the GDPR rather than that of an aggressive enforcer. Thirdly, most regulators will not have significantly more resources available over night to step-up their enforcement activities, especially not while still devoting significant resources to producing guidance and compliance tools.

With this in mind and having observed different markets and regulators over the past months, we expect:

- privacy enforcement patterns and activities in the EU not to change noticeably in the next year;
- regulators, if current practice, to continue to issue warnings and give businesses time to remedy non-compliance before considering the imposition of fines;
- areas of focus to be around health data, extensive tracking of individuals and data security breaches; and
- regulators to pursue obvious breaches by well-known players rather than going after small businesses.

This does not mean that businesses should sit back and turn a blind eye to privacy compliance as regulators will not be inactive and enforcement patterns will likely change over the next few years. But there does not seem to be an imminent increased threat from regulators. That said, another space to watch are privacy class actions initiated by associations/Data Subjects as they may well become a real threat for businesses.

3. **Major Game Changers**

The GDPR is a call to action across the globe. It is triggering many organizations to review, or devise for the first time, comprehensive privacy compliance programs. Privacy compliance is increasingly receiving attention from the C-Suite and non-compliance is seen as a real business risk. A lot of this can be attributed to the draconian sanctions introduced by the GDPR but looming reputational losses and heightened consumer expectations do also
play a noteworthy role – so much that privacy compliance is increasingly perceived as a key competitive factor.

So, where do you start the process of achieving compliance with the GDPR? The GDPR is not exactly an easy, straightforward piece of legislation to comply with. With its numerous and complex obligations spread between 99 Articles and 173 Recitals, it is challenging to filter out the obligations at theoretical level. But the next step – to work out how to comply with those obligations in practice – is even more challenging and seems at times impossible.

Arguably, the most challenging aspect of the GDPR is that it requires a new approach, a new mindset in the way companies collect, use and store Personal Data. Companies are called to design and implement a new organizational model where privacy tasks are carefully identified and assigned to key stakeholders across the organization. GDPR demands structural and behavioral change. Change is considered for a human being as one of the most difficult situations to cope with. It is generally stated that first reaction is to refuse the change, then to understand it, take action, and lastly to act in order to address the change and avoid falling back into previous behaviors. Thus, it is a difficult task for companies to set up and roll out a new internal approach to manage data protection and security issues.

We, at Baker McKenzie, have identified 13 areas of priority to help companies become GDPR-compliant. These are explored in detail in our EU GDPR in 13 Game Changers publication. The following provides a snapshot of five key changes introduced by the GDPR that warrant attention and would make for a good starting point in practice.
(a) Data Protection Officer

One of the first steps for any organization would be to consider whether or not it must or should appoint a data protection officer (DPO) to oversee their data processing operations.

Under the GDPR virtually all public sector organizations will be required to do so. Private sector organisations will only be required to appoint a DPO if their core activities consist of:

- processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of Data Subjects on a large scale; or
- processing on a large scale of special categories of data or data relating to criminal convictions and offenses.

In addition, Member States are free to introduce broader national DPO requirements. So far, only Germany has passed a law which requires the appointment of a DPO in cases that go beyond GDPR. Germany essentially
retains its (broad) pre-GDPR DPO requirement. While it appears that most countries will not require the appointment of DPOs in circumstances beyond those prescribed by the GDPR, this is a space to watch.

The GDPR leaves substantial room for businesses to argue that a DPO is not legally required (although a careful assessment should be made in practice having regard to the Article 29 Working Party Guidance on point which provides helpful guidance, including that it interprets the legal concepts of “core activities”, “large scale” and “regular and systematic monitoring”). But as data increasingly underpins whole business models, moving forward more and more businesses will be legally required to appoint a DPO. And even if not required to designate a DPO, multinationals operating across the EU would be well advised to consider appointing a DPO on a voluntary basis as this might be the most effective and efficient way to discharge their comprehensive GDPR compliance obligations, first and foremost their obligation to be able to demonstrate compliance at any point in time. It will also most likely put organizations in a better position when dealing with supervisory authorities and Data Subjects, and will help streamline privacy-relevant processes across the EU allowing other personnel to focus on revenue-raising and other key tasks.

(b) Data Mapping

Data Mapping – a process of identifying, understanding and mapping out the data collections, uses and flows of an organization – is an essential prerequisite for any privacy compliance strategy. Creating a data map which reflects what data is collected and processed and why, and where that data flows to and from, should be a first step towards GDPR compliance for many businesses. This is by no means a simple task, rather it requires careful planning and input from many business units. But from a GDPR perspective, Data Mapping will go a long way in assisting controllers (and, in some instances, processors) to become compliant with various new privacy requirements as they apply to them, including:

- the requirement to maintain detailed records of an organization’s data processing activities and to make these records available to supervisory authorities on request;

- the accountability requirement according to which controllers must ensure and be able to demonstrate that their processing activities are performed in compliance with the GDPR; and

- the important data protection by design and by default requirements.
In addition to ensuring compliance with legal and regulatory requirements, Data Mapping has multiple other operational benefits. For instance, Data Mapping can help organizations:

- improve the efficiencies of business processes and IT systems (e.g., a Data Map might reveal that data systems and flows can be streamlined);
- use data in smarter ways (e.g., a Data Map may reveal that more data sharing within an organization might be appropriate – subject to suitable privacy controls and limitations); and
- provide valuable insights into data to gain a competitive advantage.

(c) Consent

Obtaining valid consents to data processing activities appears to be one of the really challenging hurdles in practice but is an important one to tackle as a priority. While the concept of consent has long been around across EU Member States and will be retained in substance, the GDPR is much more prescriptive when it comes to the conditions for consent. The key change is that, under the GDPR, consent will require a clear affirmative action. Silence, pre-ticked boxes and inactivity will no longer suffice for there to be valid consent.

Pre-GDPR consents will continue to be valid under the GDPR (without any confirmation or other action from Data Subjects required) provided they conform to the GDPR requirements for consent. Unfortunately, in practice, most pre-GDPR consents will need to be renewed as they either do not conform to the GDPR requirements or it is impossible to demonstrate that they are GDPR-compliant due to a lack of reliable records. For instance, distribution lists used for marketing purposes which have commonly been built organically over time with no reliable records as to how, why or by whom contacts have been added, are unlikely to be supported by consents that are valid under the GDPR.

Moving forward, organizations will also need to put in place systems creating reliable records of consents which will enable them to demonstrate compliance with consent requirements. This is proving to be a real challenge in practice given consents are obtained in multiple ways (e.g., via websites, by emails, even orally in person, etc.).

To further complicate things, it is important to keep an eye on national data protection laws as the GDPR allows Member States to divert from the GDPR and adopt:

- an age below 16 as the age of consent (with 13 being the minimum age of consent);
• rules providing that the prohibition on processing of sensitive data may not be lifted by way of a Data Subject’s consent; and
• specific rules for obtaining consents in an employment context.

(d) Data Breach Notification

The GDPR will introduce general (non-sector specific) data breach notification obligations, which do not currently exist in the vast majority of EU Member States. Subject to limited exceptions, Data Controllers will be required to notify Personal Data breaches to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. These are extremely short time frames in practice. In severe cases data breaches will also need to be communicated to affected individuals.

As interconnectedness, the reliance of business operations on data, and the number of cyber attacks increase, data breaches are becoming a very serious risk for businesses leading to costly business disruptions, reputational losses and fines. Protection against data breaches and putting in place sound data breach incident management plans, should therefore be treated as a compliance priority.

(e) Data Processors

Data processors face the challenge that the GDPR (unlike the Data Protection Directive) will impose enforceable privacy compliance obligations directly on them. For instance, Data Processors will be required by law to:

• implement appropriate technical and organizational measures to ensure a certain level of data security;
• keep detailed records of their processing activities;
• appoint a DPO in certain instances and a representative located within the EU if the processor is located outside of the EU;
• comply with the same cross-border transfer requirements as Data Controllers; and
• notify Data Controllers of data breaches.

Data processors have a lot of work to do to understand their new compliance obligations, decide how to comply with them and assess their operational impact. For example, how will you be discharging your security obligations? What tools/resources will you put in place to satisfy the record keeping requirements? Do you need to or should you appoint a DPO? Do you need to appoint a representative in the EU?

Another important aspect is that controllers and processors will be required to enter into comprehensive processing agreements, the terms of which are
prescribed in detail in the GDPR. Most existing processor agreements do not satisfy the new requirements and require revision. We are already seeing many of these agreements being renegotiated, often a lengthy process in practice.

4. The ePrivacy Regulation

With all eyes are on the GDPR, it is easy to lose track of another important privacy-related legislative proposal in Europe – the ePrivacy Regulation. The ePrivacy Regulation is intended to harmonise data protection rules across the EU in relation to electronic communications (think online privacy) and will complement the GDPR in this respect (as Lex specialist). It will replace the existing Privacy and Electronic Communications Directive which is no longer up-to-date with technological progress and market reality.

In a nutshell, the ePrivacy Regulation will reform the rules relating to direct marketing, the use of cookies, online tracking and location-based tracking. It will also restrict how electronic communications content and metadata may be used respectively. Importantly, the ePrivacy Regulation will apply not only to traditional telecommunications operators but also to so-called Over-the-Top services. Like the GDPR, the ePrivacy Regulation will have a broad territorial scope and will apply to services provided to end-users and devices in the European Union, regardless of where the provider is based.

While the ePrivacy Regulation was originally intended to start to apply at the same time as the GDPR, due to various controversies, it is nowhere near finalized. The EU Parliament adopted the draft Regulation in October 2017 but the trilogue negotiations between the EU Parliament, Commission and Council are yet to begin. So, while on the horizon and worth watching, it remains to be seen what the final rules will look like and it will be a while before they will start to apply.

5. A few final words

Time and cost efforts expended by companies to develop and continually refine comprehensive GDPR compliance programs are more and more perceived by companies as an opportunity to rethink their approach to data. It is no secret that businesses that want to become or remain successful in the digital age will need to leverage digital solutions. Digital transformation is disrupting all sectors and data is a key to success. Indeed, whatever the digital solution (from AI, through internet of thing initiatives, to Big Data – where what is big is not the data but the database, as it contains significant number of data entries), all these new digital tools are fed by, they live on, data. Therefore companies need to use data in smart ways and they need to do so sooner rather than later. Businesses of all sizes should come up with a smart and compliant data strategy. Such strategy would combine the two tasks of (1) finding ways to leverage, and generate revenue from, data, and
(2) doing so in a privacy-compliant way. While such strategy will need to take into account local data protection laws and requirements, the GDPR would be the best starting point for a comprehensive global privacy program.
Argentina

Guillermo Cervio
Buenos Aires
Tel: +54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Roberto Grané
Buenos Aires
Tel: +54 11 4310 2214
roberto.grane@bakermckenzie.com
1. Recent Privacy Developments

**New law on Access to Public Information**

On 14 September 2016, the Argentine National Congress passed Law No. 27,275 on Access to Public Information (“LAPI”), which became effective on 29 September 2017. Even though the right of access to public information was recognized by the Argentine Supreme Court in numerous precedents, up to the publication of the LAPI, such right was only partially regulated by Decree No. 1172/2003 (Annex VII).

The LAPI establishes:

- The right of access to public information, allowing any individual to access, search, require, receive, copy, analyze, process, re-use and re-distribute the information held by the Obliged Subjects (as defined in the law). Such right of access is only restricted by the exceptions provided for in the LAPI.

- That any kind of data contained in a public or private document, independently of its format, which is created, obtained, modified, controlled or held by the Obliged Subjects is presumed to be public.

For the purposes of the LAPI, the following shall be regarded as Obliged Subjects: (i) the Federal Administration (both centralized and decentralized agencies); (ii) legislative and judicial branches; (iii) the Public Ministry for the Defense; (iv) the Public Ministry for the Prosecution; (v) the Council of the Judiciary; (vi) state-controlled corporations and companies (which means any business organization where the Federal Government owns a majority shareholding or holds the majority decision-making power); (vii) corporations and companies in which the Federal Government or its agencies hold a minority shareholding, only with regard to such shareholding; (viii) holders of concessions, licenses and permits over public utilities and public property; as well as Federal Government’s contractors and suppliers; (ix) any private entity receiving public funds from the Federal Government (only with respect to the information produced with or related to the use of the public funds received); (x) any institution or entity whose administration, custody or conservation is managed by the Federal Government; (xi) non-governmental public legal entities (only regarding public law matters and information related to the received public funds); (xii) trusts comprised totally or partially by assets owned by the Federal Government; (xiii) entities which have executed agreements with the Federal Government on the field of technical or financial cooperation; (xiv) the Central Bank; (xv) inter-jurisdictional entities where the Federal Government has either participation or representation; and (xvi) concessionaires, exploiters, managers and operators of gambling and betting establishments.
The list of exceptions, in which the Obliged Subject may refrain from providing the requested information, include:

- expressly classified information (deemed as reserved);
- information which disclosure might affect the functioning of the banking/financial system;
- sensitive personal information;
- industrial, commercial, financial, technical or technological secrets of the Obliged Subjects, and information threatening the life or safety of natural persons.

In addition, the LAPI provides for the creation of the Public Information Access Agency ("Public Information Agency"), which must implement the supporting regulations of the LAPI and create a technological platform to enable the exercise of the rights of the individuals. Finally, the LAPI also regulates the right to request information by imposing the Obliged Subjects the obligation to appoint an individual who shall act as an official for Public Information Access.

**Regulatory Decree to the Law on Access to Public Information**

On 28 March 2017, the Official Gazette published Decree No. 206/2017 ("Decree"), which approved the implementing regulations to the LAPI. The Decree also became effective on 29 September 2017.

The Decree establishes that the Public Information Agency will act under the scope of the Cabinet of Ministers. Further details to the LAPI are contained in the Decree, such as: (i) procedures to request public information; (ii) exceptions to the information obligation of the Obliged Subjects; (iii) complaint procedures; (iv) incompatibilities of the Public Information Agency’s Director; and (v) denials of the Obliged Subjects to the requests for public information.

**Draft bill for the Protection of Personal Data**

In March 2017, a draft bill that modifies the current data protection regime, was submitted to Congress ("Draft Bill"). The Draft Bill will replace, in its entirety, the current Argentine Personal Data Protection Law No. 25,326 ("PDPL") which created the Data Protection Authority ("DPA"), and Law No. 26,951 which regulates the Do Not Call Registry.

In line with the EU GDPR, the Draft Bill:

- limits the scope of Data Subjects to natural persons, excluding legal entities;
- adopts a more comprehensive approach than the PDPL, aiming for the general protection of Personal Data, independently of whether or not such data is stored in a database;
• incorporates new concepts such as genetic data, biometric data and cloud computing;

• includes accountability obligations and eliminates the registration requirement for databases;

• provides for the obligation to notify both the supervisory authority and Data Subjects of a data security breach of their Personal Data, providing for specific terms and information requirements in each case;

• imposes the obligation on governmental agencies/bodies and companies processing sensitive and large-scale data (big data) to appoint a Data Protection Officer, specifying duties, tasks and technical requirements applicable to that role.

Furthermore, the Draft Bill provides for additional: (i) standards for the lawfulness of data processing (in addition to consent); (ii) information requirements to be provided to Data Subjects when collecting their Personal Data; (iii) safeguards recognized as legitimate cross-border data transfer tools, such as Binding Corporate Rules, approved codes of conduct and certification mechanisms.

Finally, the Draft Bill increases the number of Data Subjects' rights by expressly recognizing the right to object to processing (including processing for marketing purposes) and the right to restrict processing and data portability. New regulations in connection with cloud computing (admitted as a data processing tool), sensitive data, minors' consent, impact analysis and data protection by design and default are also addressed.

The most controversial issue of the Draft Bill is its extraterritorial scope, an aspect which is still under review by local regulators.

**Executive Order No. 899/2017.** On 6 November 2017, the Official Gazette published Executive Order No. 899/2017 (“Order”) which provides that any reference to the DPA shall be deemed to the Agencia de Acceso a la Información Pública ("Public Information Agency" or “PIA”). It is therefore expected that the DPA will be absorbed by the Public Information Agency, whose organizational structure and budget have not yet been defined. For simplicity in this chapter references to the DPA shall mean the PIA.

2. Emerging Privacy Issues and Trends

**Mandatory Breach Notification.** There is no specific mandatory obligation under current local data protection regulations to notify the DPA of a security breach. However, best practices would indicate that it is advisable to alert the data owners about the breach in certain cases, to allow them to adopt the appropriate course of action to protect their information and minimize damages. For instance, when the incident affects information related to any
password or similar private information used by its employees, the company should report the incident to the affected employees to allow them to adopt the appropriate course of action (e.g., change of password). It is likely that the DPA will closely monitor the Data Controller’s and Data Processor’s adoption of security measures and registration of databases.

**Online Direct Marketing.** There are no restrictions regarding online direct marketing. Nevertheless, when engaging in direct marketing using various electronic channels, companies should ensure that consumers are given the freedom to choose whether or not to engage in a relationship or receive communications from companies.

**Anti-Spam Legislation.** There is no specific anti-spam legislation in Argentina. The unsolicited commercial electronic messages should contain the procedure by which consumers can avoid receiving unsolicited product or service information. In addition, this information should also be supported with articles from the Data Protection Law and its Executive Order.

**Bring Your Own Device.** The two main concerns regarding this matter are the following:

a. **Monitoring activities**

Usually, the employer informs its employees that by enrolling in the so called “Mobile Device Policy”, they allow their devices to be remotely monitored. As a general rule, an employer may not monitor an employee’s personal emails unless there is a genuine suspicion of the employee being disloyal, acting in breach of company policies or that the company has a serious concern that the employee is using the IT equipment for, e.g., pornographic or racist purposes. Nevertheless, as per current trends, even in these cases, consent of the Data Owner may be required. This matter is highly debatable.

b. **Personal information**

It is likely that an employee whose labor contract is terminated with cause will allege that the loss of certain information will cause damage. Companies should therefore refrain from maintaining information that could be clearly considered as private information of the employees.

**Social Media.** The main impact of social media is in connection with its use by employees. It is advisable that employers put into effect policies regarding the proper use of social media sites. Employees who are allowed to access social media sites during working hours should do so reasonably and must act in good faith. The employer may prohibit or limit the time spent on these sites, and sanction any infringement thereof. Sanctions should be fair and reasonable.

**Employee Monitoring.** Monitoring of employees’ computers is a sensitive matter. Employers should have in place an internal policy – duly notified to
employees – which clearly states that computers, emails received and sent from the company’s email addresses, and other IT resources used or provided by the company are work tools and therefore belong to the company, that said resources should not be used by employees for personal purposes, and that at any time the company may monitor the activities of the employees while using the work tools/resources provided by the company. It is advisable that the internal policy clearly states, in a highlighted fashion, that employees have no expectation of privacy over work tools.

**Documents and Records Retention Policy.** Documents and records retention policies apply, with different criteria depending on the content of the corresponding documents. For example, under the Argentine Civil and Commercial Code, companies have the duty to keep their corporate and accounting books for 10 years. Also, the statute of limitations for the enforcement of most civil and commercial actions is 10 years. In this regard, a 10-year retention period policy would be appropriate for commercially related documents, unless there is a special legal obligation to retain certain documents for a longer period of time. Different statutes of limitation apply for other areas (two years for labor matters, 10 years for social security matters and five years for tax matters).

**Cookie Consent Requirement.** The use of cookies and web beacons would, in principle, be permitted provided that proper notice on their use is given to users (e.g., in the privacy policy). In this regard, the terms and conditions of the privacy policy should indicate that by accepting said terms and conditions, the users accept the deployment and use of cookies and web beacons. It is also recommended that the privacy policy describes the manner in which the cookies can be deactivated (i.e., from browsers) and the consequences for doing so.

**Do Not Call Registry.** On 2 July 2014, the Argentine Congress enacted Law No. 26,951, which creates a “Do Not Call” list applicable at a national level. Pursuant to this law, any natural or legal person has the right to register their mobile or fixed phone numbers on such list on a free basis. Those who promote products or services through telemarking activities are prohibited from contacting any number registered on the list, and are required to search the registry at least once every 30 days and update their internal call list accordingly. Companies that have a pre-existing relationship with a consumer are exempted from such restriction, provided that the calls specifically relate to the purpose of the agreement with the consumer, are performed in a reasonable manner and are made within business hours. Electoral campaigns or campaigns destined for public welfare, health emergency or security emergency are also excluded from such restriction. The supervisory authority is the DPA. On 17 December 2014, the Executive Branch issued Decree No. 2501/2014, which regulates the procedural aspects of the registration and reporting of infringements.
Click-Through/Click-Wrap/Electronic Contracting. There is no integrated regulation that specifically governs electronic contracting, and therefore the general rules for contracts apply. The Argentine Civil and Commercial Code recognizes the existence of electronic contracts, and requires the supplier to provide consumers with all the necessary information to use the electronic method in a correct manner and understand the risks from using same. From an evidentiary perspective, consent can be validly expressed by tacit or express means, and therefore the contract so entered will be subject to evidence (in case it is challenged by one of the parties to the contract). According to limited legal precedents, local courts would consider: (i) evidence regarding the identities of the parties, and acceptance of the agreement by electronic means; (ii) whether the content of the electronic contract has (or has not) been altered after its acceptance; and (iii) if the messages exchanged between the parties have actually been sent and received by said parties (e.g., acknowledgement receipt, confirmatory emails, etc.).

Electronic Signature. In Argentina, electronic signatures are not at the same level of enforceability as written and/or digital signatures. According to the Digital Signatures Law No. 25,506, instruments signed with digital signatures are presumed to be signed by the signatory registered with the certifying licensee and, in the case a party denies the authorship of the digital signature, then such party must evidence its position. On the contrary, instruments signed with electronic signatures do not have this legal presumption; if a party denies the authorship of an electronic signature, then the enforcing party must prove such authorship to the courts.

Binding Corporate Rules. The DPA has not approved the Binding Corporate Rules or “Burrs”, understood as those rules developed for intra-organizational transfers of Personal Data across borders.

Data Protection Enforcement. The DPA is active in enforcing applicable regulations. However, such approach would be friendly and business-oriented in the sense that usually, before applying fines or other penalties, the DPA would seek compliance or corrective actions from the erring companies.

Cybercrime/Cybersecurity. As already indicated, in case of data breach for cybercrimes, there is no need to report to the DPA, but it is highly recommended to alert the data owners, depending on the type of information stolen. In addition, security measures must be taken, depending on the type of stored Personal Data. Please refer to Section 3 for the regulation that provides the applicable security measures.

3. Law applicable

The applicable laws in Argentina on data protection are the following:

- Law No. 25,326 (the “Act”)
• Executive Order No. 1558/2001

• Resolutions issued by the DPA. For instance, Disposition No. 11/2006 regarding “Security Measures for the Processing and Storage of Personal Data Contained in Public Non-State and Private Files, Records, Databases Databanks”; and Disposition No. 4/2009 regarding “Marketing Activities”.

• Disposition No. 11/2006

• Disposition No. 4/2009

• Executive Order No. 899/2017

4. Key Privacy Concepts

a. Personal Data
The Act defines “Personal Data” as information of any kind referring to ascertainable physical persons or legal entities. The Act protects Personal Data used for reporting purposes and recorded in data files, registers, databases or by other technical means.

b. Data Processing
The Act covers the protection of Personal Data with regard to both manual and automatic processing. The Act defines “data processing” as systematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organization, storage, modification, relation, evaluation, blocking, destruction and, in general, the processing of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers.

c. Processing by Data Controllers
The Act defines “Data Processor” as any person – public or private – carrying out, at its sole discretion, data processing, whether contained in files, records, or databases of its own, or through connection therewith. “Data Owner” is defined in the Act as any individual or corporation domiciled in the country, or having offices or branches in the country, whose data is subject to this Act. A Data Controller, a person or organization that holds personal or sensitive information on one or more Data Owners cannot, in principle, process data without the consent of the Data Owners. Nevertheless, under certain circumstances the Data Owner’s consent is not necessary. Furthermore, the Act covers all private persons creating files, records or databases that are not intended exclusively for personal use.

d. Jurisdiction/Territoriality
The Act applies to any physical person or legal entity having a legal domicile, or local offices or branches in Argentina. Registers, data files, databases or
databanks that are interconnected through networks at an inter-jurisdictional, national or international level fall within the federal jurisdiction, and are thus subject to the provisions of the Act. Other registers, data files, databases or databanks may also fall under provincial jurisdiction. In this regard, some of the provinces of Argentina have issued regulations for the “habeas data” remedy. Also, several provinces have adhered to the content of the Act.

e. **Sensitive Personal Data**

The Act defines “Sensitive Personal Data” as Personal Data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior. The Act provides that Data Owners cannot be compelled to provide Sensitive Personal Data (nevertheless, certain exceptions may apply, such as health-related and union membership information, and information which is necessary for employment purposes). It is prohibited to create files, banks or registers storing information that directly or indirectly reveal Sensitive Personal Data.

f. **Employee Personal Data**

Employees’ Personal Data is likely to include Sensitive Personal Data (e.g., health-related and union-membership information) and non-Sensitive Personal Data. Generally, an employer may be entitled to process certain Sensitive Personal Data of its employee without the employee’s consent if and to the extent it is necessary for employment purposes. This occurs, nevertheless, in very specific and limited cases and should be determined on a case-by-case basis. The Act does not set forth when it is “necessary” for the employer to collect Sensitive Personal Data.

5. **Consent**

a. **General**

Consent of the Data Owner is generally required prior to the collection, processing and disclosure of Personal Data. The processing of Personal Data is unlawful unless the Data Owner has given his or her express consent in writing, or through any other similar means, depending on the circumstances. The consent must appear in a prominent and express manner. Furthermore, consent must be an informed consent and is revocable by the Data Owner.

Consent shall not be deemed necessary when Personal Data:

- is secured from unrestricted public access sources;
- is collected for the performance of the duties inherent to the powers of the state or in virtue of legal obligations;
- consists of lists limited to name, ID number, tax or social security identification number, profession, date of birth, and domicile;
• is derived from a contractual, scientific or professional relationship with the Data Owner (e.g., employment relationship) provided that such Personal Data is necessary for the development of or compliance with the terms of such relationship; or

• is collected by financial entities in connection with transactions performed by the customers of said financial entities.

b. Sensitive Data
The Act requires express consent from Data Owners for the processing of Sensitive Personal Data.

Exceptions to this rule are the following:

• processing of Sensitive Personal Data for reasons of general interest authorized by applicable laws;

• processing of Sensitive Personal Data for statistical or scientific purposes, provided that Data Owners cannot be identified (dissociation method);

• processing of Sensitive Personal Data referring to records on criminal or other offenses, provided that the same is processed only by competent public authorities within the framework established by applicable laws and regulations; or

• processing of Sensitive Personal Data relating to the physical or mental condition of patients by public or private health institutions, and medical science professionals, in pursuance of the principles of professional secrecy.

c. Minors
There is no provision that specifically addresses consent requirements for minors. In general, consent cannot be obtained from minors, but can be given by a legal guardian or parent. The Comprehensive Protection of the Rights of Children and Teens Act No. 26,061 prohibits the exposure, circulation and/or disclosure of Personal Data and images of minors in any medium without consent from the minor and its parents, tutors or legal representatives, when such actions may affect the dignity of reputation of the minors or are intrusive to their private life.

d. Employee Consent
There is no provision that specifically addresses consent requirements for employees.
e. **Online/Electronic Consent**

In Argentina, electronic consent is permissible and can be effective if properly structured and evidenced.

6. **Information/Notice Requirements**

An organization that collects Personal Data must provide Data Owners with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Owners; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; and how to access and/or correct the Data Owners’ Personal Data.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. **Rights of Individuals**

Data Owners have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Owner; access the Data Owners’ Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Owners’ Personal Data; request the deletion and/or destruction of the Data Owners’ Personal Data; and exercise the writ of habeas data.

9. **Registration/Notification Requirements**

The Act states that any public or private “data file, register or database intended to provide reports must be registered with the registry to be established for such purpose”. The DPA has extended the registration requirement to encompass not only data collected in order to provide reports, but also all data collected for purposes beyond personal use.

10. **Data Protection Officers**

Although the Argentine Data Protection Law No. 25,326 does not set forth a specific requirement to appoint a Data Protection Officer, internal procedural regulations issued by the DPA for cases of audits and inspections establish that Data Controllers are required to appoint an “individual responsible for a database” in the privacy policy of each database, who will be accountable for the privacy practices of the organization. According to the criteria adopted by the DPA, such individual should be located in Argentina.
11. International Data Transfers

The transfer of Personal Data to a third country may take place only if such third country provides for similar levels of protection as the ones established by Argentine law. Exceptions to this requirement are the following:

- consent of Data Owners;
- execution of an international data transfer agreement by and between the data exporter and the data importer, in accordance with certain guidelines issued by the DPA;
- international judicial cooperation;
- exchange of medical information when so required for the treatment of the Data Owner;
- exchange of medical information required for epidemiological research, provided that Data Owners cannot be identified (dissociation method);
- stock exchange or banking transfers in pursuance of the applicable laws;
- when the transfer is agreed upon within the framework of international treaties signed by Argentina; or
- when the transfer is made for international cooperation purposes between intelligence agencies in order to fight against organized crime, terrorism and drug trafficking.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

The DPA has approved three different levels of security measures that the person responsible for a database shall enforce depending on the type of Personal Data that is processed in such database. The different levels of technical and organizational security measures are the following: (i) basic level (for processors of general Personal Data); (ii) medium level (for utilities, government agencies or private entities that must keep their data secret); and (iii) critical level (for entities processing Sensitive Data). The technical and organizational security measures should include the procedure to be followed by the company in case Personal Data stored in the database is stolen.
13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations shall be liable together with third-party providers in case of a breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings, and/or private rights of action. Furthermore, the DPA keeps a record of infractions that is publicly available, so reputational damages may also exist.

15. Data Security Breach

There is no specific mandatory obligation under the current applicable regulations to notify the DPA of a security breach.

From a practical standpoint, when a security breach occurs and becomes public, the DPA usually initiates an investigation to confirm whether the company affected by the security breach has adopted the security measures required by the Act and regulations enacted by the Authority.

There is also no obligation under the Act to notify consumers about a security breach. Nevertheless, companies affected by a security breach usually consider reporting the incident to Data Owners to allow them to adopt the appropriate course of action to protect their information and minimize damages. For instance, when the incident affects information related to any password or similar private information used by its employees, the company should report the incident to the affected employees to allow them to adopt the appropriate course of action (e.g., change of password).

16. Accountability

Data controllers whose databases are subject to medium level security measures under local regulations, are required to conduct trials prior to the implementation of new information systems and/or technologies, which shall not be performed directly into databases containing Personal Data, unless such organizations have adopted the necessary security measures required by local regulations.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Argentina as long as they are in compliance with local laws. If an organization plans to create a database with
the information received as a consequence of the implementation of a whistle-
blower hotline, such database will have to be registered with the Authority.
Furthermore, employees will have to be duly informed about the existence of
the whistle-blower hotline and relevant policies in relation thereto.

18. E-Discovery
The process whereby electronically-stored information is reviewed, processed
and presented for the purposes of litigation or regulatory requests is
recognized under Argentine law. Electronic information can be stored in
databases as structured content, in emails or instant messages as semi-
structured content, and in documents or files as unstructured content.
Nevertheless, employers should advise employees about the implementation
of an e-discovery system and the fact that computer use in the workplace
(e.g., email, Internet) is being monitored and that information such as emails
will be stored. Nevertheless, employees may request the employer to destroy
any Personal Data stored as a consequence of the implementation of the e-
discovery system. The employer may justify its position by alleging that such
information is crucial for complying with regulations and/or for the purposes of
litigation.

19. Anti-Spam Filtering
The main issues relate to how the spam-filtering solution is implemented,
(e.g., whether the spam-filtering solution is automatic and applicable in the
same manner to all of the employees and whether it allows certain IT officers
of the company to monitor for spam). In practice, companies install software
that filters spam and automatically sends a list of all of the spam that was
filtered by the system to the relevant employee.

20. Cookies
The use of cookies and web beacons would, in principle, be permitted
provided that proper notice on their use is given to users (e.g., in the privacy
policy). In this regard, the terms and conditions of the privacy policy should
indicate that by accepting said terms and conditions, the users accept the
deployment and use of cookies and web beacons. It is also recommended
that privacy policies describe the manner in which the cookies can be
deactivated (i.e., from browsers) and the consequences for doing so.

21. Direct Marketing
Direct Marketing performed by fixed or mobile phones is regulated by the so-
called “Do Not Call” regulations, according to which those individuals or legal
entities that promote products or services through telemarking activities are
prohibited from contacting any number registered with the list, and are
required to search the registry at least once every 30 days and update their
internal call list accordingly. As regards online direct marketing, when
engaging in direct marketing using various electronic channels, companies should ensure that consumers are given the freedom to choose whether or not to engage in a relationship or receive communications from companies. In addition, the messages provided through electronic means should also contain a transcription of certain articles from the Data Protection Law and its Executive Order.
Australia

Anne-Marie Allgrove
Sydney
Tel: +61 2 8922 5274
ann-marie.allgrove@bakermckenzie.com

Patrick Fair
Sydney
Tel: +61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Sydney
Tel: +61 2 8922 5204
adrian.lawrence@bakermckenzie.com

Toby Patten
Melbourne
Tel: +61 3 9617 4456
toby.patten@bakermckenzie.com
1. Recent Privacy Developments

The key legislation regulating privacy in Australia is the Privacy Act 1988 (the “Privacy Act”). New mandatory data breach notification requirements come into effect from 22 February 2018 as part of a recent amendment to the Privacy Act and will apply to organizations which are subject to the Privacy Act.

These changes mean that an organization will be required to notify the regulator and/or the affected individuals if the organization has reasonable grounds to believe there has been an eligible data breach.

An eligible data breach is when there is an unauthorized access, disclosure, or loss of personal information that a reasonable person would conclude is likely to result in serious harm to the individuals to whom the personal information relates. There are certain exceptions to these notification obligations, e.g., where the organization takes remedial steps which remove the risk of serious harm. Further details are set out below.

There have been some determinations, as well as a number of privacy assessments and several enforceable undertakings over the last year. The Office of the Australian Information Commissioner (the “OAIC”) has also undertaken a number of investigations into the actions of agencies or private sector organizations.

The recent determinations made were in relation to either the disclosure of personal information to third parties or the organization’s failure to take reasonable steps to protect the complainant’s personal information. Most of these determinations resulted in orders for payment of approximately AUD 3,000 in compensation. One determination, which involved the disclosure of medical information, resulted in an order for payment of AUD 12,000 in compensation to the complainant. These determinations show that the Commissioner will rely heavily on the APP Guidelines and other guidelines (referred to below) in these cases, for example, in determining whether an “unauthorized disclosure” has taken place. The OAIC has released various guidelines. The key guidelines are as follows:

- **APP Guidelines** – these provide practical guidance on the application and interpretation of the Australian Privacy Principles (“APPs”).

- **Guide to developing an APP privacy policy** – this sets out a step-by-step process to assist organizations in complying with APP 1, which relates to the creation of an organization’s privacy policy.

- **Guide to undertaking privacy impact assessments** – a privacy impact assessment identifies how a project can affect an individual’s privacy and formalizes recommendations for minimizing the impact. This guide sets out 10 steps to planning a privacy impact assessment.
• **Notifiable Data Breaches guides** – these guides have just been finalized and set out practical guidelines with respect to the new mandatory data breach notification obligations in relation to identifying the covered entities, what to do when more than one organization is involved, how to identify if there is an eligible data breach, exceptions to notification obligations, assessing a suspected data breach, notifying individuals about an eligible data breach, what to include in an eligible data breach statement, and the OAIC’s role in the scheme.

• **Guide to securing personal information** – this guide sets out practical steps for organizations to appropriately protect the personal information that they hold, e.g., the circumstances to consider when formulating reasonable steps, the internal processes to put in place.

• **Handling privacy complaints** – this guide details the regulator’s approach to handling complaints (the commissioner can make enquiries into the matter, investigate, and/or attempt to conciliate, and may also decline to investigate complaints).

• **Privacy management framework** – this guide sets out steps that the regulator has indicated it expects organizations to take to ensure their compliance with the APPs, including with respect to internal processes, culture, and response to complaints.

• **Privacy Regulatory Action Policy** – this policy indicates that the regulator’s enforcement approach will generally be conciliatory, working together with organizations to ensure compliance rather than necessarily enforcing immediate strict sanctions.

• **Privacy management plan template** – this is a template for a privacy management plan, a document which sets specific targets to identify how an organization will implement the “privacy management framework” referred to above.

2. Emerging Privacy Issues and Trends

• **Increase in privacy complaints** – the regulator has indicated that there continues to be an increase in complaints and that recent complaints have been generally due to a growing interest in privacy and privacy governance due to developments in technological, social, commercial and government service delivery environments, with more individuals indicating they avoid businesses with a history of privacy issues and mobile apps.

• **Stricter view towards hacking incidents defense** – the regulator has also indicated that it is not sufficient to use being hacked as an excuse if the organization has not implemented appropriate security protections.
3. Law Applicable

As noted above, the key privacy legislation in Australia is the Privacy Act which applies to the private sector and Commonwealth public sector. The key data-handling principles applicable to both the private and public sectors are contained in the 13 APPs.

The APPs are grouped into five sets of principles intended to reflect the “life cycle” of handling of personal information. They cover:

- the practices, procedures and systems that entities have in place relating to how they handle personal information;
- how entities collect personal information, including unsolicited personal information;
- how entities manage personal information, including how they use and disclose personal information, disclose information overseas, and how they use government identifiers;
- how entities ensure the integrity, quality and security of personal information; and
- how entities deal with requests for access to, and correction of, personal information.

**APP Guidelines**: The regulator responsible for the Privacy Act, the OAIC has issued guidelines to provide further context to the APPs.

Some states and territories have privacy legislation and/or administrative guidelines which apply to the state/territory public sector.

Victoria and New South Wales also have specific legislation governing the collection, storage, use and transfer of health information (the Victorian Health Records Act 2001 and the New South Wales Health Records and Information Privacy Act 2002), which applies in addition to the applicable APPs. “Health information” is broadly defined as personal information about the physical or mental health or a disability of an individual, or information relating to the provision of health services, the donation of body parts or substances, or genetic information that could be predictive of the health of an individual or their relatives.

To the extent that an organization collects, uses, stores or discloses health information, it will be subject to the Health Privacy Principles, which require consent in Victoria and notification in New South Wales when that health information is collected and which restrict trans-border data flows out of the state, except in limited circumstances.

The Australian Capital Territory also has health specific legislation, the Health Records (Privacy and Access) Act 1997, which covers health records held in
the public sector in the Australian Capital Territory. This legislation also seeks to apply to acts or practices in the private sector to the extent not covered by the Privacy Act.

Finally, Victoria and the Australian Capital Territory also have human rights legislation, which includes a right for individuals not to have their privacy interfered with unlawfully or arbitrarily.

The responses below relate specifically to the obligations in the Privacy Act that are applicable to private and Commonwealth public sector entities.

4. Key Privacy Concepts

a. Personal Data

“Personal information” is defined in the Privacy Act as “information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not”.

The APP Guidelines provide that the concept of information being “reasonably identifiable” can include information which is not “personal information” in its own right, and can therefore still come under the Privacy Act if there is a likelihood of it being combined with other information held by an organization which would enable an individual to be reasonably identifiable.

b. Data Processing

The APPs in the Privacy Act apply to the acts and practices of entities in respect of personal information, including in relation to open and transparent management of personal information (including clear and technology neutral privacy policies), anonymity, collection of solicited and unsolicited information, notification of collection, use, disclosure, direct marketing, cross-border disclosure, use of government-related identifiers, quality and security of the information held and access and correction of information held. The EU definition of “processing” is not used in the Privacy Act. The Privacy Act applies to personal information held in hard-copy and electronically and to both manual and automated handling of data.

c. Processing by Data Controllers

The Privacy Act applies to entities that undertake any of the acts or practices covered by the APPs. No distinction is made between entities that control the personal information and those that process it on behalf of other entities.
d. Jurisdiction/Territoriality

Subject to certain exemptions (see below), the Privacy Act applies to acts and practices:

- done in Australia in relation to personal information by an entity that is subject to Australian law (other than state or territory Authorities); and
- done outside of Australia in relation to personal information of an Australian citizen or person living in Australia by an entity that either has a link to Australia (such as being a Commonwealth government agency, a partnership formed in Australia or a body corporate incorporated in Australia) or that carries on business in Australia (including by having an online presence in Australia) and collected or held the information in Australia at the time of the act or practice.

The Privacy Act contains a number of exemptions, including in respect of acts or practices:

- of individuals only for the purpose of or in connection with their personal, family or household affairs, or otherwise other than in the course of a business carried on by that individual;
- of small businesses with a turnover of AUD 3 million or less (except those which: are related to an entity that has a turnover greater than AUD 3 million; provide a health service; or satisfy other criteria specified in the Privacy Act);
- relating to employee records (see Section 4(f) below for further detail); or
- undertaken overseas and that are required by foreign laws.

e. Sensitive Personal Data

“Sensitive information” is personal information relating to racial or ethnic origin, political opinions, membership of a political association, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, criminal record, biometric information or health information.

Pursuant to APP 3, an entity must not collect sensitive information unless:

- the entity obtains the consent of the individual (see Section 5(a) below for further detail) and the information is reasonable necessary for the activities or functions of the entity;
- collection is required by law;
- collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where it is unreasonable or
impracticable to obtain the consent of the individual to whom the information relates;

- the information is collected by a non-profit organization and relates solely to the organization’s activities and to the organization’s members or persons who have regular contact with the organization in connection with its activities;

- collection is necessary for the establishment, exercise or defense of a legal or equitable claim;

- where the entity is a Commonwealth enforcement body, the collection is necessary for the performance of that enforcement body’s functions or activities;

- the information is collected in the process of providing a health service, and is either collected as authorized by law or subject to a professional code of ethics; or

- the information is collected in the course of medical research that is subject to professional safeguards and where obtaining consent is impracticable, and the research cannot be performed without the information being collected.

Unless consent is given for an additional use, sensitive information may only be used for the purpose for which it was collected or for a secondary purpose directly related to the purpose of its collection for which the individual would reasonably expect the information to be used.

f. Employee Personal Data

Employee records are given a limited exemption from coverage under the Privacy Act, to the extent applicable to a private organization (as opposed to a Commonwealth public sector agency). This exemption effectively allows private employers to use information concerning their employees for appropriate internal purposes. Three requirements need to be satisfied for the exemption to apply:

- the organization is acting in its capacity as a current or former employer of an individual;

- the use of employee information is directly related to a current or former employment relationship between the employer organization and the individual; and

- the use of employee information is directly related to an employee record held by the employer organization and relating to the individual.

For the exemption to apply, the individual and the organization must be or have been in an employment relationship. The Privacy Act does not define the
The use of employee information must be directly related to the employment relationship and also must be directly related to employee records held by the employer. This is intended to prevent employers from using employee records for commercial purposes unrelated to the employment relationship or exploiting the employee records exemption for commercial purposes.

The employee records exemption only applies to employee records held by the employer and does not continue if the employee records are disclosed by the employer to another organization. For example, if records containing personal information about an employee are disclosed to the employer’s insurer for the purposes of workers’ compensation insurance, then those records do not retain their exempt status in the hands of the insurance company. That is, in the hands of the insurance company, the personal information is subject to the coverage of the Privacy Act.

**g. Data handling practices**

Entities are required to take reasonable steps to implement practices, procedures and systems to ensure they comply with the APPs and can deal with inquiries or complaints about their compliance with the APPs. This principle is intended to keep the Privacy Act up to date with international trends and encourage entities to ensure that privacy compliance is included in the design of information systems, goods and service offerings from their inception. An organization is expected to take an active role in monitoring its privacy handling practices, including determining whether information it holds is still required for the purposes for which it was collected, the accuracy of that information and whether the use of identifiable information is necessary for an organization’s intended purposes or if de-identified information could instead be used. Information which is no longer required should be destroyed or de-identified.

5. **Consent**

a. **General**

There is no express requirement for an entity to obtain an individual’s consent to collect personal information so long as the entity only uses that information for the purpose for which it was collected or for a related purpose (or directly
related secondary purpose in the case of Sensitive Data) for which the individual would reasonably expect the information to be used. Except in limited circumstances, an entity must obtain the individual’s consent to use the Personal Data for any other purpose.

Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is usually understood to only cover the identified purpose(s).

There is no mandatory requirement that consent must be in writing for it to be valid. It can be usually provided orally or in different forms and formats. The Data Subject also has the right to withdraw consent at any time.

In addition, consent does not need to be in the local language provided that the Data Subject understands the language in which consent is given.

b. Sensitive Data

Australian law recognizes Sensitive Data as a special category of Personal Data. It is therefore subject to additional and special consent requirements. In non-binding guidelines, the Privacy Commissioner expressed the view that an entity would ordinarily need clear evidence that an individual had consented to it collecting Sensitive Data (see Section 5 (a)).

c. Minors

While consent from minors is not specifically addressed in the Privacy Act, the Privacy Commissioner has expressed the view through non-binding guidelines that organizations should consider in each case whether an individual has capacity to give consent. According to the guidelines, “as a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person”.

d. Employee Consent

In Australia, there are some doubts as to whether consent given in the context of an employment relationship can be considered valid. It is questionable whether consent would qualify as voluntary, given that the employee may feel forced to consent due to the subordinate nature of his/her relationship with the employer. Consent has also been construed as misleading where statutory permission to collect, process, and use Personal Data is available. As a matter of practice, in order for such consent to be valid, the employer may need to be able to demonstrate that the employee had a genuine option not to consent. This issue arises less commonly under the Privacy Act because of
the limited employee records exemption for some aspects of employee record processing (see Section 4(f)).

e. Online/Electronic Consent
In Australia, online or electronic consent is permissible and deemed effective if it is properly structured and evidenced.

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) whether Personal Data is collected from a third party or, if the Data Subject is not aware that the organization has collected the Personal Data, the fact that the organization has collected that Personal Data and the circumstances of the collection; (iii) whether the collection is required or authorized by Australian law or court order, the fact that the collection is required by that law or court order (including the details of the law or court which issued the order); (iv) the types of Personal Data being collected; (v) the purposes for collecting Personal Data; (vi) the fact that the organization has a privacy policy containing information on how the Data Subject may access Personal Data about the Data Subject and seek correction, and associated complaint processes; (vii) third parties to which the organization will disclose the Personal Data; (viii) the consequences to the Data Subject if the Personal Data is not collected; and (ix) whether the Personal Data is likely to be disclosed outside of Australia, and if so, to which countries (if known and practicable to specify those countries).

7. Processing Rules
An organization that processes Personal Data must: (i) limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; (ii) anonymize the Personal Data whenever possible; (iii) provide the Data Subject with the option to use a pseudonym or remain anonymous whenever possible; (iv) and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Data.
9. Registration/Notification Requirements

An organization that collects and processes Personal Data is not required to register, file and/or notify the appropriate data authority.

10. Data Protection Officers

In Australia, although it is considered best practice to do so, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization. However, organizations are required to make available a privacy policy on request from a Data Subject (see Section 1).

11. International Data Transfers

If an organization discloses Personal Data to a recipient outside of Australia, it must take reasonable steps to ensure that the recipient does not breach the APPs. Unless an exception applies, if the recipient handles the Personal Data in a manner that would breach the APPs if that recipient were subject to the APPs, the organization that disclosed the information will be taken to have breached the APPs. A key exception is if the recipient to which Personal Data is disclosed is subject to a law or binding scheme which provides the same protection as under the Privacy Act, and there are mechanisms that the Data Subject can access to enforce that law or binding scheme. A further exception is if the organization expressly informs Data Subjects that if information is disclosed outside of Australia, the organization will not be responsible for any failure of the recipient to protect the Personal Data in a manner consistent with the APPs, and having been so informed the Data Subject consents to the disclosure.

12. Security Requirements

Organizations are required to take steps to: (i) ensure that Personal Data in its possession and control are protected from unauthorized access and use; and (ii) implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties should ensure there are contractual or other means in place to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors, including, for example, the financial sector. In case of a data breach incident, the outsourcing organization may be held liable together with the third-party provider.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, class actions, and/or private rights of action.

15. Mandatory Data Breach Notification Requirements

From 22 February 2018, mandatory data breach notification obligations will come into effect as part of the Privacy Act.

The data breach notification requirements apply to all personal information and all industries.

An eligible data breach requiring notification is triggered when there is an unauthorized access, disclosure, or loss of personal information that a reasonable person would conclude is likely to result in serious harm to the individuals to whom the personal information relates.

An organization will be exempt from notification if:

i. the organization takes sufficient remedial action in response to unauthorized access or disclosure of personal information such that the access or disclosure would not likely result in serious harm;

ii. the organization takes sufficient remedial action in response to loss of personal information such that there is not unauthorized access to or disclosure of the information or any access or disclosure would not likely result in serious harm;

iii. the organization is a law enforcement body and the CEO believes on reasonable grounds the disclosure would likely prejudice one or more “enforcement related activities”; or

iv. notification would be inconsistent with any Commonwealth law that prohibits or regulates the use or disclosure of information (“secrecy provisions”).

Subject to the exemptions above, an organization must, as soon as practicable after the organization becomes “aware that there are reasonable grounds to believe” there has been an eligible data breach, prepare a statement regarding the breach (“Statement”) and provide it to the Information Commissioner.

As soon as practicable after completion of the Statement to the Information Commissioner, the organization must notify each individual to whom the personal information relates, or the individuals who are at risk from the eligible data breach.
If the organization cannot do either of these, the organization must publish a copy of the Statement on its website (if it has one) and otherwise take reasonable steps to publicise the contents of the Statement.

There is no legal requirement to notify other bodies but the guidance issued by the Privacy Commissioner suggests that consideration be given to notifying the Federal Police, insurers, credit card companies, professional regulatory bodies and/or any government agency that has an association with the relevant information.

Under the Privacy Act, the Information Commissioner has the power to investigate organizations based on complaints or of the Commissioner's own accord, accept enforceable undertakings, make determinations, apply to the court for injunctions or civil penalties. The maximum penalty for a corporation for serious and repeated interferences of privacy is AUD 2,100,000.

16. Accountability

The Privacy Act is in many ways non-prescriptive, and puts the onus on an organization to develop its systems such that privacy compliance is a key consideration. The OAIC has stated that “establishing a comprehensive and practical privacy policy … will get you started with a “privacy by design” approach to your business”, and further recommends that organizations look closely at their information security plans. Finally, it is also recommended that organizations conduct privacy impact assessments for new projects. The OAIC has issued a “Privacy Impact Assessment Guide” to assist organizations.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Australia, provided that they are in compliance with local laws.

18. E-Discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved and advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.
20. Cookies

There are no specific laws/rules that regulate the use and deployment of cookies in Australia. In general, the use of cookies must comply with data privacy laws.

21. Direct Marketing

Whether businesses can use Personal Data for direct marketing will depend on how they collected the information (whether it was directly from the relevant Data Subject or from a third party) and whether individuals would reasonably expect their information to be used for this purpose. There is also an opt-out requirement that applies to all direct marketing communications. Additional restrictions apply to the use of Sensitive Data for direct marketing.

In addition to requirements under the Privacy Act, direct marketing communications are also subject to requirements under the Spam Act 2003, which prohibit the sending of electronic commercial messages without consent and require all such messages to contain certain information and an unsubscribe facility. The Do Not Call Register Act 2006 prohibits businesses from contacting individuals on the Do Not Call Register by telephone or fax except in certain restricted circumstances.

To the extent the Spam Act or the Do Not Call Register Act applies, the Privacy Act does not apply.

As an example of the interaction between the Spam Act and the Privacy Act, the Australian Communications and Media Authority which enforces the Spam Act has indicated that targeted advertising to a social media account may not be spam whiles the OAIC has indicated that in the APP Guidelines that the display of an advertisement on a social media site that an individual is logged into where those advertisements are tailored based on that individual’s browsing history may be direct marketing.
Austria

Dr. Lukas Feiler, SSCP, CIPP/E
Vienna
Tel: +43 1 24250 450
lukas.feiler@bakermckenzie.com

Marisa Elisa Schlacher
Vienna
Tel: +43 1 2 4250 278
marisa.schlacher@bakermckenzie.com
1. Recent Privacy Developments

The Data Protection Amendment Act 2014, which was passed in May 2013 and entered into force on 1 January 2014, transformed the Data Protection Commission into a monocratic agency and renamed it the Data Protection Authority (“Authority”). Appeals against decisions by the Authority will now have to be lodged at the Federal Administrative Court, which was created by the Administrative Judicial Reform in 2012.

After long negotiations with the US Department of Commerce, the European Commission announced the EU-US Privacy Shield on 12 July 2016. Starting 1 August 2016, data transfers from Austria to a US company that has obtained a certification under the Privacy Shield no longer require the Authority’s prior approval. While the Privacy Shield is likely to be ultimately challenged by privacy activists before the European Court of Justice, the Authority fully accepts international data transfers on the basis of the Privacy Shield.

The EU General Data Protection Regulation 2016/679 (“GDPR”) entered into force on 14 April 2016 and will be directly applicable in Austria from 25 May 2018. In order to incorporate the GDPR into national law, the Austrian Federal Data Protection Act 2018 (“DPA 2018”) has been passed by the Austrian Parliament and has been promulgated in Austria’s Federal Law Gazette. The DPA 2018 will enter into force on 25 May 2018 and thereby repeal the current Austrian Federal Data Protection Act 2000 (“DPA 2000”).

The DPA 2018 has a minimalistic approach regarding the use of opening clauses and generally implements only mandatory opening clauses.

The most important subject matters covered by the DPA 2018 are:

- The processing of the Personal Data of a child in an online context on the basis of the child’s consent is lawful where the child is at least 14 years old (§ 4 para 4 DPA 2018);
- The DPA 2018 does not provide any protection for data relating to legal persons – however, the constitutional right to data protection under § 1 DPA 2000 remains unchanged and will continue to protect data relating to legal persons (but no fines will exist in case of any violation of this constitutional right);
- The processing of Personal Data relating to criminal convictions and offenses or related security measures is authorised according to § 4 para 3 DPA 2018 subject to a prevailing legitimate interest of the controller or a statutory authorization.

2. Emerging Privacy Issues and Trends

**Internal compliance investigations** – Internal compliance investigations are becoming more common, particularly with potential competition law
enforcement actions and leniency applications. The requirements concerning the confidentiality and swiftness of such investigations pose significant challenges under Austrian data protection law, in particular if the investigation entails the review of corporate and private emails sent or received via corporate email accounts. Practice has shown that compliance risks can only be mitigated to acceptable levels if certain technological safeguards are implemented in the forensic process.

**Big Data** – The use of analytics applications in analyzing huge amounts of typically unstructured data has significant economic potential for any enterprise and also brings with it serious data protection compliance challenges regarding the principle of purpose limitation. To address these challenges, data protection should be considered early on when designing Big Data applications and the associated (automated) decision processes.

3. **Law Applicable**

The amended Austrian Federal Data Protection Act 2000, effective as of 1 January 2000, which implements the Data Protection Directive 95/46/EC and was last amended by the Data Protection Amendment Act 2014 (which was passed in May 2013 and entered into force on 1 January 2014). As from 25 May 2018, the DPA 2000 will be replaced by the new DPA 2018 which incorporates the GDPR into national law.

4. **Key Privacy Concepts**

a. **Personal Data**

The DPA 2000 applies to information relating to Data Subjects who are identified or identifiable (individuals and legal persons) (the “Data Subject”).

b. **Data Processing**

“Processing of data” means collecting, recording, storing, keeping, sorting, comparing, modifying, linking, reproducing, culling, disseminating, utilizing, committing, blocking, deleting, destroying or any other kind of handling of data, with the exception of the transmission of data.

“Transmission of data” is the transfer of data to recipients other than the Data Subject, the Controller or a Processor, in particular the publishing of such data as well as the use of the data for another application or purpose.

“Committing of data” is the transfer of data from the Controller to a Processor.

“Use” describes any kind of handling of data, therefore includes both the processing and the transmission of data.

c. **Processing by Data Controllers**

The DPA 2000 applies to the party responsible for the purposes and manner in which Personal Data is to be used (“Data Controller”). If the Data Controller
outsources processing activities to a third party (a “Processor”), that
Processor is subject to the DPA 2000 as well.

d. Jurisdiction/Territoriality
The DPA 2000 applies to:

- Data Controllers established in Austria;
- Data Controllers established outside Austria, but within an EU Member
  State that uses Personal Data for an establishment that the Data
  Controller has in Austria;
- Data Controllers not established in any EU Member State which uses
  Personal Data in Austria.

e. Sensitive Personal Data
The DPA 2000 imposes additional requirements for the use of special
categories of Personal Data (“Sensitive Personal Data”) – that is, data relating
to natural persons concerning their racial or ethnic origin, political opinion,
religious or philosophical beliefs, trade union membership, health and sexual
life. Specifically, the use of Sensitive Personal Data is prohibited, unless

certain conditions are met, including:

- the Data Controller obtains the explicit and unambiguous consent of the
  Data Subject (see Section 5(b) below);
- the use is necessary to protect the vital interests of the Data Subject or of
  a third party where the Data Subject is physically or legally incapable of
  giving consent;
- the data has evidently been made public by the Data Subject himself or
  herself;
- the use is necessary in order to assert, exercise, or defend legal claims,
  and there is no reason to assume that the Data Subject has an overriding
  legitimate interest in excluding the use;
- the use is necessary for the purposes of scientific research, and the
  scientific interest in carrying out the research project substantially
  outweighs the Data Subject’s interest in excluding the use, and the
  purpose of the research cannot be achieved in any other way or would
  otherwise necessitate disproportionate effort;
- the use is necessary for medical purposes and the processing is
  undertaken by a health professional or person with the equivalent duty of
  confidentiality as a health professional; or
- the use is required in view of the Data Controller’s rights and obligations
  in connection with labor or employment law and is admissible pursuant to
special legal provisions, whereby the rights of the works council relating to the use remain unaffected.

f. Employee Personal Data
Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information, religious denomination) and Personal Data.

An employee’s Sensitive Personal Data generally may only be processed with the employee’s explicit consent (as the other circumstances mentioned in Section 4(e) above will usually be irrelevant in a standard employment relationship), unless specific statutory rules (other than the DPA 2000) otherwise allow the processing of such data, as is the case, e.g., with respect to information regarding religious denomination for church tax reasons (pursuant to relevant tax provisions).

An employee’s Personal Data may be processed by a Data Controller in certain circumstances, including if the processing activities are necessary for the performance of the employment contract, i.e., if: (i) they are required for the fulfillment of primary or collateral contractual or pre-contractual duties; or (ii) they are necessary to safeguard justified interests of the Data Controller and there is no reason to assume that the employee has an overriding legitimate interest in his or her Personal Data being excluded from processing or use.

A fallback justification for the processing of both Sensitive Personal Data and Personal Data in the employment context is the provision of consent by the Data Subject. However, it is debatable whether consent can be validly given in the employment context (see Section 5(d) below).

5. Consent

a. General
Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.
There is no requirement that consent must be in writing. It can be provided orally or in different forms and formats. In addition, the Data Subject also has the right to withdraw consent at any time.

Generally, consent must be in the local language to be valid. However, it may be considered valid consent even if it is not in the local language if the Data Subject understands the language in which consent is given.

Pre-GDPR consents will continue to be valid under the GDPR (without any confirmation or other action from Data Subjects required) provided they conform to the GDPR requirements for consent.

b. Sensitive Data
Austrian law recognizes Sensitive Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed with the express consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances.

c. Minors
While consent from minors is not specifically addressed in the DPA 2000 or any other law currently applicable, the general rule is that minors are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor, and may even be allowed to obtain information about the minor from third parties without the need of consent from the minor. Nevertheless, there are certain circumstances where consent given by a minor may be considered valid.

Article 8 GDPR makes express provisions for consents provided by children in an online context. It prescribes that the age of consent is 16 unless Member State law provides for a younger age of consent (which must not be below 13). The Austrian legislator made use of this opening clause and stipulates that the processing of the Personal Data of a child on the basis of the child’s consent is lawful where the child is at least 14 years old (§ 4 para 4 DPA 2018).

d. Employee Consent
In Austrian legal literature, there are doubts as to whether consent given in the context of an employment relationship can be considered valid. First, it is questioned whether the consent would qualify as voluntary, given that the employee may feel forced to consent due to the subordinate nature of his/her relationship with the employer.

Secondly, it has been held that consent would be misleading where statutory permission to collect, process, and use Personal Data is available.
Therefore, a consent declaration is only considered unproblematic if the declaration of intent is based on a free decision. In a relationship of dependence, such as an employer-employee relationship, this freedom of decision can be significantly restricted, potentially making consent declarations by employees problematic.

In any case, where a works council exists, the conclusion of an agreement with that works council regarding the employee data processing is typically required.

The general rule is that employee consent is required to collect and process an employee’s Personal Data; however, there are instances when employee consent is not required, e.g., to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. Online/Electronic Consent

In Austria, online or electronic consent is permissible and deemed effective if properly structured and evidenced.

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about the organization's identity, the purposes for collecting Personal Data, the consequences of not providing consent, and the rights of the Data Subject. Under the GDPR, notice requirements will become more exhaustive. The Data Controller will have to additionally inform the Data Subjects regarding the legal basis of the processing, the right to withdraw consent at any time in case the processing is based on consent, the data recipients, international data transfers, retention periods, the right to lodge a complaint with a supervisory authority and the existence of automated decision-making.

7. Processing Rules

An organization that processes Personal Data must: (i) limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; (ii) anonymize the Personal Data whenever possible; (iii) provide the Data Subject with the option to use a pseudonym or remain anonymous whenever possible; and (iv) delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

The GDPR introduces additional data protection principles: Personal Data must be processed lawfully (principle of lawfulness), fairly (principle of fairness) and in a transparent manner (principle of transparency). Moreover Personal Data must be accurate and, where necessary, kept up to date (principle of accuracy) and in a form which permits identification of Data
Subjects for no longer than is necessary for the purposes for which the Personal Data is processed (principle of storage limitation). Finally, Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (principle of integrity and confidentiality).

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; (iv) request the deletion and/or destruction of the Data Subject’s Personal Data; and (v) exercise the writ of habeas data.

The GDPR additionally introduces the right to restriction of processing (Article 18 GDPR), the right to data portability (Article 20 GDPR) as well as the right to object to the processing of Personal Data in certain circumstances.

9. Registration/Notification Requirements

An organization that processes Personal Data is required to make a filing at the Authority under the current DPA 2000. This filing requirement will become void once the GDPR and the DPA 2018 will be applicable.

10. Data Protection Officers

In Austria, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization under the DPA 2000.

The DPA 2018 does not use the opening clause in the GDPR concerning the mandatory appointment of a Data Protection Officer. Therefore the obligation to appoint a Data Protection Officer will be limited to the cases specified in the GDPR: (i) the processing is carried out by a public authority or body; (ii) the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of Data Subjects on a large scale; or (iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and Personal Data relating to criminal convictions and offenses.

11. International Data Transfers

Transfers of Personal Data (including the Transmission or Committing of Data) from Austria to other EEA countries are generally permitted without the need for further approval by the Authority, provided that such transfers would
be legal within Austria. The same applies with respect to transfers to Canada, Switzerland, the Isle of Man, Argentina, Andorra, New Zealand, Uruguay, Faroe Islands, Israel, Jersey, and Guernsey, which are subject to European Commission findings of adequacy (subject to the fulfillment of certain pre-conditions) in relation to their data protection laws.

As of 1 August 2016, transfers to the US are permitted without prior approval by the Authority where the recipient has certified itself under the EU-US Privacy Shield and provided that the transfers would be legal within Austria. Transfers to the US or any other countries outside the EEA that do not provide an adequate level of data protection are legal if based on unmodified or modified versions of the relevant EU Model Clauses, provided always that such transfers would be legal within Austria.

However, the Austrian Data Processing Register has to be notified in any case, unless covered by the above mentioned exceptions (covered by a standard application; contain solely published data or data for the management of public registers and catalogues; contain data solely for which neither the Data Controller, any Processor or any recipient can determine the identity of the Data Subject; contain only Personal Data or family data for private purposes or data for journalistic purposes). Furthermore, any transmissions based on the EU Model Clauses also require the prior approval by the Authority. Notification and filing requirements to the Authority will become void once the GDPR will be applicable. Transfers that have already been approved of by the Authority will continue to be permissible (unless the Authority amends or nullifies them, which it is not likely to do).

Transfers of Personal Data to countries outside the EEA may further take place even without additional measures to ensure an adequate level of data protection at the recipient’s end where:

- the Data Subject has consented to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or to take steps at the Data Subject’s request with a view to entering into a contract with them;
- the transfer is necessary for the performance of a contract between the Data Controller and a third party in the interest of the Data Subject;
- the transfer is necessary for the purpose of establishing, exercising, or defending legal claims before a foreign authority; or
- the Personal Data have been published legitimately in Austria (e.g., available from a public register).

The general rules concerning the legality of processing must always be fulfilled (i.e., the transfer would need to be legal within Austria).
In all other cases, prior authorization by the Authority is required by law.

Under the GDPR, the basis for a transfer of Personal Data even without additional measures at the recipient’s end will stay basically the same. Additionally the transfer will be permissible if:

- the transfer is necessary for important reasons of public interest;
- the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; or
- the transfer is made from a public register, under certain circumstances.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of the occurrence of a data breach, the outsourcing organization may be held liable together with the third-party provider.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Organizations that are involved in a data breach situation are required to comply with mandatory data breach notification requirements, take steps to contain the breach, and comply with data authority orders and court orders. Depending on the nature and scope of the breach, the organization is not required to notify the Authority. However, the organization may have to notify the impacted Data Subjects in case of any systematic and serious illegal use of data if there is a risk of harm for the Data Subject. The organization may be required to gather information about the breach, assess the potential risk of
harm to the Data Subjects, take steps to prevent future similar breaches and assist authorities with any investigation relating to the breach.

An organization that is involved in a data breach situation may be subject to a closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions.

Under GDPR, a data breach notification to the Authority will become obligatory in most cases.

16. Accountability

There is no existing law in Austria that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

Under GDPR, the Controller will have to conduct a privacy impact assessment prior to the processing of Personal Data, if the processing is likely to result in a high risk to the rights and freedoms of natural persons.

17. Whistle-Blower hotline

Whistle-blower hotlines may be established in Austria provided that they are in compliance with local laws

18. E-Discovery

When implementing an e-discovery system, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, give employees the opportunity to opt-out from the spam-filtering solution, and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.
21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject's failure to respond.

The GDPR expressly gives the Data Subject the right to object to the processing of his or her Personal Data for direct marketing purposes.
Azerbaijan

Gunduz Karimov
Baku
Tel: +994 12 4971 801
gunduz.karimov@bakermckenzie.com

Jamil Alizada
Baku
Tel: +994 12 4971 801
jamil.alizada@bakermckenzie.com

Gunduz Karimov
Baku
Tel: +994 12 4971 801
gunduz.karimov@bakermckenzie.com
1. Recent Privacy Developments
There have been no major developments recently.

2. Emerging Privacy Issues and Trends
Not applicable.

3. Law Applicable

4. Key Privacy Concepts

a. Personal Data
The Personal Data Law defines Personal Data as any information which makes it possible to identify a person directly or indirectly. Under the Labor Code, general information on an employee, such as his or her name, home address, and any other information reflected in his or her national identification card, is also considered Personal Data.

Personal Data may be classified as either general or private. Personal information such as a person’s first, second and patronymic name is regarded as general Personal Data.

The Information Acquisition Law restricts the collection of private information on an individual’s political views, religious affiliation, ethnicity, health and similar matters.

b. Data Processing
The Information Law defines data processing as the creation, collection, processing, storage, search and dissemination of information. The Information Law further regulates data processing through the use of information
resources. Resolution 38 establishes rules on data processing applicable to: (i) document storage, systematization and protection; (ii) the creation, storage and updating of document registers; and (iii) the use of documents maintained in a register.

c. Processing by Data Controllers
A Data Controller is a “holder of information” required by law to provide information to the public upon request. Under the Information Acquisition Law, a “holder of information” is defined as including: (i) state and municipal authorities; (ii) public entities (vested with certain social responsibilities); and (iii) legal entities and individuals providing services in the areas of education, medicine and culture. Entities having a dominant position in a particular market are also regarded as “holders of information”.

d. Jurisdiction/Territoriality
The privacy-related laws listed in Section 3 apply to the creation, collection, processing, storage, search and dissemination of information in Azerbaijan.

e. Sensitive Personal Data
The Information Acquisition Law restricts public access to certain categories of Personal Data, including information: (i) on political views, religion, ideology, ethnic and racial origin; (ii) on health and physical and mental disabilities; (iii) collected during criminal investigations prior to publication in open court hearings; (iv) on social welfare program applications; (v) on previous convictions; (vi) on domestic violence; (vii) on collected taxes, excluding tax arrears; (viii) on domestic violence; and (ix) on financial transactions. The Biometric Information Law also restricts public access to biometric information, i.e., information on a person’s intrinsic physical traits such as fingerprints, DNA, face and iris recognition, etc.

The Information Acquisition Law also restricts public access to certain information on family life, including data relating to: (i) sex life; (ii) matrimonial and other family matters; (iii) child adoption; and (iv) notarial acts.

f. Employee Personal Data
Employee-related information (i.e., name, residential address and any other information reflected on a national identification card) is Personal Data. Information on an employee’s salary, title, business address and telephone number, however, is not Personal Data.

5. Consent Requirements
a. General
Article 32.3 of the Constitution requires the subject’s consent for the collection, processing, storage and dissemination of information relating to the subject’s data.
b. Sensitive Data
It is prohibited to release Personal Data relating to the subject without his or her consent.

c. Minors
No consent is required to release information on minors (under 18) to their parents, guardians and other legal representatives.

d. Employee Consent
The Labor Code prohibits employers from releasing information relating to its employees without the employees’ consent.

e. Online/Electronic Consent
While the Information Acquisition Law specifically provides for an electronic release of information, it is silent on the availability of “electronic” consent. As a general matter, consent must be in writing (i.e., signed) to be effective.

6. Information/Notice Requirements
Not applicable.

7. Processing Rules
Resolution 38 establishes the processing rules.

8. Rights of Individuals
An individual is entitled to have access to information unless such information is classified. The Data Subject has also a right to obtain documented personal information without restriction.

The Information Acquisition Law authorizes certain entities and individuals to gain access to Personal Data including: (i) parents, guardians and custodians – with regard to Personal Data relating to the children in their custody; and (ii) guardians – with regard to Personal Data relating to handicapped persons in their custody.

Azerbaijani law provides additional rights, including an individual’s right to: (i) correction of information about himself or herself, if information is inaccurate; and (ii) assistance from Data Controllers in connection with the release of information.

9. Registration/Notification Requirements
A Data Controller must register in its database: (i) information in its possession, including Personal Data; and (ii) requests for release of information. No particular notification requirements are established (other than notifications to Data Controllers from data requesters).
10. Data Protection Officers

The Information Acquisition Law imposes certain obligations on Data Controllers.

11. International Data Transfers

Under the Personal Data Law, any data transfer, including international data transfers, requires the subject’s written consent. International data transfers are prohibited if: (i) they pose a threat to the national security of Azerbaijan; or (ii) the laws of a recipient country do not provide the legal protection of Personal Data afforded to subjects under Azerbaijani law. In the latter case, the international transfer may be permitted upon the express consent of subjects or if the international transfer is required for protection of life and health.

12. Security Requirements

The Information Acquisition Law requires a Data Controller to ensure protection of Personal Data.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

It is neither prohibited nor specifically authorized to outsource data processing to third parties.

14. Enforcement and Sanctions

Violation of legislation on Personal Data is punished by a fine in the amount of AZN 300-500.

Various sanctions, listed in Chapter 32 of the Administrative Code, also apply in relation to violations of the rules on the use, dissemination and protection of information.

15. Data Security Breach

Except for the general right of a person to require adequate protection of collected data, Azerbaijani laws do not set legal requirements in the event of a data security breach.

16. Accountability

Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.
17. Whistle-Blower Hotline
There are no rules/laws in Azerbaijan that govern whistle-blower hotlines.

18. E-Discovery System
There are no rules/laws in Azerbaijan that govern e-discovery.

19. Anti-Spam Filter
As spam filtering (often coupled with deleting emails) involves a detailed analysis of email content, it raises a customer’s privacy concern.

20. Cookies
The use of cookies must comply with Azerbaijani privacy laws.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. The organization may be required to obtain consent for a specific activity as bundled consent may not be considered valid consent.
Belgium

Elisabeth Dehareng
Brussels
Tel: +32 2 639 36 11
elisabeth.dehareng@bakermckenzie.com

Daniel Fesler
Brussels
Tel: +32 2 639 36 11
daniel.fesler@bakermckenzie.com
1. Recent Privacy Developments

**Records of processing activities: recommendation and template published by the Belgian Privacy Commission**

In June 2017, the Belgian Privacy Commission issued a recommendation on the requirement to maintain a record of processing activities, as set forth under Article 30 of the GDPR. It provides guidance on who must maintain such records, the exemptions to the record keeping requirement and the type of information to be included in the records. In August, the Privacy Commission published a template of the record of processing activities (in excel format).

**Recommendation on the appointment of a Data Protection Officer (DPO)**

In May 2017, the Belgian Privacy Commission issued a recommendation regarding the obligation to appoint a DPO under Articles 37 to 39 of the GDPR, focusing on who could carry out the DPO function within the organization in light of possible conflicts of interest.

**Report of the Belgian Privacy Commission on “Big Data”**

In 2017, following a public consultation, the Privacy Commission published a report on big data, including an analysis of the concept of “big data” and the appropriate guarantees that must be in place to allow a legitimate and acceptable use of such data in light of applicable data protection requirements.

This report takes a multidisciplinary and practical approach and provides 33 concrete recommendations to assist Data Controllers in their big data projects.

**Draft recommendation on Data Protection Impact Assessment under the GDPR**

In December 2016, the Belgian Privacy Commission issued a draft recommendation on the requirement for Data Controllers to conduct a data protection impact assessment, as set forth in Article 35 of the GDPR. This draft was submitted to public consultation, which is now closed. The final recommendation is expected in 2018.

**New Act creating the new Belgian Data Protection Authority to replace the Belgian Privacy Commission:**

An Act creating the new Belgian Data Protection Authority was adopted on 3 December 2017. Most of its provisions will enter into force on 25 May 2018. This Act creates and regulates the functioning of the new Belgian Data Protection Authority (replacing the Belgian Privacy Commission). The new Data Protection Authority will have the power to control (via enquiries and
inspections) and sanction (notably by means of administrative fines) compliance with the GDPR and Belgian national provisions supplementing the GDPR. The Data Protection Authority shall supervise the processing of Personal Data on the territory of Belgium, regardless of the national law that applies to the processing concerned.

**General Data Protection Regulation (GDPR): the Privacy Commission has published a plan in 13 steps to help businesses to prepare for the GDPR**

In September 2016, the Privacy Commission published a thematic file and a manual (in the form of a plan in 13 steps) to explain the GDPR and to help Data Controllers and Processors understand the differences between the GDPR and the current Belgian Data Protection Act and to adapt their policies and procedures. The Privacy Commission notably insists on the accountability principle.

**Opt-in v. opt-out requirements for targeted marketing on TV based on users’ television viewing and surfing behavior**

In 2017, the Belgian Privacy Commission reviewed and issued opinions regarding marketing practices of Belgian internet and television providers relating to the sending of targeted marketing based on users’ television viewing habits.

In June 2016, the Brussels Court of Appeal annulled a judgment of the Chairman of the Brussels Court of First Instance in summary proceedings in a case that had been initiated by the Belgian Privacy Commission against a social media website in relation to the use of cookies and social media plug-ins. This follows their 13 May 2015 recommendation which notably concerned plug-ins. In a judgment of 9 November 2015, the Chairman of the Brussels Court of First Instance ordered the said group to cease registering via cookies and social plug-ins websites internet users from Belgium who do not have an account. This judgment was annulled by the Brussels Court of Appeal in June 2016, on the grounds that Belgian courts are not competent for the non-Belgian entities at stake, and that there was a lack of urgency with respect to the Belgian entity. The current judicial procedure is still pending on the merits (before the Dutch Court of First Instance in Brussels).

2. Emerging Privacy Issues and Trends

- **GDPR** – The hot topic in 2017 was the revision of the EU data protection framework, particularly around the preparation for the EU General Data
Protection Regulation that will be directly applicable as of 25 May 2018 and the adoption of implementing national provisions.

The Belgian Privacy Commission is quite active regarding the GDPR and dedicated a new section on its website to the GDPR, including (i) practical guidance in 13 steps for businesses to prepare for the GDPR, (ii) FAQs in relation to certain aspects of the GDPR, (iii) a draft recommendation on data protection impact assessment, including a public consultation which is now closed, (iv) a recommendation on the appointment of a data protection officer, (v) a recommendation on the records of processing activities and a template of record, etc.

- **Reform of the Data Protection Authority** – As mentioned above, another key trend is future enforcement in light of the powers of control and sanction of the newly created Belgian Data Protection Authority (see Act of 3 December 2017 creating the new Belgian Data Protection Authority).

- **Big data** – Nowadays, tons of data are created from emails, social media information, mobile applications, digital videos and photos, use of searches engines, GPS signals, etc. The concept of “big data” offers the possibility to derive value from such data through the use of innovative technology. The Belgian Privacy Commission pays close attention to the risks involved for the privacy of individuals.

- **Consent to targeted marketing based on internet and TV users’ viewing habits** – As mentioned above, the Belgian Privacy Commission has examined the practices of internet and television providers consisting of processing customers’ television viewing and surfing behavior to send them targeted marketing (including offering more relevant information on their products and services and better adapting advertisement on TV) and the way the customers’ consent to such processing is collected (opt-in or opt-out).

3. **Law Applicable**

The applicable law includes the Act of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as modified by the implementing Act of 11 December 1998 and the Act of 29 February 2003, and as supplemented by the Royal Decree of 13 February 2001 (the “DPA”). Data protection rules may also be found in, other legislation, including the Criminal Code, the Act of 11 March 2003 on Certain Legal Aspects of Information Society Services, the Electronic Communications Act of 13 June 2005, the Act of 21 March 2007 on Surveillance Cameras and in collective bargaining agreements.

The Belgian DPA should, however, be repealed as of 25 May 2018, once the GDPR will apply in all EU Member States.
So far, Belgium has not yet adopted a national data protection legislation to supplement the GDPR, except for the new Act of 3 December 2017 (published on 10 January 2018) creating the new Belgian Data Protection Authority in accordance with the GDPR. This Act shall enter into force as of 25 May 2018, except for the provisions on the appointment of the members of the Executive Committee, the Knowledge Center and the Disputes Resolution Body that already entered into force on 10 January 2018.

Besides, a draft bill amending the existing Belgian Act of 21 March 2007 on camera surveillance has been submitted to the Parliament. This draft revises the existing legal framework for the use of surveillance cameras in order to reflect the modifications brought by the GDPR (including with regard to notification of data processing activities to the Data Protection Authority and establishment of a record of processing activities by the controller).

4. Key Privacy Concepts

The privacy concepts below are described on the basis of the current Belgian DPA and their interpretation by the Belgian Privacy Commission. As mentioned above, the Belgian DPA should, however, be repealed and the GDPR will be directly applicable as of 25 May 2018.

a. Personal Data

The DPA applies to any information (“Personal Data”) relating to an identified or identifiable individual (“Data Subject”). An identifiable person is one who can be identified directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data is not necessarily identifying data.

Data will only be considered “anonymous”, and therefore not “Personal Data” in the sense of the DPA, provided that the individual to whom it relates cannot be identified, whether by the Data Controller or by any other person, taking account of all the means reasonably likely to be used either by the controller or by any other person to identify that individual.

b. Data Processing

“Processing” is very broadly defined and will cover any operation or set of operations performed on Personal Data including collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, as well as blocking, erasure, and deletion of Personal Data.

The DPA applies to the processing of Personal Data wholly or partly by automatic means, as well as to manual data processing where the data so processed is recorded in or is intended to form part of a filing system.
c. **Processing by Data Controllers**
The DPA applies to those persons who, alone or jointly with others, determine the purposes for which and the manner in which any Personal Data is or will be processed ("Data Controller").

d. **Jurisdiction/Territoriality**
The current DPA applies to:

- Data processing activities carried out by Data Controllers established in Belgium; and

- Data processing activities of Data Controllers that are not established in the EU but that use equipment based in Belgium to carry out data processing activities (other than merely for transit purpose).

The DPA therefore applies independently of the nationality/residence/location of the Data Subjects whose data is being processed.

Please note that the above will no longer apply as of 25 May 2018 and will be replaced by the material and territorial scope of application of the GDPR.

e. **Sensitive Personal Data**
The current DPA imposes additional requirements for the processing of Sensitive Personal Data, i.e., data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning sex life, as well as health-related data.

Pursuant to Article 6 of the DPA, the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership as well as data concerning sex life is prohibited unless:

a. the Data Subject has given his written consent to the processing, it being understood that such consent can be withdrawn at any time (see Section 5(b) below);

b. the processing is necessary for the purpose of carrying out the specific obligations and rights of the Data Controller in the employment field;

c. the processing is necessary to protect the vital interests of the Data Subject or another person, provided that the Data Subject is physically or legally incapable of giving his consent;

d. the processing relates to Personal Data that has obviously been made public by the Data Subject;

e. the processing is necessary for social security purposes;

f. the processing is necessary for the establishment, exercise or defense of legal claims;
g. the processing is necessary for scientific research and carried out under the terms established by the King in a decree agreed upon in the Council of Ministers after advice of the Commission for the protection of privacy;

h. the processing is carried out in pursuance of the law of 4 July 1962 on public statistics; or

i. the processing is made mandatory by law, decree, or ordinance, or another important reason of public interest, etc.

Pursuant to Article 7 of the DPA, the processing of health-related data is prohibited unless:

a. the Data Subject has given his or her written consent to the processing, it being understood that such consent can be withdrawn at any time;

b. the processing is necessary for the purpose of carrying out the specific obligations and rights of the Data Controller in the employment field;

c. the processing is necessary for social security purposes;

d. the processing is made mandatory by law, decree, or ordinance, or another important reason of public interest;

e. the processing is necessary to protect the vital interests of the Data Subject or of another person, provided that the Data Subject is physically or legally incapable of giving his or her consent;

f. the processing is necessary for the prevention of an actual danger or the suppression of a specific criminal offense.

g. the processing relates to Personal Data that has obviously been made public by the Data Subject; or

h. the processing is necessary for the establishment, exercise or defense of legal claims, etc.

Additionally, pursuant to Article 7, § 4, of the current DPA, health-related data can only be processed under the responsibility of a health care professional, except where the written consent of the Data Subject has been obtained or if the processing is necessary for the prevention of an actual danger or the suppression of a specific criminal offense.

It is worth noting that Article 42, § 2, of the Act of 13 December 2006 containing various health provisions provides that the communication of any Personal Data relating to health is subject to an authorization of principle of the Health Section of the Sector Committee of Social Security; specific exemptions may apply.

Furthermore, the processing of judicial data, including Personal Data relating to litigations that have been submitted to courts as well as administrative
judicial bodies, regarding suspicions, persecutions or convictions in matters of criminal offenses, administrative sanctions or security measures, is also prohibited in principle, unless such processing is performed:

- under the supervision of a public authority or ministerial officer, if processing is necessary for the performance of their tasks;
- by other persons, if processing is necessary for the realization of objectives that have been laid down by or by virtue of a law, decree, or ordinance;
- by natural persons or private or public legal persons, as far as necessary for the management of their own litigations;
- by attorneys at law or other legal advisers, as far as necessary for the protection of the interests of their clients; or
- where the processing is necessary for scientific research and carried out under the conditions established or laid down by royal decree.

Persons authorized to process such Personal Data shall be subject to secrecy obligations.

Under Belgian law, an employer (current or potential) cannot rely on its employees’ written consent to process their Sensitive Personal Data, except where the processing aims to grant them an advantage. The same applies if the Data Subject is in a dependent position with respect to the Data Controller, preventing the Data Subject from giving his or her free consent.

Lastly, additional security measures apply to the processing of Sensitive Personal Data (in addition to the security requirements applying to all data):

a. the categories of persons having access to the Personal Data must be designated by the Data Controller, or, as the case may arise, by the Data Processor, with a detailed description of their function with respect to the processing of Sensitive Personal Data;

b. a list of categories of the designated persons must be put at the Privacy Commission’s disposal by the Data Controller or, as the case may arise, by the Data Processor;

c. the designated persons must be held, by a legal or statutory obligation, or by an equivalent contractual provision, to preserve the confidential character of Sensitive Personal Data;

d. when informing the Data Subject about the processing of his or her data, the Data Controller must mention the act or regulation authorizing the processing;
e. if the processing is only authorized with the Data Subject’s written consent, the Data Controller must inform the latter of the reasons for the processing and provide him or her with a list of the categories of individuals having access to the Personal Data.

Non-Sensitive Personal Data may be processed if at least one of the following preconditions is met:

a. the Data Subject has unambiguously given his or her consent to the processing (although there are some concerns regarding consent given in the employment context – see Section 5(d) below);

b. the processing is necessary for the performance of a contract to which the Data Subject is a party or for the performance of pre-contractual measures taken at the request of the Data Subject;

c. the processing is necessary for compliance with an obligation to which the Data Controller is subject by or by virtue of law (to be understood as Belgian law);

d. the processing is necessary in order to protect the vital interests of the Data Subject;

e. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed;

f. the processing is necessary for the purposes of the legitimate interests of the Data Controller or of the third party to whom the data is disclosed, provided that such interest is not overridden by the Data Subjects’ fundamental rights and freedoms.

It is worth noting that, as of 25 May 2018, once the GDPR will be directly applicable, the processing of certain special categories of data, including Sensitive Personal Data identified above, will likely be subject to specific national provisions. The Belgian national provisions that will supplement the GDPR have not been adopted yet.

f. Employee Personal Data

Employee Personal Data is likely to include Sensitive Personal Data (e.g., trade union membership or health-related information) and non-Sensitive Personal Data. Sensitive Employee Personal Data may only be processed in the circumstances mentioned in Section 4(e) above and, in particular, for the purpose of carrying out the Data Controller’s specific rights and obligations under employment law.

For instance, employers must process data with respect to leaves of absence of their employees in order to allow the due payment of social security indemnities. However, employers are not entitled to record the nature of
illnesses affecting their employees. It must be stressed that, in Belgium, such processing operations are generally performed by the so-called “Secrétariats sociaux”, i.e., external service providers that manage the payrolls of their clients.

Additionally, trade union membership data may only be processed by the employer for the purpose of payment of trade union premiums and/or to register the status of a protected employee.

Lastly, it is worth noting that an employee’s National Registry Number (Social Security Number) may only be processed for the purpose of complying or proceeding with ONSS (National Social Security Office) requests and/or filings, and in no case as a company internal reference for the employee. This number should also not be transferred to third-party Data Controllers outside the EEA.

Non-Sensitive Personal Data may be processed by a Data Controller in the circumstances mentioned in Section 4(e) above and, in particular, for the performance of a contract to which the Data Subject is a party, for the purpose of carrying out the Data Controller’s legal obligations, or where processing is necessary for the purposes of the legitimate interests of the Data Controller not overriding the Data Subject’s fundamental rights and freedoms.

A fallback justification for processing non-Sensitive Personal Data in the employment context may be the Data Subject’s consent. However, employees may not consent to the processing of their Sensitive Personal Data (except where the processing aims to grant advantages to the employee), and there is some concern whether employees may validly consent to the processing of their Personal Data by their employers (see Section 5(d) below).

As of 25 May 2018, once the GDPR will be directly applicable in all EU Member States, the processing of Personal Data in the field of employment law will likely be subject to specific national provisions. The Belgian national provisions that will supplement the GDPR have not been adopted yet.

5. Consent

The consent requirements below are described on the basis of the current Belgian DPA and their interpretation by the Belgian Privacy Commission. They will, however, be modified and replaced under the GDPR, once it is fully applicable (i.e., as of 25 May 2018).

a. General

Consent of the Data Subject is generally a straightforward way to justify the collection, processing and disclosure of Personal Data. Consent given by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.
Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

There is no mandatory requirement that consent be in writing, except for the processing of Sensitive Personal Data. It may be provided orally or in different forms and formats. In addition, the Data Subject also has the right to withdraw consent at any time.

There is no specific language requirement other than resulting from Belgium’s general linguistic legislation, which requires the use of a specific language depending on the geographical location of the employer and the status of the employee. The Data Subject should in any case be informed about the processing of his/her Personal Data (and be invited to give his or her consent, as the case may arise) in an understandable language.

b. Sensitive Data

Belgian law recognizes Sensitive Personal Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Personal Data may only be collected and processed with the express (written) consent of the Data Subject, it may be processed without obtaining consent in certain prescribed circumstances.

c. Minors

The general rule is that minors under the age of 18 are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor, and may even be allowed to obtain information about the minor from third parties without the need of consent from the minor. Further, parents or legal guardians have the right to be informed of the collection of information, to access and rectify the Personal Data and to have recourse to the Privacy Commission or the President of the First Instance Court. Nevertheless, there are certain circumstances where consent given by a minor may be considered valid. In its Opinion 38/2002 relating to the privacy protection of minors on the Internet, the Privacy Commission seems to consider that the legal representative’s consent should not be systematically required when data relating to minors who have not reached the age of discernment (which is between 12 and 14 years old) is processed on the internet.

The GDPR contains specific rules in terms of minor consent that will apply as of 25 May 2018. National deviations are also possible with respect to the age of consent in an online context.
d. Employee Consent
The Article 29 Working Party has produced an opinion on the processing of Personal Data in the employment context which states that it is not appropriate for an employer to try to rely on an employee’s consent as it is unlikely to be freely given.

In Belgium, the processing of Sensitive Personal Data generally cannot be validly authorized by employees, except where the processing aims to grant them advantages.

However, subject to caution, such consent might validly permit the processing of non-Sensitive Personal Data.

However, employee consent is generally not required where the data processing is necessary to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

The GDPR contains specific rules in terms of consent that will apply as of 25 May 2018. National deviations are also possible with respect to consent in the employment context.

e. Online/Electronic Consent
In Belgium, online or electronic consent is permissible and deemed effective if properly structured and evidenced.

However, where the law requires written consent (e.g., regarding sensitive data), specific requirements need to be met.

6. Notice Requirements
Under the current DPA, a Data Controller that collects Personal Data must provide Data Subjects, at the time his or her data is collected or first recorded, with information about the Data Controller’s identity and address; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; whether the provision of Personal Data is mandatory and the consequences of refusal to provide Personal Data; the rights of access, rectification and objections of the Data Subject; where the Personal Data is to be transferred; where the Personal Data is to be stored; and how to access and/or correct the Data Subject’s Personal Data.

Information requirements will be strengthened under the GDPR.

7. Processing Rules
Under the current DPA, a Data Controller that processes Personal Data must: limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected;
anonymize the Personal Data whenever possible; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

In addition, when entrusting the processing of Personal Data to a third-party processor acting on its behalf (a “Data Processor”), the Data Controller must choose a Data Processor providing sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out.

In addition, the processing must be carried out under a contract that (i) is in writing, (ii) requires the Data Processor to act – and causes any person acting under its authority and having access to Personal Data to act – only on the instructions of the Data Controller, (iii) requires the Data Processor to comply with security obligations equivalent to those imposed on the Data Controller, and (iv) lays out the liability of the Data Processor towards the Data Controller.

More specific processing rules are set forth under the GDPR and will apply as of 25 May 2018.

8. Rights of Individuals

Under the current DPA, Data Subjects have the general right to: be informed by a Data Controller of the Personal Data the Data Controller holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; object to the processing of Data Subject’s Personal Data for direct marketing purposes at any time and free of charge; and request the deletion and/or destruction of the Data Subject’s Personal Data for legitimate reasons.

New Data Subject rights are set forth under the GDPR and will apply as of 25 May 2018.

9. Registration/Notification Requirements

Under the current DPA, any Data Controller established in Belgium or, if established outside the European Economic Area, using means located on the Belgian territory for the purpose of its data processing (other than for mere transit purposes) is required to file a notification with the Belgian Privacy Commission before any wholly or partly automated data processing starts. Exemptions to the requirement for notification apply for the processing of data dealing merely with the management of employees’ wages and/or payroll, as well as for mere clientele management, subject to certain conditions.

This notification obligation will no longer exist as from 25 May 2018 under the GDPR.
10. Data Protection Officers

In Belgium, under the current DPA, there is no requirement to appoint or designate a data privacy officer accountable for the privacy practices of the organization.

This will change under the GDPR as DPO will have to be appointed in certain circumstances.

11. International Data Transfers

Under the current DPA, except for the communication of health-related data (see Section 4(e)), transfers of Personal Data from Belgium to EEA Member States are permitted without the need for further approval. The same applies to transfers to countries that have been recognized by the European Commission as having adequate data protection laws. So far, Andorra, Argentina, Australia (for PNR data), Canada (with regard to transfers made to recipients subject to the Canadian Personal Information Protection and Electronic Documents Act), Switzerland, Faeroe Islands, Guernsey, State of Israel, Jersey, Isle of Man, New Zealand and Uruguay have been recognized as providing adequate level of data protection. On 6 October 2015, the Court of Justice of the European Union invalidated the Safe Harbor Decision. Therefore, the Safe Harbor scheme no longer serves as a legal basis to transfer Personal Data from the EU to the United States. However, on 12 July 2016, the EU Commission adopted the EU-US Privacy Shield which allows adhering companies to transfer Personal Data from the EU to the US.

Subject to the specific exceptional authorizations above, Personal Data may not be transferred to countries outside the EEA, unless the destination country provides adequate protection for the Personal Data. Exceptions are as follows:

- the Data Subject has given his or her unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or for the implementation of pre-contractual measures taken in response to the request of the Data Subject;
- the transfer is necessary for the performance of a contract concluded or to be concluded in the interest of the Data Subject between the Data Controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;
- the transfer is made from a public register which, by law, is intended to provide information to the public and which is open to consultation either
by the public in general or by any person who can demonstrate a legitimate interest; or

- a data transfer agreement is in place. Following a Protocol entered into between the Privacy Commission and the Belgian Department of Justice in June 2013, as amended in 2014, all data transfer agreements intended to cover transfers of data out of the European Economic Area to countries not providing an adequate level of data protection must be submitted to the Belgian Privacy Commission. Data transfers agreements not conforming to EU Commission's Standard Contractual Clauses must be approved by the King (i.e., the Federal Government).

The GDPR will slightly amend the above rules on data transfers as of 25 May 2018.

12. Security Requirements
Under the current DPA, data Controllers and Data Processors are required to take steps to: ensure that Personal Data in their possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

The GDPR contains further requirements in terms of security of Personal Data that will apply as of 25 May 2018.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Under the current DPA, Data Controllers that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. In case of an occurrence of data breach, the outsourcing organization may be held liable together with the third-party provider.

14. Enforcement and Sanctions
Under the current DPA, failure to comply with data privacy laws can result in complaints; data authority investigations/audits; seizure of equipment or data; civil actions; criminal proceedings; and/or private rights of action.

The court may also order the seizure of any privacy infringing equipment or data, the rectification or destruction of Personal Data, and the publication of its judgment in whole or by excerpt in one or more newspapers. The court may also prohibit the Data Controller from processing any Personal Data for up to two years.
As indicated above, a new Belgian Data Protection Authority has been created by the Act of 3 December 2017 and will have control and enforcement powers as of 25 May 2018.

15. Data Security Breach

There is currently no express general legal requirement under Belgian law for a Data Controller or a Data Processor to notify Data Subjects or government authorities about the hacking of Personal Data or, more generally, to notify them about a security failure allowing unauthorized access to such data.

However, the Act of 10 July 2012 amending the 2005 Electronic Communications Act implemented into Belgian law a limited notification obligation in case of a security breach of an electronic communications service accessible to the public relating to Personal Data. In case of a security breach of an electronic communications service accessible to the public relating to Persona Data, the undertaking providing the services must notify without delay the Belgian Institute for Post and Telecommunications (BIPT) about the data breach. Where such breach may negatively affect Personal Data or a subscriber or an individual’s privacy, the undertaking must also inform without delay the subscriber or individual at stake about the breach.

The notification to the subscriber or individual is not necessary if the undertaking has satisfactorily evidenced to the BIPT that it put all appropriate technological measures in place and that these were applied to data concerned by such breach. Such technological measures render data incomprehensible for any person not authorized to access them. Without prejudice to the foregoing, the BIPT may require that the undertaking inform the concerned subscribers or individuals.

The notification to be made to the subscriber or individual shall describe, at minimum, the nature of the Personal Data breach and contact points where further information may be obtained, and recommend measures to be taken to reduce potential negative consequences. In addition, the notification to the BIPT must describe the consequences of the data breach, the appropriate measures proposed or implemented to remedy the breach.

Additionally, the Belgian Act of 11 March 2003 on certain legal aspects of the information society, makes it an obligation for transport, caching and hosting service providers to report to the public prosecutor alleged illegal activities on their systems of which they become aware. This might then apply to the hacking of Personal Data or to the unauthorized access to data they transport, cache or host.

More generally, informing the Data Subjects about a potential data security breach arguably falls within the scope of the Data Controller’s general loyalty obligation set forth by Article 4 of the DPA, combined with the obligation to
inform Data Subjects about the “recipient(s)” of their data (Article 9 of the DPA).

In a Recommendation nr. 1/2013, dated 21 January 2013 on information security and, in particular, working with computer files, the Belgian Privacy Commission even considers that companies must implement procedures for reporting data security incidents. In the case of a public incident (it being noted that a public incident is not defined by the Privacy Commission), the Privacy Commission considers that it should be informed of the cause(s) and impact of the incident with 48 hours and that awareness campaigns to inform the public should be initiated within 24 to 48 hours following notification to the Commission.

In any case, in accordance with the Belgian civil law principles of good faith and fairness in contractual relationships between the parties as well as with the Belgian law on torts, it is advisable for a Data Controller to inform Data Subjects about a potential data security breach so that the latter can take appropriate measures, if any, to mitigate their risks or prejudice.

Any Data Controller that is involved in a data breach situation may be subject to the sanctions outlined under Section 14 above.

Violations of the limited security breach notification requirement under the 2005 Electronic Communications Act are also sanctioned by fines from EUR 400 to EUR 400,000.

As of 25 May 2018, mandatory notification requirements will apply to all controllers in case of Personal Data breaches. Data processors will have to notify Data Controllers about Personal Data breaches.

16. Accountability

Under the current DPA and subject to regulatory guidance, organizations in Belgium may be required to conduct privacy impact assessments (DPIA) prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

DPIAs will become mandatory in certain circumstances under the GDPR.

17. Whistle-Blower Hotline

Under the current DPA, whistle-blower hotlines may be established in Belgium provided they are in compliance with local laws and with requirements of registering and filing with the Belgian Privacy Commission. (cf. the Belgian Privacy Commission’s recommendation of 2006 regarding the compatibility of whistleblowing hotlines with the Belgian DPA).
18. E-Discovery

When implementing an e-discovery system, an organization must comply with the general requirements of the current DPA, as well as with other legal requirements applicable to the review of employees’ or Data Subject’s electronic communication data, including, the Criminal Code, the Electronic Communications Act of 13 June 2005, and the Collective Bargaining Agreement n° 81 on the monitoring of electronic online communication data. The organization may be required to obtain the consent of employees. In addition, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information in accordance with the above-mentioned legal texts.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization will have to comply with the general requirements of the current DPA.

Besides, to the extent that a spam-filtering solution consists of intercepting emails, it must comply with the Electronic Communications Act of 13 June 2005 and the Criminal Code. Article 125, § 1, 6°, of the Electronic Communications Act provides that Article 124 of the same and Articles 259bis and 314bis of the Criminal Code (which prohibit to intercept data transferred by way of telecommunications without the consent of all persons interested, directly or indirectly, in such communications) do not apply to acts carried out for the sole purpose of providing spam-filtering services to the end-user, provided that the end-user’s prior authorization is obtained to that effect.

20. Cookies

There are specific laws/rules that currently regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used, except in limited exemptions. The Belgian Privacy Commission issued guidance on the use of cookies and similar technologies in February 2015.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, depending on the communication means to be used. Consent can generally not be inferred from a Data Subject’s failure to respond. An organization may be required to obtain consent for a specific activity. The Belgian Privacy Commission issued guidance on the use of Personal Data for direct marketing purposes in 2013.
Brazil

Flavia Rebello
Sao Paulo
Tel: +55 11 3048 6851
flavia.rebello@trenchrossi.com

Gabriela Paiva Morette
Sao Paulo
Tel: +55 11 3048 6785
gabriela.paiva-morette@trenchrossi.com
1. Recent Privacy Developments

In January 2015, the Federal Government, through the Ministry of Justice, submitted the first draft of a bill of law that specifically addresses data protection in Brazil for public consultation. On 13 May 2016, the draft was sent to Congress under No. 5,276/2016 (the “Bill of Law”). The Bill of Law aims to heavily regulate the processing and protection of Personal Data in Brazil in order to protect Data Subjects’ fundamental rights to freedom, intimacy and privacy, and intends to create a set of obligations and responsibilities applicable to all public and private entities and individuals who collect and use Personal Data in any way, regardless of where they are located or where the data is to be stored.

Among other provisions, the Bill of Law: (i) creates a legal definition for Personal Data and Sensitive Personal Data; (ii) stresses the necessity to obtain express, informed, free, specific and prior consent from Data Subjects when processing their Personal Data; (iii) determines the rights of Data Subjects in relation to data processing already consented for; (iv) establishes joint responsibility among all entities involved in the communication and interconnection of such data; (v) determines rules for international transfers of Personal Data; (vi) requires the appointment of a person responsible for privacy in each entity; and (vii) imposes penalties and fines in case of non-compliance.

The Bill of Law suggests the creation of a specific governmental agency (data protection authority) to regulate and ensure compliance with the law, create guidelines, publish reports, issue further regulations on the matter, and impose sanctions on data privacy infringers.

The Bill of Law will be examined together with another bill of law on data protection, bill of law 4,060/2012, which is not as thorough. As the Bill of Law is in a relatively early stage of the law-making process, it may still be subject to significant changes. Likewise, it is difficult to determine when it may be approved.

2. Emerging Privacy Issues and Trends

As well as the consultations on the Bill of Law, as discussed in Section 1, consumer authorities in Brazil have been consistently enforcing privacy rules related to consumer protection. Enforcement actions range from requests for explanations from entities to administrative procedures that could lead to the imposition of penalties against entities deemed to be violating the privacy rules under the Consumer Defense Code.

3. Law Applicable

The legal protection afforded to Personal Data arises from general rules and principles disseminated in several different pieces of legislation.
Brazilian Federal Constitution (Article 5, X): contains general provisions on privacy. According to the Brazilian Federal Constitution, the individual’s rights to intimacy, privacy, honor and image are fundamental rights and any violation thereof entitles the Data Subject to indemnification for both moral and material damages. Moreover, the secrecy of correspondence, telegraphic, data and telephone communications is also a Constitutional guarantee.

Brazilian Civil Code (Law No. 10,406/02, Article 21): among other general provisions, it considers the right to privacy as a personality right, which cannot be waived or assigned as a matter of public policy.

Brazilian Consumer Protection Code (“CDC”) (Law No. 8,078/90): contains certain rules regarding the collection, storage and use of consumer databases. The CDC regulates the creation of databases containing consumers’ personal information. Under the CDC, a “consumer” is any individual or legal entity that acquires goods or services as an end-user. By this definition of consumer, the CDC governs not only retail sales to consumers, but also sales of products and services to legal entities that will be treated as consumers when and if they are end-users of products and services (on a case-by-case basis).

Internet Legal Framework (Law No. 12,965/14): establishes general principles, warranties, rights and duties that govern the use of the internet in Brazil and regulates the protection of privacy and data online. It contains several provisions regarding internet users’ rights to the protection of logs, Personal Data and private communications, as discussed in further detail below. Although the Internet Legal Framework is recent and, in theory, only applies to data collected over the internet, it may be used by courts as a general guideline in the absence of a specific data privacy law.

On 11 May 2016, the Brazilian Federal Government published Decree No. 8,711/2016, regulating some of the provisions of the Internet Legal Framework. The decree mainly addresses network neutrality and the protection of Personal Data and private communications. It also provides a minimum set of security standards, applicable to all internet connection and application providers, for the storage and processing of Personal Data and private communications, including strict control over data access by defining the responsibilities of the persons who may have access to it; and authentication mechanisms for accessing records.

Brazilian Criminal Code (as amended by Law No. 12,737/12): has general provisions addressing crimes relating to the inviolability of correspondence and the invasion of information technology devices. Accordingly, the Law provides that it is a criminal offense to invade third parties’ information devices, whether or not such devices are connected to the internet, by means that aim to obtain, alter or destroy data or information without the express or implied authorization from the device owner or to install vulnerabilities to
obtain illicit advantages. The crime is punishable by detention of three months to one year, plus a fine. This penalty also applies to anyone who makes, offers, distributes, sells or discloses a computer device or software aimed at enabling the conducts described above. Also, in the event that the invasion results in obtaining content from private electronic communications, industrial or trade secrets, confidential information or the unauthorized remote control of the device, the penalty is increased to imprisonment of six months to two years, plus a penalty. This latter penalty is also increased in the event that the data or information obtained is disclosed, traded or transmitted to third parties.

**Interception of Telephone Communication Law** (Federal Law 9,296/96): determines that such procedure may only be authorized by a judge in the context of a criminal investigation. The same rules apply to wiretapping of information technology devices.

**Complementary Law No. 105/01**: establishes rules regarding bank secrecy with which financial institutions must comply. Please note that other sector-specific rules may also apply.

**Brazilian Information Access Law** (Law No. 12,527/11, article 4, IV): regulates access to information held by public entities and agencies in Brazil, and also gives a legal definition of what is considered “personal information”, as discussed in Section 4.

4. **Key Privacy Concepts**

a. **Personal Data**

The Constitutional protection of privacy and the provisions of the Civil Code are very broad as they refer to the protection of the individual’s privacy and intimacy. The CDC refers to any information included in registrations or forms and any data regarding the acquisition of products or services. Decree No. 8,711/2016, which regulates the Internet Legal Framework, provides a definition of Personal Data which, in theory, is limited to the purposes of such law. The Decree defines Personal Data as any data related to an identified or identifiable individual, including identification numbers, location data or electronic identifiers when these are related to a person.

In addition to the above, the Brazilian Information Access Law defines personal information as any information regarding an identified or identifiable individual (i.e., subject to be identified). This definition may be used as reference for the purposes of data protection laws and is generally adopted in courts and by scholars when addressing this matter.

b. **Data Processing**

The concept of data processing should be understood in a broad way, including any form of use, collection, processing, disclosure, transfer,
organizing, amending, recording, handling and storage of data, whether on a manual or automated basis.

As with the concept of Personal Data, Decree No. 8,711/2016, which regulates the Internet Legal Framework, provides a definition of Personal Data handling (a concept comparable to data processing) which, in theory, is limited to the purposes of such law. The Decree defines Personal Data handling as every operation carried out with Personal Data, such as the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, assessment or control, modification, communication, transfer, dissemination or extraction of information.

c. Processing by Data Controllers
Brazilian laws still do not contain specific definitions of “Data Controllers”.

d. Jurisdiction/Territoriality
The Brazilian Federal Constitution, Civil Code, and CDC are considered public order rules and apply to the use, collection, processing, disclosure, transfer, organizing, amending, recording, handling and storage of data relating to Data Subjects residing in Brazil.

In addition to the aforementioned, the Internet Legal Framework sets forth the mandatory application of Brazilian laws for the collection, storage and processing of Personal Data or communications if: (a) at least one of such actions takes place in Brazil; or (b) at least one of the endpoints is located in Brazil. This rule shall equally apply to foreign companies: (i) to the extent there is a Brazilian entity of the corporate group in Brazil; or (ii) their services are offered to the Brazilian public. The main goal of such provisions is to prevent Brazilian entities of multinational groups from arguing that data is stored in servers abroad, subject to foreign laws and, accordingly, that Brazilian laws should not apply.

e. Sensitive Personal Data
There is no specific definition of “Sensitive Personal Data” under Brazilian laws. This definition is also expected to be introduced with the approval of the Bill of Law regarding the protection of Personal Data, as mentioned in Section 1 above.

f. Employee Personal Data
There is no specific definition of “Employee Personal Data”. Consequently, Employee Personal Data is generally treated as other Personal Data, but with some particularities that are typical of an employment relationship (please refer to Item 5(d) below).
5. Consent

a. General
Consent of the Data Subject is required prior to the collection, use, processing, transfer and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances. The consent should include: (a) clear and complete information on the purposes for which the company intends to collect information; (b) to whom data may be disclosed; (c) where data will be stored (indicating if cross-border transfers are necessary/envisaged); and (d) what means are used to protect the data.

When a Data Subject gives consent, such consent only covers the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

The Data Subject also has the right to withdraw consent at any time in given circumstances.

b. Sensitive Data
There are no specific rules in Brazil defining or regulating Sensitive Personal Data. It is important to note that the more sensitive the data is, the greater the risks of claims for damages regarding its improper collection, use or disclosure. Therefore, to the extent feasible, any use, such as the collection and processing of Sensitive Personal Data (e.g., health or financial information), without the previous and specific consent from the Data Subject should be avoided.

c. Minors
According to the Brazilian Civil Code, only individuals over the age of 18 are capable of binding themselves personally. Minors under 16 are considered absolutely incapable, while those between 16 and 18 are considered relatively incapable (i.e., they can bind themselves with the assistance of their parents or guardians). As it is advisable under the Brazilian Federal Constitution and Brazilian Civil Code to secure the prior consent of the Data Subject for the collection of Personal Data in Brazil, parental consent is likewise advisable for those under 18 years old.

It should be noted, however, that relatively incapable minors (between 16 and 18) will not be able to claim the invalidity of a contract (or the consent to collect, process and/or use Personal Data) if they have falsely declared themselves to be above 18.

d. Employee Consent
There are no specific rules addressing this matter. Consequently, Personal Data relating to an employee is generally treated in the same way as other
Personal Data. It should be noted, however, that the general interpretation of Brazilian laws is that, with respect to Employee Personal Data, Constitutional privacy rights should be interpreted in a more flexible manner in view of the duties imposed by the Brazilian Labor Code to employers to manage and control their employees’ activities during working hours, as well as by the Brazilian Civil Code, which establishes that the employer may also be liable for the implications arising from actions taken by its employees during working hours. In fact, based on those grounds, Brazilian Courts have adopted the understanding that the employer has the right to monitor and review the use of companies’ electronic resources (including email, internet and corporate computers) made available to employees, regardless of previous notice, as long as the employee is advised of such possibility and has, therefore, no privacy expectations when using these work tools.

e. **Online/Electronic Consent**

There is no provision that specifically addresses online/electronic consent requirements. However, because the Internet Legal Framework applies to data collected over the internet and requires the Data Subject’s prior express consent, it is implied that online/electronic consent is permitted. Since the Data Subject’s consent shall be express, an opt-in system (e.g., a check-box or an “I agree” button) is usually understood as the appropriate means for such purpose.

Electronic consent mechanisms are generally enforceable in Brazil and considered sufficient to evidence the Data Subject’s agreement with the terms of a consent form to the extent that the Data Controller is able to prove that the systems and processes used to secure the consent are robust and reliable for the purposes of establishing the authenticity and integrity of the consent.

It is worth noting that under the Internet Legal Framework, consent language shall stand out from other provisions of the agreement, such as the terms of use. The law does not establish a clear definition of how such language should be different, but such obligation is commonly interpreted as writing that stands out from other provisions, by using bold or capital letters, or a different font size, for instance. Furthermore, consumer protection rules further provide that the terms of the agreement must be readable (with a minimum font size of 12 pt.) and written in easily comprehensible Portuguese.

6. **Information/Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) its privacy practices (which must be given in a clear and transparent way); (v) third parties to which the organization will disclose the Personal Data; (vi) the consequences of not providing consent; (vii) the rights of the Data Subject; (viii) how the Personal Data is to be retained; (ix) where the Personal Data is stored; (x) the period for which Personal Data will be retained; and (xi) the identity and contact information of the Data Protection Officer. Additionally, the organization must provide information about the rights of the Data Subject, including the right to access, rectify, update, erase, and restrict the processing of Personal Data, as well as the right to object to automated decision-making and profiling.

Data controllers must also inform the Data Subject of the existence, purposes, and legal bases of the processing, as well as the right to object to the processing and the legal basis for the processing. Furthermore, the Data Subject must be informed of the right to lodge a complaint with the relevant data protection authority and of the existence of a procedure for resolving disputes through binding arbitration.

Data controllers are also required to inform the Data Subject of the right to withdraw consent at any time, without affecting the lawfulness of the processing based on the consent prior to its withdrawal. In cases where the Data Subject withdraws consent, the Data Controller must stop the processing, except where it is necessary for compliance with a legal or public interest obligation.

The above information must be provided in a clear and transparent manner, ensuring that the Data Subject is fully informed of the processing of their Personal Data. Additionally, organizations must obtain the Data Subject’s express consent before processing sensitive Personal Data, such as race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, and data concerning a natural person’s sex life.

Organizations must also implement appropriate technical and organizational measures to ensure the security of the Personal Data they process, including the protection of the Personal Data against unauthorized or unlawful processing and against accidental loss or destruction.

Data controllers must implement appropriate security measures to ensure that the Personal Data is not transferred to a third country or international organization without the Data Subject’s consent, unless the transfer is necessary for the performance of a contract or the provision of a service, or is based on a legal obligation, or is in the public interest.

Organizations must also provide information about the right to lodge a complaint with the relevant data protection authority, the existence of a procedure for resolving disputes through binding arbitration, and the existence of a procedure for resolving disputes through binding arbitration.

In cases where the Data Subject withdraws consent, the Data Controller must stop the processing, except where it is necessary for compliance with a legal or public interest obligation.

The above information must be provided in a clear and transparent manner, ensuring that the Data Subject is fully informed of the processing of their Personal Data. Additionally, organizations must obtain the Data Subject’s express consent before processing sensitive Personal Data, such as race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, and data concerning a natural person’s sex life.
to be transferred; (x) where the Personal Data is to be stored; (xi) how to access and/or correct the Data Subject’s Personal Data; and (xii) the duration of the proposed processing.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected and consent was provided; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations have been met.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; (iv) request the deletion and/or destruction of the Data Subject’s Personal Data; and (v) exercise the writ of habeas data, a constitutional remedy that grants individuals access to any information about his or her person.

9. Registration/Notification Requirements

There are no requirements for organizations that collect and process Personal Data to register, file or notify a local data authority.

10. Data Protection Officers

There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

The Internet Legal Framework determines that Personal Data may only be transferred to third parties (including abroad) upon the free, express and informed consent of the Data Subject.

12. Security Requirements

Organizations are required to take steps to: (i) ensure that Personal Data in its possession and control are protected from unauthorized access and use; (ii) implement appropriate physical, technical and organization security safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.
According to the Internet Legal Framework, Data Subjects shall be informed in a clear manner about the security measures and proceedings employed by an organization, which should meet at least the standards determined by the applicable regulation enacted on 11 May 2016.

As mentioned above, Decree No. 8,711/2016 provides a minimum set of security standards applicable to all internet connection and application providers, for the storage and processing of Personal Data and private communications. These requirements include, for instance: (i) authentication mechanisms for accessing records, such as double authentication mechanisms to ensure the identification of the person responsible for data processing; (ii) the creation of detailed inventories of any access to connection and access logs, including the time, duration and identity of the employee or person designated by the company who is responsible for the access, as well as the file accessed; and (iii) the use of log management solutions that ensure the inviolability of data, such as encryption or equivalent protection measures.

Relevant authorities may promote studies and advise on further proceedings, rules and technical and operational standards for compliance with the security requirements set forth in the Decree, taking into account the specificities and size of the company.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector-specific requirements. Organizations shall be liable together with third-party providers in case of breach by the latter.

The Internet Legal Framework provides that Personal Data may only be transferred to third parties (including abroad) upon the free, express and informed consent of the Data Subject.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, administrative fines, penalties, sanctions, civil actions, and/or criminal proceedings.

Specifically in relation to the Internet Legal Framework, failure to comply with any of its rules regarding protection of Personal Data and private communications may result in: (i) warnings; (ii) fines in the amount of up to 10% of the economic group’s gross revenues in Brazil in the last fiscal year; (iii) temporary suspension of data collection activities in Brazil; and/or (iv) prohibition of data collection activities in Brazil. Furthermore, the law expressly determines that the Brazilian entity of a group shall be jointly liable with the
foreign entity for any fines imposed on the foreign entity for failure to comply with these data protection requirements.

15. Data Security Breach

There are no specific rules addressing data security breaches. However, as Data Controllers are generally liable for any data security breach, it is highly advisable to inform the affected Data Subjects and the relevant bodies as soon as the Data Controller becomes aware of a data security breach.

This is especially important in situations where an early notice can be helpful to mitigate possible damages to the Data Subjects (e.g., by allowing the Data Subjects to change passwords or take other precautionary measures to avoid damages). Accordingly, the Data Controllers may also be able to reduce their liability for damages that can be mitigated by means of an early notification of the security breach.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions. However, neither the Internet Legal Framework nor any other Brazilian law regulates the applicable procedure for such cases.

In case of a breach of consumer data, depending on the specifics of the case, it might be advisable to notify the Federal and State consumer authorities.

16. Accountability

Organizations are not required to conduct privacy impact assessments prior to implementing new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Brazil as long as they are in compliance with local laws.

18. E-Discovery

In Brazil, there are no specific rules regarding the discovery of electronically stored information, therefore, the general rules under the Brazilian Civil Procedure Code shall apply.

Moreover, if an organization obtains prior written consent from its employees for the collection of Personal Data in connection with the implementation of an e-discovery system, then no specific issues should arise. On the other hand, if no consent is obtained, specific privacy issues may develop depending on the specific circumstances of the case and the type of data to be collected, processed and/or disclosed.
19. Anti-Spam Filtering

In theory, no privacy issue arises from the introduction of a spam-filtering solution in an organization. However, in case there is a possibility of the organization gaining access to private emails received by an employee due to the spam-filtering solution, the employee should be previously informed of such possibility so that he or she would have no privacy expectations related to the use of the corporate email account.

20. Cookies

There are no specific laws/rules in Brazil that regulate the use and deployment of cookies.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject's failure to respond.

- **Do-Not-Call Registry** – The State of São Paulo Decree No. 53,921, of 30 December 2008, created the Telemarketing Enrollment List to Blocked Calls (“Register”), regulating State Law No. 13,226 of 7 December 2008. This legislation provides users of fixed and mobile telephony with area code numbers from the State of São Paulo. The Consumer Defense and Protection Foundation is responsible for maintaining and implementing the Register, which is available through the internet or in local service centers of the State of São Paulo. Thirty days after consumers are listed in the Register, telemarketing companies will no longer be allowed to call the numbers included, unless the consumer grants prior permission in writing and with an express expiration date.

Companies that fail to comply with the rules of State Decree No. 53,921 will be subject to administrative penalties of the CDC. Philanthropic entities that use telemarketing to raise funds are exempted from the effects of the Decree. Moreover, many States in Brazil have adopted similar laws, including Alagoas (Law No. 7,127/09), Amazonas (Law No. 3,633/11), Ceará (Law No. 15,111/12), Espírito Santo (Law No. 9,176/09), the Federal District (Law No. 4,171/08), Goiás (Law No. 17,424/11), Maranhão (Law No. 9,053/09), Mato Grosso do Sul (Law No. 3,641/09), Paraíba (Law No. 8,841/09), Paraná (Law No. 16,135/09), Pernambuco (Law No. 13,796/09), Rio Grande do Sul (Law No. 13,249/09), and Santa Catarina (Law No. 15,329/10).

- **Marketing Emails** – A Code of Self-Regulation (“Code”) aimed at the responsible, ethical and correct use of marketing emails, and which serves as guidance for the use of marketing emails, has been published by a Council formed by representatives of 14 civil society organizations.
Some of these associations are the Brazilian Direct Marketing Association, the Brazilian Internet Steering Committee, the Brazilian Internet Providers Association, and the Brazilian Consumer Defense Association.

While the Code is not formal law, it provides important guidelines on how marketing emails can be sent without breaching Brazilian privacy law. In addition to other provisions, the Code requires the parties to provide a “Privacy and Data Use Policy” on their respective websites, under penalty of, among others, recommending blockage of the sender’s domain name. The Code adopted an “opt-in” system according to which non-solicited messages are considered to be non-ethical. The only exception to this is when the parties have a long-standing commercial relationship which implies the concept of the so-called “soft-opt-in”. The Code also contains other requirements that must be observed, including the identification of the sender and the nature of the email in the subject field. In addition, the Code provides that the users’ option to unsubscribe must be complied with within two days when directly requested by the user through an unsubscribe link, or within five days when requested by other means. Furthermore, the company responsible for sending marketing emails must use its own domain names. If any of the Code’s provisions are violated, sanctions shall be imposed by an Ethics Committee formed by the Self-Regulation Code Council.
Canada

Theodore Ling
Toronto
Tel: +416 865 6954
theodore.ling@bakermckenzie.com

Arlan Gates
Toronto
Tel: +416 865 6978
arlan.gates@bakermckenzie.com

Dean Dolan
Toronto
Tel: +416 865 3856
dean.dolan@bakermckenzie.com

Lisa Douglas
Toronto
Tel: +416 865 6972
lisa.douglas@bakermckenzie.com

Randeep Nijjar
Toronto
Tel: +416 865 6952
randeep.nijjar@bakermckenzie.com
1. Recent Privacy Developments

*Mandatory Breach Notification Obligations*

In June 2015, amendments to Canada’s federal privacy legislation, the Personal Information Protection and Electronic Documents Act (“PIPEDA”), were passed, including mandatory breach notification obligations. While this amendment has still not been declared in force, in September 2017, the proposed data breach notification regulations were released for public comment. As of the date of publication, the government has neither commented on the public consultation process nor released revised draft regulations.

*Canada’s Anti-Spam Law*

One of the most contentious provisions of Canada’s Anti-Spam Law (“CASL”) was a private right of action for non-compliance which would have allowed private lawsuits (including class actions) to be filed against individuals and organizations for alleged violations of the statute. It was to have come into force on 1 July 2017. However, in a surprise move in June 2017, this provision of CASL was repealed. Since that time, the government has given no indication whether the repeal will be permanent or whether it will seek to reintroduce the provision at some time in the future.

*Public Consultation on Consent*

In May 2016, the Office of the Privacy Commissioner of Canada launched a public consultation on the issue of consent under PIPEDA, and, in September 2017, the Commissioner published its Report on Consent together with draft guidance documents. The guidance addresses the Commissioner’s views on obtaining consent in an online environment, and also identifies areas where the Commissioner believes that it is not appropriate to collect, use or disclose personal information even where consent is obtained. The Commissioner sought public feedback on the guidance, and it is anticipated that it will be finalized and released in early 2018.

*Significant Canadian Data Breaches*

In May 2017, Bell Canada, the country’s largest telecom company, issued an apology to customers after it said nearly 1.9 million customer email addresses and 1,700 names and phone numbers were illegally accessed. Ominously, an anonymous note posted online threatened that “more will leak” if Bell did not cooperate with the (unidentified) individuals responsible for the breach. Bell reported the breach to the RCMP cyber-crime unit and was working closely with the Privacy Commissioner’s Office.

In January 2018, Bell suffered another data breach which compromised customer names and email addresses. Bell stressed that no credit card, banking or other information was accessed and that the breach affected fewer
than 100,000 customers. As with the first breach, Bell was working with the RCMP and the Privacy Commissioner’s Office.

Equifax Canada was impacted by the enormous data breach of its American parent company in which the personal information of 146 million consumers was compromised. The hack was reported in September of 2017 and affected 19,000 Canadians.

2. Emerging Privacy Issues and Trends

The Privacy Commissioner of Canada continues its focus on its Strategic Privacy Priorities as follows:

- **Economics of Personal Information**
  This relates to the exchange of Personal Information for services such as applications and access to free offerings, and related issues of transparency, fair information practices and lack of regulation.

- **Government Services and Surveillance**
  This relates to the privacy risks and benefits of the Government of Canada’s consideration of adopting new technologies and increasing information sharing between departments, the government and jurisdictions.

- **Protecting Canadians in a Borderless World**
  This relates to privacy issues around cross-border transfers of data and the Office of the Privacy Commissioner’s increasing coordination with international privacy regulators in conducting investigations.

- **Reputation and Privacy**
  This relates to questions around profiling individuals and how to suppress and refute negative, outdated or inaccurate information about oneself that has been shared publicly.

- **The Body as Information**
  This relates to the security and privacy issues accompanying the prevalence of sensors, wearables and other technologies used to extract information from the body.

- **Strengthening Accountability and Privacy Safeguards**
  This reflects an increased focus on ensuring that the government and private organizations remain accountable for their privacy practices and secure the Personal Information under their control/custody.
3. Law Applicable

An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23 (“CASL”).

Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (“PIPEDA”).


Organizations in the Province of British Columbia Exemption Order, SOR/2004-220.

Organizations in the Province of Quebec Exemption Order, SOR/2003-374.


Regulations Specifying Investigative Bodies, SOR/2001-6.


PIPEDA applies to all collection, use or disclosure of Personal Information (as defined in Section 4(a) below) in the course of commercial activity by:

- federally regulated private sector organizations, including those in the telecommunications, broadcasting, and inter-provincial transportation and banking sectors, with respect to both customer and Employee Personal Information; and
- organizations that trade in Personal Information across provincial or national borders for consideration.

An “organization” is defined to include an association, a partnership, a person and a trade union. However, in provinces where a law has been passed that is substantially similar to PIPEDA, organizations and their collection, use or disclosure activities within the province that are covered by the provincial law are exempted from the application of PIPEDA. Provincial private sector
privacy legislation has been deemed substantially similar to PIPEDA in British Columbia, Alberta, Quebec, and, in relation to personal health information, Ontario, New Brunswick and Newfoundland and Labrador (Nova Scotia is expected to be added to this list with regard to personal health information). PIPEDA continues to apply to Employee Personal Information of federally regulated businesses everywhere in Canada, and to inter-provincial and international collection, use or disclosure of Personal Information.

4. Scope of the Law

a. Personal Data

PIPEDA applies to personally identifiable information (“Personal Information”) about an identifiable individual (“Data Subject”), i.e., any factual or subjective information, recorded or not about a Data Subject. Financial, health, employment, consumer contact and preferences data typically fall within the definition of Personal Information. Personal Information includes personal health information, which is defined as information about a Data Subject’s mental or physical health, including information concerning health services provided and information about tests and examinations. Personal Information generally does not include the name, title or business address or telephone number of an employee of an organization.

PIPEDA applies broadly to the collection, use, disclosure, handling and care, and any other processing of Personal Information in any form or representation, including electronic data recorded or stored on any medium, computer system, or other similar device, and that can be read or perceived by a person, system, or other device (e.g., display, printout, audio/video recording, or other data output).

b. Data Processing

“Processing” is not expressly defined in PIPEDA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating and deleting Personal Information – whether on a manual or automated basis.

c. Processing by Data Controllers

PIPEDA applies to Personal Information that:

- the organization collects, uses or discloses in the course of commercial activities; or
- is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.
d. Jurisdiction/Territoriality

PIPEDA applies to all Personal Information collected or processed in Canada, subject to the qualifications noted in Section 3 above regarding provinces where a law has been passed that has been deemed substantially similar to PIPEDA.

Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

In determining the requisite form of consent to be obtained, organizations are required to take into account the sensitivity of the Personal Information. Accordingly, the form of the consent sought by the organization below may vary, depending upon the circumstances and the type of Personal Information to be collected, used or disclosed. Although any Personal Information can be sensitive, depending on the context, note that some types of Personal Information, such as medical records and income records, are almost always considered to be sensitive. Employment and health care are generally matters of provincial regulation, and as such are not covered by PIPEDA for provincially regulated companies.

f. Employee Personal Data

Employee Personal Information is treated in the same manner as other Personal Information. Employee Personal Information typically does not include an employee’s name, title or business address or telephone number. Note, however, that PIPEDA does not apply to Employee Personal Information of a provincially regulated organization, because regulation of the processing of such Personal Information falls under the jurisdiction of applicable provincial privacy laws.

g. Other

The OPC may enter into binding compliance agreements with organizations where it believes, on reasonable grounds, that an organization has, will, or is likely to commit an act or omission that would contravene PIPEDA. Compliance agreements are voluntary on the part of the organizations and, in exchange, the OPC will not apply to the court for a hearing or suspension of any pending applications. At the same time, entering into a compliance agreement does not preclude individual complaints against the organization or the prosecution of an offense under PIPEDA. The agreements may contain any terms that the OPC considers necessary to ensure compliance with PIPEDA. If the OPC is of the opinion that the organization has complied with the agreement, the OPC shall notify the organization and withdraw any
outstanding applications. If, however, the OPC is of the opinion that the organization has not complied with the agreement, the OPC shall notify the organization and may apply to the court for an order requiring compliance with the agreement or commence or reinstate proceedings under PIPEDA.

5. Consent

a. General
The consent of a Data Subject is required for the collection, use or disclosure of Personal Information.
Consent must be obtained before or at the time of collection. When Personal Information that has been collected is to be used for a purpose not previously identified, consent of the Data Subject shall be obtained prior to use by informing the Data Subject of such new purpose.

PIPEDA does not necessarily require that the consent be obtained in writing. In determining the appropriate form of consent to be obtained from a Data Subject, consideration should be given to the reasonable expectations of the Data Subject, circumstances surrounding the collection and sensitivity of the Personal Information involved.

However, when consent is implied or obtained orally, for evidentiary reasons, an organization should as a matter of course keep some record of the consent obtained. The Privacy Commissioner of Canada recommends that express consent be used whenever possible and in all cases when the Personal Information is considered to be sensitive.

Relying on express consent protects both the Data Subject and the organization.

At a minimum, a request for consent should specify in plain language: (i) the nature of the Personal Information to be collected, used or disclosed; (ii) the specific uses to which the Personal Information will be put by receiving parties; (iii) the identity of the parties, if any, to whom Personal Information is to be disclosed; and (iv) the channels available for the Data Subject to amend or withdraw his or her consent (e.g., email, regular mail, 1-800 number, etc.).

A Data Subject should only be required to consent to the collection, use or disclosure of Personal Information in order to fulfill the explicitly specified and legitimate purposes.

Data Subjects can give consent in many ways.

Data Subjects can withdraw consent at any time. Consent can be given by an authorized representative (such as a legal guardian or a Data Subject having a power of attorney).
Consent clauses should be easy to find, use clear and straightforward language, avoid using blanket categories for purposes, uses and disclosures, and be as specific as possible about which organizations handle the Personal Information. Consent shall not be obtained through deception.

In certain circumstances, Personal Information may be collected, used or disclosed without the knowledge and consent of the Data Subject.

For example, consent may not need to be obtained where legal, medical or security reasons make it impossible or impractical to seek consent. Similarly, when the Personal Information is being collected for the detection and prevention of fraud or for law enforcement, it may not be necessary to obtain consent of the Data Subject, as doing so might defeat the purpose of collecting the Personal Information.

Organizations are expressly permitted to use and disclose individuals’ Personal Information without their knowledge or consent where the Personal Information is necessary to determine whether to proceed with or complete a business transaction, and certain measures are taken to protect the information. If the transaction is not completed, all Personal Information must be returned or destroyed by the recipient. If the transaction is completed, the recipient may continue to use the Personal Information as long as certain security measures are taken, the Personal Information is necessary for carrying on the activity that was the object of the transaction, and the individuals are notified of the completion of the transaction and the disclosure of their Personal Information within a reasonable amount of time afterwards. Notably, this exception to the general consent requirement does not apply where the purpose of the transaction is to buy, sell or lease Personal Information.

Organizations may disclose Personal Information to another organization without the knowledge or consent of an individual where it is reasonable for the purposes of investigating a breach or possible breach of an agreement or Canadian law and it is reasonable to expect that obtaining the individual’s consent would compromise the investigation. Similar exceptions also apply to investigations involving the detection, suppression or prevention of fraud where a person is suspected of being a victim of financial abuse.

b. Sensitive Data

An organization should seek express consent from a Data Subject when the Personal Information involved is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis.

c. Minors

For a Data Subject who is a minor, consent may be obtained from a legal guardian or person having power of attorney.
d. **Employee Consent**

Federal works, undertakings and business (e.g., airlines and banks) may collect, use and disclose the Personal Information of an employee without his or her consent where it is necessary to establish, manage or terminate the employment relationship as long as the employee is informed of such collection, use or disclosure. All the requirements set out by PIPEDA for the giving of consent by any Data Subject shall equally apply to consent given by employees covered by PIPEDA.

e. **Online/Electronic Consent**

Electronic consent will usually suffice if appropriate steps are taken to ensure that a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., an appropriately accessible hyperlink – directly above a consent button).

6. **Notice Requirements**

Under PIPEDA, an organization is required to ensure that individuals are able to acquire information about an organization’s policies and practices without unreasonable effort. The organization shall also ensure that this information is in a form that is generally understandable, and includes:

- the name or title, and the address, of the person who is accountable for the organization’s policies and practices and to whom complaints or inquiries can be forwarded;
- the means of gaining access to Personal Information held by the organization;
- a description of the type of Personal Information held by the organization, including a general account of its use;
- a copy of any brochures or other information that explain the organization’s policies, standards or codes; and
- what Personal Information is made available to related organizations (e.g., subsidiaries).

7. **Processing Rules**

An organization that processes Personal Data must: limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.
8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject; (ii) be informed by an organization of how the Data Subject’s Personal Data is being processed; (iii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iv) request the correction of the Data Subject’s Personal Data; and (v) request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

No formal registration requirements apply.

10. Data Protection Officers

Under PIPEDA, an organization is responsible for Personal Information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the principles. Upon request, the organization shall disclose the identity of the designated individual(s).

Notwithstanding the fact that the designated individual(s) are accountable for the organization’s compliance with the principles, other individuals within the organization may be responsible for the day-to-day collection and processing of Personal Information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

11. International Data Transfers

Under PIPEDA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, an organization is obligated to put appropriate data transfer agreements or other measures in place to address the obligations of third-party Data Processors and recipients of Personal Information in the context of onward transfers.

12. Security Requirements

Organizations are required to take steps to: (i) ensure that Personal Data in their possession and control is protected from unauthorized access and use; (ii) implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Under PIPEDA, an organization shall be responsible for Personal Information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other
means to provide a comparable level of protection while the information is being processed by the third party.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings, publication of breaches and/or private rights of action.

15. Data Security Breach

On an unspecified date in the future, amendments establishing a data breach notification requirement under PIPEDA will come into force. According to this new requirement, where there is a security breach and it is reasonable in the circumstances to believe that the breach could create a risk of significant harm, an organization must notify the OPC, any affected individual(s), and any third-party organizations that may be able to reduce the possible harm. The disclosure to the OPC and other third parties may be made without the prior consent of the individual where it is made for the purpose of reducing harm to the individual(s) affected by the security breach. The notification must contain sufficient information to allow the affected individual(s) to understand the significance and consequence of the breach to allow them to take any necessary steps to prevent or mitigate such harm. Any notice must be conspicuous and given directly to the individual in the prescribed form and manner as soon as is feasible.

PIPEDA defines significant harm as “bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property”.

Organizations must also keep and maintain records of all security breaches and provide these records to the OPC upon request by the OPC.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions and/or a criminal prosecution.

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.
17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.

18. E-Discovery
To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with PIPEDA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that Personal Information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering
Subsection 184(1) of the Criminal Code sets out the general rule that it is illegal to wilfully intercept a private communication: “Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”.

Therefore, organizations should ensure that the introduction and implementation of a spam-filtering solution are in compliance with PIPEDA and the Criminal Code.

20. Cookies
There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Alberta, Canada

1. Recent Privacy Developments

Global Privacy Sweep Finds Websites and Apps Often Do Not Effectively Communicate Privacy Practices

The Office of the Information & Privacy Commissioner of Alberta, together with 23 other privacy regulators around the world, examined 455 websites and mobile apps to understand how privacy policies are being communicated to users and to determine the degree of control users possess over the information they provide to websites and mobile applications. While most of the organizations were clear on the types of information collected, 20% of the 20 Alberta websites included in the review did not have privacy policies despite collecting personal information from users. 65% of the websites failed to disclose to users the specific location of the information. Over 50% of the websites did not provide a clear means for users to have personal information about them deleted or removed. Moreover, 40% of the sites failed to adequately explain whether personal information is being shared with third parties. As emphasized by the Information & Privacy Commissioner, “all sectors would be well served to ensure control is given back to consumers and citizens for both legal and ethical reasons. These include having mechanisms in place for individuals to access, delete and better understand what is happening to their personal information”.

OIPC Releases Survey Results On Awareness of Access and Privacy Laws

In October 2017, the Office of the Information & Privacy Commissioner of Alberta commissioned a public opinion survey to obtain feedback and input from Albertans around their awareness of access and privacy laws. Of the 800 respondents, only 27% felt more secure about the privacy of their personal information today compared to five years ago. While 90% felt it is important to protect their right to access information, only 39% were confident about their ability to exercise said right. From the survey results, the following issues have been identified as the most significant: identity theft and fraud; hacking, malware, ransomware and email phishing; inappropriate employee access; mobile device security; and child and youth privacy. The survey results can be viewed here: https://www.oipc.ab.ca/media/892286/Survey_Population_Survey_2017.pdf.
2. Emerging Privacy Issues and Trends

In its strategic business plan for 2015-2018, the OIPCA has stressed that it will take a more proactive approach to privacy law enforcement and has highlighted the following, among others, as items that it may focus on:

- compliance in events of data breach;
- compliance with privacy impact assessments under Alberta’s personal health information laws; and
- the privacy implications of the use and prevalence of:
  - biometrics;
  - mobile devices;
  - geo-location tracking software;
  - interoperability of information systems;
  - social media; and
  - open data initiatives.

3. Law Applicable

Personal Information Protection Act, SA 2003, c P-6.5 (“Alberta PIPA”) and related regulations.

Health Information Act, RSA 2000, c H-5 and related regulations.

This chapter focuses on the Alberta PIPA and related regulations.

The purpose of the Alberta PIPA is to govern the means by which private sector organizations handle Personal Information, and to ensure this occurs in a manner that recognizes both the right of an individual (“Data Subject”) to have his or her personally identifiable information (“Personal Information”) protected and the need of organizations to collect, use or disclose Personal Information for purposes that are reasonable.

An organization includes a corporation, an association that is not incorporated, a trade union, a partnership and an individual acting in a commercial way (e.g., an individual running an unincorporated business).

4. Scope of the Law

a. Personal Data

The Alberta PIPA applies to information about an identifiable individual (“Personal Information”) (e.g., name, home address, home phone number, ID numbers, physical description, educational qualifications, blood type, etc.).
“Business contact information” is a subset of Personal Information. It includes a Data Subject’s name, position or title, business telephone number, business email address, and other business contact information. The Alberta PIPA does not apply to business contact information when it is collected, used or disclosed for the purpose of contacting an individual in his or her business capacity.

The Alberta PIPA applies to a “record”, which means a record of information in any form or in any medium, whether in written, printed, photographic, electronic or any other form, but does not include a computer program or other mechanism that can produce a record.

b. Data Processing
Processing is not expressly defined in the Alberta PIPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating or deleting of Personal Information whether on a manual or automated basis.

c. Processing by Data Controllers
The Alberta PIPA applies to every organization and with respect to all Personal Information.

The Alberta PIPA does not apply:

- if the collection, use or disclosure of Personal Information is for personal or domestic purposes;
- if the collection, use or disclosure of Personal Information is for artistic, literary or journalistic purposes;
- if the collection, use or disclosure of business contact information is for the purpose of contacting an individual in that individual’s capacity as an employee of an organization;
- if the Personal Information is in the custody or control of a “public body”;
- if the Freedom of Information and Protection of Privacy Act applies;
- if the information is health information as defined in the Health Information Act;
- if the information is about an individual who has been dead for 20 years or more or in a record that is 100 years old or older; or
- if the information is Personal Information in court files.
An organization is responsible for all of the Personal Information that is either in its custody or under its control. Where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance with the Alberta PIPA. The organization must designate one or more individuals to be responsible for ensuring the organization complies with the Alberta PIPA.

An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under the Alberta PIPA, and make information about such policies and practices available on request.

d. Jurisdiction/Territoriality

The Alberta PIPA applies to provincially regulated businesses, non-profit organizations (only when they collect, use or disclose Personal Information in connection with a “commercial activity”), trade unions and other organizations in Alberta. “Commercial activity” means a transaction, act or conduct that has a commercial character to it, such as selling, bartering or leasing donor, membership or other fundraising lists. It also includes operating a private school or college or an early childhood services program.

However, PIPEDA will, in most instances, still apply to provincially regulated organizations when they transfer Personal Information across Alberta’s borders, in the course of commercial activity (i.e., for consideration). Organizations should thus consider obtaining consent, as appropriate, in connection with such trans-border transfers.

PIPEDA will also still apply to federally regulated businesses in Alberta.

Federal and provincial public sector privacy statutes apply to Personal Information in records held by the government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

The form of the consent sought by the organization pursuant to Section 5 below may vary, depending upon the circumstances and the type of information to be collected, used or disclosed. In determining the form of consent to use, organizations shall take into account the sensitivity of the information.

Although some information (for example, health and financial information) is almost always considered to be sensitive, any information can be sensitive depending on the context. In such circumstances, as a best practice, organizations should obtain clear and express consent.
f. Employee Personal Data
An “Employee” includes an apprentice, volunteer, participant, work experience or co-op student and an individual acting as an agent for an organization, employed by the organization or who performs a service for the organization as a partner or director, officer or other office-holder of the organization, whether or not the individual is paid.

“Employee Personal Information” means, with respect to an individual who is a potential, current or former employee of an organization, Personal Information that is reasonably required by an organization to establish, manage or end an employment or volunteer work relationship, or to manage a post-employment relationship.

5. Consent
a. General
An organization generally must not collect, use or disclose Personal Information about a Data Subject without first obtaining consent.

A Data Subject may give consent subject to any reasonable terms, conditions or qualifications established, set or approved by, or otherwise acceptable to, the Data Subject.

Consent may not be obtained by providing false or misleading information regarding the collection, use or disclosure of information through deception.

The Alberta PIPA recognizes the following types of consent: express consent, implied consent and opt-out consent.

The Alberta PIPA does not require an organization to provide notice when relying on implied consent to collect Personal Information.

An organization may not collect, use or disclose Personal Information for a different purpose than the purpose or purposes for which it was collected. A Data Subject can consent to an organization collecting his or her Personal Information from another organization.

A Data Subject is deemed to have consented to the collection of his or her Personal Information by an organization if the collection took place prior to 1 January 2004, and such consent may be relied upon where the Personal Information is used or disclosed for the purposes for which it was originally collected.

A Data Subject can change or withdraw consent by giving the organization reasonable notice, as long as doing so does not contravene a legal duty or obligation between the Data Subject and the organization. On receipt of such notice, an organization must inform the Data Subject of the likely consequences to the Data Subject of withdrawing consent. An organization
must not prohibit a Data Subject from withdrawing consent to the collection, use or disclosure of Personal Information related to the Data Subject.

Following withdrawal of consent to the collection, use or disclosure of Personal Information by a Data Subject, the organization must stop collecting, using or disclosing the Personal Information unless the collection, use or disclosure is permitted without consent. A Data Subject may not withdraw consent given for the performance of a legal obligation.

The Alberta PIPA provides that neither an organization nor a Data Subject can impose a liability or an obligation on the other as a result of the withdrawal or variation of consent. An organization must not, as a condition of supplying a product or service, require a Data Subject to consent to the collection, use or disclosure of Personal Information beyond what is necessary to provide the product or service.

An organization may collect, use or disclose Personal Information about a Data Subject without consent, if the collection, use and disclosure are clearly in the interests of the Data Subject:

- when another act or regulation requires or allows for collecting information without consent;
- when the Personal Information is collected in accordance with the provisions of a treaty;
- when it relates to a subpoena, warrant or court order;
- when it is provided by a public body;
- when it is necessary for medical treatment;
- when the collection is for an investigation or a proceeding;
- when the Personal Information is publicly available;
- when the organization is a credit reporting agency;
- when it is required or authorized by law;
- for disclosures without consent;
- for the collection of a debt; or
- for the transfer of Personal Information to a third party.

Under certain circumstances, a trade union may also collect Personal Information about an individual without his or her consent for the purpose of informing or persuading the public about a significant matter relating to a labor relations dispute involving the trade union.
An organization may disclose Personal Information about its employees, customers, directors, officers or shareholders without their consent to a prospective party in a business transaction. A business transaction is defined to mean the purchase, sale, lease, merger, amalgamation, acquisition or disposal of an organization (or part of an organization), or any business or activity or business asset of an organization. If a business transaction does not proceed or is not completed, a prospective party must destroy or return to the organization any Personal Information that the prospective party collected about the employees, customers, directors, officers and shareholders of the organization. An organization may not disclose Personal Information in a business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of Personal Information.

b. Sensitive Data
An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis. Thus, at a minimum, a request for consent should refer to: (i) the nature of the information to be collected, used or disclosed; (ii) the specific uses to which the information will be put by the parties receiving it; and (iii) the identity of the parties to whom information is to be disclosed, as applicable. A request for consent should also specify, in simple terms, the channels that are available (e.g., email, regular mail, 1-800 number, etc.) for the Data Subject to amend or withdraw his or her consent.

The more sensitive the Personal Information is, the greater the likelihood that express consent will be required for its collection, use and disclosure.

c. Minors
The guardian of a minor may give or refuse consent to the collection, use and disclosure of the minor’s Personal Information if the minor is incapable of exercising that right (i.e., if the minor is incapable of understanding his or her rights under the Alberta PIPA and the consequences of exercising them).

d. Employee Consent
The Alberta PIPA permits an organization to collect, use or disclose Employee Personal Information without consent for reasonable purposes related to managing or recruiting personnel. “Managing personnel” means the carrying out of that part of human resource management relating to the duties and responsibilities of employees. It can also refer to administering personnel and includes activities such as payroll and succession planning.

Consent is required for the collection by the employer of Personal Information that does not constitute Employee Personal Information, such as information
collected in relation to charitable donations, personal family issues or non-work-related health, religious or financial issues.

An organization shall collect, use or disclose Employee Personal Information only if it is for a reasonable purpose, the information relates to the employment or volunteer work relationship and the organization has provided the Data Subject with reasonable notification before collection, use or disclosure of the information.

Where an organization outsources “back office” human resources functions, such as payroll or administration, the Alberta PIPA may also permit the contracting organization to collect the Employee Personal Information without consent.

e. Online/Electronic Consent

Consent given or transmitted by electronic means will qualify as “written consent” only where the receiving organization produces or is capable of producing a version of that consent in paper form. Organizations that make use of paper-less and/or signature-less contracts via their websites must ensure that they can produce evidence or paper versions of the consent upon request.

6. Notice Requirements

An organization that collects Personal Information generally must or should provide Data Subjects with information about the organization’s identity, the types of Personal Information collected, the purposes for collecting the Personal Information, the organization’s privacy practices (which must be clear and transparent), third parties to which the organization will disclose the Personal Information, the rights of the Data Subject, how the Personal Information is to be retained, where the Personal Information is to be transferred, where the Personal Information is to be stored, how to make an enquiry or file a complaint, how to access and/or correct the Data Subject’s Personal Information, the duration of the proposed processing, and the means of transmitting the Personal Information.

7. Processing Rules

An organization that processes Personal Information must limit the use of the Personal Information to those activities that are necessary to fulfill the identified purpose(s) for which the Personal Information was collected, and delete/destroy/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Information that the organization holds about the Data Subject,
and how the Data Subject’s Personal Information will be used and disclosed; (ii) access the Data Subject’s Personal Information, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Information; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Information.

9. Registration/Notification Requirements
An organization that collects and processes Personal Information is not required to register, file and notify the appropriate data authority.

10. Data Protection Officers
An organization must designate one or more individuals to be responsible for ensuring that the organization complies with the Alberta PIPA.

11. International Data Transfers
Under the Alberta PIPA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, organizations are required to notify individuals if they use service providers outside Canada to collect and/or process Personal Information. As the definition of “service providers” is quite broad and includes affiliated entities, it is recommended that appropriate data transfer agreements be put in place to address the obligations of recipients of Personal Information in the context of onward transfers.

12. Security Requirements
Organizations are required to: (i) take steps to ensure that Personal Information in their possession and control is protected from unauthorized access and use; and (ii) implement appropriate physical, technical and organizational security safeguards to protect Personal Information.

13. Special Rules for Outsourcing of Data Processing to Third Parties
An organization is responsible for Personal Information that is in its custody or under its control and where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints; data authority investigations/audits; data authority inquiries and orders; administrative fines, penalties or sanctions; seizure of equipment or data; civil actions/private rights of action; class actions; and prosecution for offenses.
15. Data Security Breach

Alberta is the first Canadian jurisdiction to require mandatory data security breach notification in the private sector. Organizations are required to report incidents of security breach to the Information and Privacy Commissioner of Alberta when there is a real risk of significant harm to an individual and the Commissioner can require such organizations to notify affected individuals.

An organization that is involved in a data breach situation may be subject to various penalties as noted above under “Enforcement and Sanctions”.

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Information.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Alberta provided that they are in compliance with local laws.

18. E-Discovery

To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with the Alberta PIPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization is required to use contractual or other means to ensure that Personal Information and the system employed are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code (Canada) sets out the general rule that it is illegal to wilfully intercept a private communication: “Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”.

Therefore, the organization shall ensure that the introduction and implementation of a spam-filtering solution is in compliance with the Alberta PIPA and the federal Criminal Code.
20. Cookies

There are specific laws/rules in Alberta that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
1. Recent Privacy Developments

**Guidance Document on Access to Data for Health Research**

In January 2018, the Office of the Information & Privacy Commissioner for British Columbia published a guidance document entitled “Access to Data for Health Research”. The document outlines the legal provisions that apply to the disclosure of personal information of British Columbians for the purpose of health research. Under applicable privacy laws, disclosure of personal information, even without the consent of the Data Subject, is permitted as long as it is for research purposes that are of public interest.

**Safeguarding Privacy Rights in the Implementation of Employee Monitoring Programs**

The Office of the Information & Privacy Commissioner for British Columbia issued a guidance document in November 2017 on “Employee Privacy Rights”. The guidance document provides an assessment of the privacy impact of various employee monitoring programs, including the implementation of video and audio surveillance, employee monitoring software and GPS tracking. In implementing employee monitoring programs, organizations should ensure that the privacy rights of employees are safeguarded.

**Supreme Court of Canada rules on the “right to be forgotten” principle**

The Supreme Court of Canada released its landmark ruling in *Equustek* in 2017, upholding a decision of the Court of Appeals of British Columbia, which ordered an internet search engine to de-index websites from its global search index. The decision arose from a lower court ruling that ordered the search engine to block websites that were selling goods online in violation of intellectual property rights. The plaintiffs sought the help of the search engine after defendants continued selling illegal goods online. While the search engine voluntarily de-indexed over 300 domains on the Canadian version of the search engine, they refused to further de-index the websites from the rest of its search engines worldwide. Plaintiffs then brought a preliminary injunction against the search engine. The Supreme Court of Canada affirmed the lower courts’ decisions and ordered the search engine to de-index the websites worldwide. This case highlights the importance of preserving the effectiveness of law in the online environment by striking a balance between the interests of parties, internet search engines and the general public.
2. Emerging Privacy Issues and Trends

In its most recent budget submission, the OIPCBC enumerated its priorities for 2018-2019, which include:

- more timely service to citizens on complaint and appeal cases;
- increase in the implementation of effective privacy management programs by public and private sector organizations; and
- decrease in the unwarranted use of surveillance technologies.

3. Law Applicable

Personal Information Protection Act, SBC 2003, c 63 (“BC PIPA”) and related regulations.

The purpose of the BC PIPA is to govern the collection, use and disclosure of Personal Information by organizations in a manner that recognizes both the right of individuals to protect their Personal Information and the need of organizations to collect, use or disclose Personal Information for purposes that a reasonable person would consider appropriate in the circumstances.

An organization includes a person (which at law includes corporations), an unincorporated association, a trade union, a trust or a not-for-profit organization. It excludes a “private trust” and an individual “acting as an employee”.

4. Scope of the Law

a. Personal Data

The BC PIPA applies to personally identifiable information (“Personal Information”) about an identifiable individual (“Data Subject”) and includes Employee Personal Information, but does not include:

- business contact information; or
- work product information.

The BC PIPA applies to a “Document” which includes:

- a thing on or by which information is stored; and
- a document in electronic or similar form.

The BC PIPA applies broadly to the collection, use, disclosure, handling and care, and any other processing of Personal Information in any form or representation, including electronic data recorded or stored on any medium, computer system or other similar device, and that can be read or perceived by a person, system or other device (e.g., display, printout, audio/video recording...
or other data output). The BC PIPA does not apply to general information used to operate the organization’s business.

b. Data Processing
Processing is not expressly defined in the BC PIPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of a Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating or deleting of Personal Information – whether on a manual or automated basis.

c. Processing by Data Controllers
The BC PIPA applies with limited exceptions to “every organization”. It covers commercial and not-for-profit activities and Employee Personal Information within employment relationships. The BC PIPA does not apply:

- if collection, use or disclosure is for personal or domestic purposes, journalistic, artistic or literary purposes or where the federal PIPEDA or the Freedom of Information and Protection of Privacy Act (BC) applies;
- to Personal Information in a court document;
- to solicitor-client privilege information;
- to information available by law to a party or a proceeding; and
- to the collection of Personal Information that was collected prior to the date the legislation came into force.

The BC PIPA applies to Personal Information that:

- an organization considers appropriate in the circumstances; and
- is under its control, including Personal Information that is not in the custody of the organization.

PIPEDA applies to transfers of Personal Information across borders.

d. Jurisdiction/Territoriality
The BC PIPA applies to provincially regulated businesses, non-profit organizations, trade unions and other organizations in British Columbia. However, PIPEDA will, in most instances, still apply to provincially regulated organizations when they transfer Personal Information across British Columbia’s borders in the course of commercial activity (i.e., for consideration). Organizations should thus consider obtaining consent, as appropriate, in connection with such trans-border transfers. PIPEDA will also still apply to federally regulated organizations operating in British Columbia.
Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. **Sensitive Personal Data**

The form of the consent sought by the organization pursuant to Section 5 below may vary, depending upon the circumstances and the type of information to be collected, used or disclosed. In determining the form of consent to use, organizations are required to take into account the sensitivity of the information.

Although some information (for example, health and financial information) is almost always considered to be sensitive, any information can be sensitive depending on the context. In such circumstances, as a best practice, organizations should obtain clear and express consent.

f. **Employee Personal Data**

Employee Personal Information includes Personal Information about a Data Subject that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that Data Subject, but does not include Personal Information that is not about a Data Subject’s employment. Employee Personal Information does not include business contact information or work product information. The term “employees” is defined to include volunteers.

5. **Consent**

a. **General**

An organization must not collect, use or disclose Personal Information about a Data Subject without first obtaining consent. In order for a consent to be valid, the organization must inform the Data Subject, verbally or in writing, of the purpose for the collection of his/her Personal Information.

An organization must not, as a condition of supplying a product or service, require a Data Subject to consent to the collection, use or disclosure of Personal Information beyond what is necessary to provide the product or service.

Consent shall not be obtained by providing false or misleading information respecting the collection, use or disclosure of information through deception.

The BC PIPA recognizes the following types of consent: express consent, deemed consent and opt-out consent.
An organization may not collect, use or disclose Personal Information for a purpose different than the purpose for which it was collected.

The BC PIPA does not apply to the collection, use or disclosure of Personal Information that was collected before 1 January 2004. However, if the Personal Information that was collected before 1 January 2004 is used for a new purpose, fresh consent would have to be obtained in connection with such new purpose.

A Data Subject can cancel or change his or her consent by giving the organization reasonable notice. On receipt of such notice, an organization must inform the Data Subject of the likely consequences to the Data Subject of withdrawing his or her consent. An organization must not prohibit a Data Subject from withdrawing his or her consent to the collection, use or disclosure of Personal Information. Pursuant to withdrawal of consent to the collection, use or disclosure of Personal Information by an organization, the organization must stop collecting, using or disclosing the Personal Information unless continued collection, use or disclosure is permitted without consent. A Data Subject may not withdraw consent given for the performance of a legal obligation or consent given to a credit reporting agency.

An organization may collect, use or disclose Personal Information about a Data Subject without consent in certain situations (e.g., medical emergency, investigation, or required or authorized by law). An organization may disclose Personal Information about its employees, customers, directors, officers or shareholders without their consent to a prospective party in a business transaction. A business transaction is defined to mean the purchase, sale, lease, merger, amalgamation, acquisition or disposal of an organization (or part of an organization) or any business or activity or business asset of an organization. If a business transaction does not proceed or is not completed, a prospective party must destroy or return to the organization any Personal Information that the prospective party collected about the employees, customers, directors, officers and shareholders of the organization. The organization is not authorized to disclose Personal Information to a party or prospective party for the purposes of a business transaction that does not involve substantial assets of the organization other than this Personal Information. An organization may disclose, without the consent of a Data Subject, Personal Information for a research purpose, including statistical research and for archival or historical purposes.

b. Sensitive Data
An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis. Thus, at a minimum, a request for consent should refer to: (i) the nature of the information to be collected, used
or disclosed; (ii) the specific uses to which the information will be put by the parties receiving it; and (iii) the identity of the parties to whom information is to be disclosed, as applicable. A request for consent should also specify, in simple terms, the channels that are available (e.g., email, regular mail, 1-800 number, etc.) for the Data Subject to amend or withdraw his or her consent. It should be noted that the more sensitive the Personal Information is, the greater the likelihood that express consent will be required for its collection, use and disclosure.

c. Minors
The guardian of a minor may give or refuse consent to the collection, use and disclosure of the minor’s Personal Information if the minor is incapable of exercising that right in the circumstances.

d. Employee Consent
An organization may collect, use and disclose Employee Personal Information without the consent of the Data Subject if the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the Data Subject. An organization must notify the Data Subject that it will be collecting Employee Personal Information about the Data Subject and the purposes for the collection before the organization collects the Employee Personal Information without the consent of the Data Subject.

e. Online/Electronic Consent
Electronic consent will suffice if appropriate steps are taken to ensure that a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., inclusion of an appropriately accessible hyperlink – directly above a consent button).

6. Notice Requirements
A organization that collects Personal Information generally must or should provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Information being collected; (iii) the purposes for collecting the Personal Information; (iv) its privacy practices (which must be clear and transparent); (v) third parties to which the organization will disclose the Personal Information; (vi) the rights of the Data Subject; (vii) how the Personal Information is to be retained; (viii) where the Personal Information is to be transferred; (ix) where the Personal Information is to be stored; (x) how to make an enquiry or file a complaint; (xi) how to access and/or correct the Data Subject’s Personal Information; (x) the duration of the proposed processing; and (xi) the means of transmitting the Personal Information.
7. Processing Rules
An organization that processes Personal Information must limit the use of the Personal Information to those activities that are necessary to fulfill the identified purpose(s) for which the Personal Information was collected and delete/destroy/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: (i) be informed by an organization of the Personal Information that the organization holds about the Data Subject, and how the Data Subject’s Personal Information will be used and disclosed; (ii) access the Data Subject’s Personal Information, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Information; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Information.

9. Registration/Notification Requirements
An organization that collects and processes Personal Information is not required to register, file and notify the appropriate data authority.

10. Data Protection Officers
An organization must designate one or more individuals to be responsible for ensuring compliance. The identity and contact information of the privacy officer(s) must be made available to the public. The privacy officer(s) may also be the contact person(s) for answering questions about the BC PIPA and for handling access requests and complaints.

11. International Data Transfers
Under the BC PIPA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, it is recommended that appropriate data transfer agreements be put in place to address the obligations of recipients of Personal Information in the context of onward transfers.

12. Security Requirements
Organizations are required to: (i) take steps to ensure that Personal Information in their possession and control is protected from unauthorized access and use; and (ii) implement appropriate physical, technical and organizational security safeguards to protect Personal Information.
13. Special Rules for Outsourcing of Data Processing to Third Parties

Under BC PIPA, an organization is responsible for Personal Information under its control, including Personal Information that is not in the custody of the organization.

Organizations that disclose Personal Information to third parties are required to use contractual or other means to protect Personal Information and comply with sector-specific requirements. Organizations shall be liable together with the third-party providers in case of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints; data authority investigations/audits; data authority inquiries and orders; administrative fines, penalties or sanctions; seizure of equipment or data; civil actions/private rights of action; class actions; and prosecution for offenses.

15. Data Security Breach

While the BC PIPA does not create an explicit legal requirement to notify the BC Commissioner or affected individuals in the event of a data security breach, it obliges organizations to take reasonable security measures to protect Personal Information in their custody. The Information & Privacy Commissioner for British Columbia has also published guidance documents regarding privacy breaches and breach notification, which provide information on how to address data security breaches and what information to include if an organization decides to report the breach to the Commissioner or to affected individuals.

An organization that is involved in a data breach situation may be subject to various penalties as noted above under “Enforcement and Sanctions”.

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Information.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in British Columbia provided that they are in compliance with local laws.

18. E-Discovery

To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with the
BC PIPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization is required to use contractual or other means to ensure that Personal Information and the system employed are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code (Canada) sets out the general rule that it is illegal to wilfully intercept a private communication: “Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”.

Therefore, the organization shall ensure that the introduction and implementation of a spam-filtering solution are in compliance with the BC PIPA and the federal Criminal Code.

20. Cookies

There are specific laws/rules in British Columbia that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Manitoba, Canada

1. Recent Privacy Developments

*Manitoba Enacts “Revenge Porn” Law*

In January 2016, the Manitoba government enacted the Intimate Image Protection Act, to help individuals whose intimate images are distributed without their permission. The Act applies when someone with an intimate image of another person distributes it (or threatens to distribute it) without that person’s consent. The Act creates a private right of action whereby victims can sue in civil court to hold a person accountable financially for distributing an intimate image without consent. In such case, the court may make an order for damages, disgorgement of profits or any other order the court considers appropriate, such as an injunction.

*Manitoba Enacts Private Sector Privacy Law*

In 2013, the Manitoba government enacted the Personal Information Protection and Identity Theft Prevention Act ("Manitoba PIPITPA"), making it the fourth province along with British Columbia, Alberta and Quebec to enact broadly applicable private sector privacy legislation. The Manitoba PIPITPA, which is not yet in force, will apply to all private sector organizations including corporations, unincorporated associations, unions, partnerships and individuals acting in a commercial capacity. The Manitoba PIPITPA generally requires organizations to obtain the consent of an individual before collecting, using or disclosing his or her Personal Information. The Manitoba PIPITPA also requires organizations to provide Data Subjects with reasonable access and correction rights and to take reasonable security precautions against privacy risks.

The Manitoba PIPITPA resembles the private sector privacy laws of Alberta and British Columbia in many ways, such as by establishing offenses punishable by fines of up to CAD 100,000 and by providing exceptions for employers collecting, using and disclosing the Personal Information of employees under certain circumstances. An important distinction between the Manitoba PIPITPA and the privacy laws of Alberta and British Columbia is that it provides fewer circumstances in which an individual gives implied consent. For example, the privacy legislations of Alberta and British Columbia provide that consent is implied where the individual has an interest in a pension plan and the processing of Personal Information relates to enrollment or coverage under the plan. The Manitoba PIPITPA does not contain a similar provision.

The Manitoba PIPITPA will be administered in part by the Manitoba Ombudsman, who is currently responsible for investigating complaints and
reviewing compliance with respect to The Freedom of Information and Protection of Privacy Act, which is Manitoba’s public sector privacy legislation, and the Personal Health Information Act, which relates to Manitoba’s health sector. Unlike the privacy commissioners of Alberta, British Columbia and Quebec, the Manitoba Ombudsman does not have the power to make orders respecting issues of legal compliance. The privacy regime in Manitoba is further complemented by the provincial Privacy Act, which creates a private cause of action for breach of privacy.

2. Emerging Privacy Issues and Trends

*Manitoba Ombudsman 2016 Annual Report*

In May 2017, the Manitoba Ombudsman released its 2016 Annual Report, highlighting the work and accomplishments of the office under the Freedom of Information and Protection of Privacy Act, the Personal Health Information Act, the Ombudsman Act and the Public Interest Disclosure (Whistleblower Protection) Act. In respect of access and privacy, the Report discusses the office’s approach to complaint investigations, its role in formal and informal consultations, its commitment to minimizing the harm associated with privacy breaches and its commitment to interjurisdictional collaboration.

3. Law Applicable

The Personal Information Protection and Identity Theft Protection Act, CCSM c P33.7 (“Manitoba PIPITPA”) (not yet in force).

The Privacy Act, CCSM c P125.

Personal Health Information Act, CCSM c P33.5 and related regulations.

This chapter focuses on the Manitoba PIPITPA.

The purpose of the Manitoba PIPITPA is to govern the collection, use and disclosure of Personal Information by organizations in a manner that recognizes both the right of individuals to protect their Personal Information and the need of organizations to collect, use or disclose Personal Information for purposes that a reasonable person would consider appropriate in the circumstances.

An organization includes a person (which at law includes corporations), an unincorporated association, a trade union, a trust or a non-profit organization. It excludes a “private trust” and an individual “acting as an employee”.

4. Scope of the Law

Please note that the Manitoba PIPITPA is not yet in force.
a. Personal Data
The Manitoba PIPITPA applies to Personal Information that can identify an individual (e.g., name, home address, home phone number, ID numbers) and information about a Data Subject (e.g., physical description, educational qualifications, blood type).

“Business contact information” is a subset of Personal Information. It includes a Data Subject’s name, position or title, business telephone number, business email address, and other business contact information. The Manitoba PIPITPA does not apply to business contact information when it is collected, used or disclosed for the purpose of contacting an individual in his or her business capacity.

The Manitoba PIPITPA applies to a “record”, which means a record of information in any form or in any medium, whether in written, printed, photographic, electronic or any other form, but does not include a computer program or other mechanism that can produce a record.

b. Data Processing
Processing is not expressly defined in the Manitoba PIPITPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of a Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating or deleting of Personal Information – whether on a manual or automated basis.

c. Processing by Data Controllers
The Manitoba PIPITPA applies to every organization and with respect to all Personal Information.

The Manitoba PIPITPA does not apply:

- if the collection, use or disclosure of Personal Information is for personal or domestic purposes;
- if the collection, use or disclosure of Personal Information is for artistic, literary or journalistic purposes;
- if the collection, use or disclosure of business contact information is for the purpose of contacting an individual in that individual’s capacity as an employee of an organization;
- if the Personal Information is in the custody or control of a “public body”;
- if the Freedom of Information and Protection of Privacy Act applies;
- if the information is health information as defined in the Personal Health Information Act;
• if the information is about an individual who has been dead for 20 years or more or in a record that is 100 years old or older; or

• if the information is Personal Information in court files.

An organization is responsible for all of the Personal Information that is either in its custody or under its control. Where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance with the Manitoba PIPITPA. The organization must designate one or more individuals to be responsible for ensuring the organization complies with the Manitoba PIPITPA.

An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under the Manitoba PIPITPA, and make information about such policies and practices available on request.

d. Jurisdiction/Territoriality

The Manitoba PIPITPA applies to provincially regulated businesses, non-profit organizations (only when they collect, use or disclose Personal Information in connection with a “commercial activity”), trade unions and other organizations in Manitoba. “Commercial activity” means a transaction, act or conduct that has a commercial character to it, such as selling, bartering or leasing donor, membership or other fundraising lists. It also includes operating a private school or college or an early childhood services program.

However, PIPEDA will, in most instances, still apply to provincially regulated organizations when they transfer Personal Information across Manitoba’s borders, in the course of commercial activity (i.e., for consideration). Organizations should thus consider obtaining consent, as appropriate, in connection with such trans-border transfers.

PIPEDA will also still apply to federally regulated businesses in Manitoba.

Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

The form of the consent sought by the organization pursuant to Section 5 below may vary, depending upon the circumstances and the type of information to be collected, used or disclosed. In determining the form of consent to use, organizations shall take into account the sensitivity of the information.
Although some information (for example, health and financial information) is almost always considered to be sensitive, any information can be sensitive depending on the context. In such circumstances, as a best practice, organizations should obtain clear and express consent.

f. Employee Personal Data
An “Employee” includes an apprentice, volunteer, participant, work experience or co-op student and an individual acting as an agent for an organization, employed by the organization or who performs a service for the organization as a partner or director, officer or other office-holder of the organization, whether or not the individual is paid.

“Employee Personal Information” means, in respect to an individual who is a potential, current or former employee of an organization, Personal Information that is reasonably required by an organization to establish, manage or end an employment or volunteer work relationship or to manage a post-employment relationship.

5. Consent
a. General
An organization must not collect, use or disclose Personal Information about a Data Subject without first obtaining consent.

A Data Subject may give consent subject to any reasonable terms, conditions or qualifications established, set or approved by or otherwise acceptable to, the Data Subject.

Consent shall not be obtained by providing false or misleading information regarding the collection, use or disclosure of information through deception.

The Manitoba PIPITPA recognizes the following types of consent: express consent, deemed consent and opt-out consent.

The Manitoba PIPITPA does not require an organization to provide notice when relying on implied consent to collect Personal Information.

An organization may not collect, use or disclose Personal Information for a different purpose than the purpose for which it was collected. A Data Subject can consent to an organization collecting his or her Personal Information from another organization.

A Data Subject is deemed to have consented to the collection of his or her Personal Information by an organization if the collection took place prior to the date upon which the Manitoba PIPITPA comes into force, and such consent may be relied upon where the Personal Information is used or disclosed for the purposes for which it was originally collected.
A Data Subject can change or take back his or her consent by giving the organization reasonable notice, as long as doing so does not break a legal duty or promise between the Data Subject and the organization. On receipt of such notice, an organization must inform the Data Subject of the likely consequences to the Data Subject of withdrawing his or her consent. An organization must not prohibit a Data Subject from withdrawing his or her consent to the collection, use or disclosure of Personal Information related to the Data Subject.

Pursuant to withdrawal of consent to the collection, use or disclosure of Personal Information by a Data Subject, the organization must stop collecting, using or disclosing the Personal Information unless the collection, use or disclosure is permitted without consent. A Data Subject may not withdraw consent given for the performance of a legal obligation.

The Manitoba PIPITPA provides that neither an organization nor a Data Subject can impose a liability or an obligation on the other as a result of the withdrawal or variation of consent. An organization must not, as a condition of supplying a product or service, require a Data Subject to consent to the collection, use or disclosure of Personal Information beyond what is necessary to provide the product or service.

An organization may collect, use or disclose Personal Information about a Data Subject without consent, if the collection, use and disclosure are clearly in the interests of the Data Subject:

- when another act or regulation requires or allows for collecting information without consent;
- when the Personal Information is collected in accordance with the provisions of a treaty;
- when it relates to a subpoena, warrant or court order;
- when it is provided by a public body;
- when it is necessary for medical treatment;
- when the collection is for an investigation or a proceeding;
- when the Personal Information is publicly available;
- when the organization is a credit reporting agency;
- when it is required or authorized by law;
- for disclosures without consent;
- for the collection of a debt; or
• for the transfer of Personal Information to a third party.

An organization may disclose Personal Information about its employees, customers, directors, officers or shareholders without their consent to a prospective party in a business transaction. A business transaction is defined to mean the purchase, sale, lease, merger, amalgamation, acquisition or disposal of an organization (or part of an organization) or any business or activity or business asset of an organization. If a business transaction does not proceed or is not completed, a prospective party must destroy or return to the organization any Personal Information that the prospective party collected about the employees, customers, directors, officers and shareholders of the organization. An organization may not disclose Personal Information in a business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of Personal Information.

b. Sensitive Data
An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis. Thus, at a minimum, a request for consent should refer to: (i) the nature of the information to be collected, used or disclosed; (ii) the specific uses to which the information will be put by the parties receiving it; and (iii) the identity of the parties to whom information is to be disclosed, as applicable. A request for consent should also specify, in simple terms, the channels that are available (e.g., email, regular mail, 1-800 number, etc.) for the Data Subject to amend or withdraw his or her consent.

The more sensitive the Personal Information is, the greater the likelihood that express consent will be required for its collection, use and disclosure.

c. Minors
The guardian of a minor may give or refuse consent to the collection, use and disclosure of the minor’s Personal Information if the minor is incapable of exercising that right.

d. Employee Consent
The Manitoba PIPITPA permits an organization to collect, use or disclose Employee Personal Information without consent for reasonable purposes related to managing or recruiting personnel. “Managing personnel” means the carrying out of that part of human resource management relating to the duties and responsibilities of employees. It can also refer to administering personnel and includes activities such as payroll and succession planning.

Consent is still required for the collection by the employer of Personal Information that does not constitute Employee Personal Information, such as
information collected in relation to charitable donations, personal family issues or non-work-related health, religious or financial issues.

An organization shall collect, use or disclose Employee Personal Information only if it is for a reasonable purpose, the information relates to the employment or volunteer work relationship and the organization has provided the Data Subject with reasonable notification before collection, use or disclosure of the information.

Where an organization outsources “back office” human resources functions, such as payroll or administration, the Manitoba PIPITPA may also permit the contracting organization to collect the Employee Personal Information without consent.

The Manitoba PIPITPA applies to Employee Personal Information in the same manner and to the same extent as it does to all other Personal Information.

e. **Online/Electronic Consent**

Consent given or transmitted by electronic means will qualify as “written consent” only where the receiving organization produces or is capable of producing a version of that consent in paper form. Organizations that make use of paper-less and/or signature-less contracts via their websites must ensure that they can produce evidence or paper versions of the consent upon request.

6. **Notice Requirements**

An organization that collects Personal Information must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Information being collected; (iii) the purposes for collecting Personal Information; (iv) its privacy practices (which must be given in a clear and transparent way); (v) third parties to which the organization will disclose the Personal Information; (vi) the rights of the Data Subject; (vii) how the Personal Information is to be retained; (viii) where the Personal Information is to be transferred; (ix) where the Personal Information is to be stored; (x) how to access and/or correct the Data Subject’s Personal Information; and (xi) the duration of the proposed processing.

7. **Processing Rules**

An organization that processes Personal Information must limit the use of the Personal Information to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Information was collected, and delete/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.
8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Information the organization holds about the Data Subject and how the Data Subject’s Personal Information is being processed; (ii) access the Data Subject’s Personal Information, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Information; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Information.

9. Registration/Notification Requirements

No formal registration requirements apply.

10. Data Protection Officers

An organization must designate one or more individuals to be responsible for ensuring that the organization complies with the Manitoba PIPITPA.

11. International Data Transfers

Under the Manitoba PIPITPA, there are no formal restrictions on transfers of Personal Information from Canada to other jurisdictions. However, organizations are required to notify individuals if they use service providers outside Canada to collect and/or process Personal Information. As the definition of “service providers” is quite broad and includes affiliated entities, it is recommended that appropriate data transfer agreements be put in place to address the obligations of recipients of Personal Information in the context of onward transfers.

12. Security Requirements

An organization must protect Personal Information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

13. Special Rules for Outsourcing of Data Processing to Third Parties

An organization is responsible for Personal Information that is in its custody or under its control and where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines,
penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Yes. An organization is required to report incidents of security breach to an individual when the Personal Information about the individual that is under its control is stolen, lost or accessed in an unauthorized manner.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, and/or a criminal prosecution.

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Information.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.

18. E-Discovery

To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with the Manitoba PIPITPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that Personal Information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code sets out the general rule that it is illegal to willfully intercept a private communication: “Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”.

Therefore, the organization shall ensure that the introduction and implementation of a spam-filtering solution are in compliance with the Manitoba PIPITPA (not yet in force) and the Criminal Code.
20. Cookies

There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is generally required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
1. Recent Privacy Developments

**Ontario Government Introduces New Mandatory Breach Notification Requirements Under PHIPA**

In June 2017, the Ontario government amended the Personal Health Information Protection Act (“PHIPA”) and its related regulation to require health information custodians to report certain privacy breaches to the Information and Privacy Commissioner of Ontario (“IPCO”) starting 1 October 2017. Custodians are required to notify the IPCO in the following circumstances: use or disclosure without authority, stolen information, further use or disclosure without authority after a breach, pattern of similar breaches, disciplinary action against a health regulatory college or non-college member, or significant breach. The new amendments to PHIPA also require custodians to report privacy breach statistics to the IPCO starting 1 January 2018, and provide the IPCO with an annual report of the previous calendar year’s statistics, starting in March 2019.

**Ontario Government Introduces New Privacy Legislation for Child Protection Sector**

In June 2017, the Ontario government passed the Child, Youth and Family Services Act (“CYFSA”) which expanded the IPCO’s mandate to make the child protection sector subject to access and privacy rules. The CYFSA is expected to enter into force in Spring 2018 and will require service providers such as children’s aid societies to obtain consent to collect, use and disclose personal information, report certain privacy breaches to the IPCO, and allow individuals to access and correct their personal information.

**Ontario Court Recognizes New Privacy Tort of “Public Disclosure of Private Facts”**

In a January 2016 case, the Ontario Superior Court (“ONSC”) was confronted with a particularly egregious violation of privacy colloquially referred to as “revenge porn”. The plaintiff brought an action against her ex-boyfriend after he posted a sexually explicit video of her on the internet without her consent. The ONSC recognized a new privacy tort of public disclosure of private facts, outlining the elements of the new tort as follows:

- the facts arise from the publication or publicity of a matter concerning the private life of another;
- it would be highly offensive to a reasonable person; and
• it is not a legitimate concern to the public.

In this case, the defendant was noted in default for failing to defend himself, however, the default judgment was subsequently overturned by the ONSC. The matter is still before the courts.

2. Emerging Privacy Issues and Trends

*IPCO 2016 Annual Report*

In June 2017, the IPCO released its 2016 Annual Report, calling for a number of legislative changes to enhance both access to information and protection of privacy in Ontario. The IPCO recommended that the Ontario government enact legislation that authorizes public institutions to share personal information for policy and research purposes while protecting individual privacy by establishing a government-wide framework for big data programs.

*IPCO Big Data Guidelines*

In May 2017, the IPCO released Big Data Guidelines in response to the increasing use of big data by government institutions to shape and improve government policies, programs and services. The Guidelines aim to inform government institutions of the key issues to consider and best practices to follow when they conduct big data projects. The Guidelines offer practical guidance to ensure that personal information is appropriately collected, used, retained and disclosed throughout the project.

3. Law Applicable


PHIPA establishes rules that govern the collection, use and disclosure of Personal Health Information regarding an individual (“Data Subject”) in order to protect the confidentiality of the information and the privacy of the Data Subject with respect to that information.

PHIPA applies to “health information custodians” when they collect, use or disclose Personal Health Information. Health information custodians are doctors, other health care practitioners, long-term care facilities, health care clinics, laboratories, pharmacies, the Ministry of Health and Long-Term Care as well as certain other health-related organizations. PHIPA also applies to organizations and individuals outside the health system when they receive Personal Health Information from an organization or an individual within the health system, such as employers or insurance companies. It applies to everyone with respect to the collection, use or disclosure of health insurance plan numbers of Ontario residents.
4. Scope of the Law

a. Personal Data

“Personal Health Information” means identifying information with respect to a Data Subject in oral or recorded form, whether the information relates to the physical or mental health of the Data Subject, including for example, information regarding the health history of the Data Subject’s family and the provision of health care to the Data Subject. “Identifying information” means information that identifies a Data Subject or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify a Data Subject (“Personal Information” or “Personal Data”).

Personal Health Information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if either: (i) the identifying information contained in the record relates mostly to one or more employees or agents of the custodian; or (ii) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.

b. Data Processing

“Processing” is not expressly defined in PHIPA but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of a Data Controller, including handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating and deleting Personal Information – whether on a manual or automated basis. Further, a health information custodian may use Personal Health Information about a Data Subject for the purpose of obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services.

c. Processing by Data Controllers

PHIPA governs the manner in which Personal Health Information is collected, used and disclosed within the health care system. It also regulates individuals and organizations that receive Personal Information from health care professionals.

d. Jurisdiction/Territoriality

PHIPA governs the Personal Health Information that is collected, used and disclosed in Ontario’s health care system. PIPEDA applies to all commercial activities relating to the exchange of Personal Health Information between provinces and territories and to information transfers outside of Canada. PIPEDA also applies to federally regulated commercial organizations operating in Ontario.
Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. **Sensitive Personal Data**
In determining the requisite form of consent to be obtained, organizations are required to take into account the sensitivity of the Personal Information. Personal Health Information is almost always considered sensitive; therefore it should be treated in the manner described in Section 5 below.

f. **Employee Personal Data**
Personal Health Information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if: (i) the identifying information contained in the record relates primarily to one or more employees or other agents of the custodian; or (ii) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.

5. **Consent**

a. **General**
Generally, health information custodians must obtain a Data Subject’s consent to collect, use and disclose Personal Health Information unless an exception to this requirement applies. A Data Subject’s consent may be express or implied. A Data Subject may withdraw his or her consent at any time for the collection, use or disclosure of his or her Personal Health Information by providing notice to the health information custodian.

In accordance with PHIPA, consent is valid if it is knowledgeable, voluntary, related to the information in question and given by the Data Subject. In order to meet the criteria of knowledgeable, the Data Subject must know why a health information custodian collects, uses or discloses his or her Personal Health Information and that he or she may withhold or withdraw consent.

A health information custodian is not required to obtain a Data Subject’s written or verbal consent each time Personal Health Information is used, disclosed or collected. PHIPA allows a custodian to assume implied consent where information is exchanged between custodians within the circle of care when providing direct health care unless the custodian has reason to believe that the Data Subject has expressly withdrawn or withheld their consent.

Implied consent is also acceptable if a health information custodian collects, uses or discloses names or addresses for the purpose of fundraising. Also, if the Data Subject has provided information regarding his or her religious beliefs to the health care facility, the facility may rely on implied consent to
disclose the Data Subject's name and location within the facility to a person representing his or her religious organization in certain circumstances.

Express consent is required in the following circumstances and is subject to very few exceptions: (i) where the Personal Health Information is disclosed to a Data Subject or organization, such as an insurance company if the organization is not a health information custodian; (ii) where information is disclosed from one custodian to another for a purpose other than providing or assisting in providing health care; and (iii) when a custodian:

- collects, uses or discloses Personal Health Information other than a Data Subject’s name and mailing address for the purposes of fundraising;
- collects Personal Information for marketing research or activities; and/or
- collects, uses or discloses Personal Information for research purposes, unless certain conditions are met.

When a Data Subject requests a health information custodian not to use or disclose his or her Personal Health Information to another custodian, the custodian must inform the recipient custodian that some Personal Health Information is inaccessible because it was "locked" by the Data Subject, if the custodian considers some of the locked information to be reasonably necessary for the provision of health care. However, a custodian may disclose the locked information in certain circumstances.

PHIPA generally presumes that Data Subjects are able to provide their consent to collection, use or disclosure of Personal Information when they are able to understand and appreciate the consequences of providing, withholding or withdrawing consent. However, if a health information custodian is of the opinion that a Data Subject is not able to provide consent, PHIPA allows a substitute decision-maker to make a decision on behalf of the Data Subject.

b. Sensitive Data

An organization should seek express consent from a Data Subject when Personal Health Information is involved, as health information is almost always considered sensitive. This is intended to ensure that the consent is given freely and is provided on an informed basis.

c. Minors

If the Data Subject is a child who is less than 16 years of age, a parent of the child or a children’s aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent may give consent on behalf of the child unless the information relates to: (i) treatment within the meaning of the Health Care Consent Act, 1996, about which the child has made a decision on his or her own in accordance with that Act; or (ii) counselling in which the child has participated on his or her own under the Child and Family Services Act. If
the Data Subject is a child who is less than 16 years of age and who is capable of consenting to the collection, use or disclosure of the information and if there is a person who is entitled to act as the substitute decision-maker of the child as described above, a decision of the child to give, withhold or withdraw the consent or to provide the information prevails over a conflicting decision of that person.

d. Employee Consent
All the requirements set out by PHIPA for the giving of consent by any Data Subject shall equally apply to consent given by employees covered by PHIPA.

e. Online/Electronic Consent
Electronic consent will usually suffice if appropriate steps are taken to ensure a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., an appropriately accessible hyperlink – directly above a consent button).

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) its privacy practices (which must be given in a clear and transparent way); (v) third parties to which the organization will disclose the Personal Data; (vi) the rights of the Data Subject; (vii) how the Personal Data is to be retained; (viii) where the Personal Data is to be transferred; (ix) where the Personal Data is to be stored; (x) how to access and/or correct the Data Subject’s Personal Data; and (xi) the duration of the proposed processing.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Data.
9. Registration/Notification Requirements

No formal registration requirements apply.

10. Data Protection Officers

A personal health information custodian must designate a contact person who is authorized to:

- facilitate the custodian’s compliance;
- ensure that all agents of the custodian are appropriately informed of their duties under PHIPA;
- respond to inquiries from the public about the custodian’s information practices;
- respond to requests of an individual for access to or correction of a record of Personal Health Information about the individual that is in the custody or under the control of the custodian; and
- receive complaints from the public.

Where the custodian is an individual (i.e., a natural person, not a company or an institution), the personal health custodian may act as the contact person.

11. International Data Transfers

Under PHIPA, the following restrictions apply in the case of transfers of Personal Health Information outside Ontario. A health information custodian may disclose Personal Health Information about a Data Subject collected in Ontario to a person outside Ontario only if:

- the Data Subject consents to the disclosure;
- PHIPA permits the disclosure;
- the person receiving the information performs functions comparable to the functions performed by a person to whom PHIPA would permit the custodian to disclose the information in certain prescribed circumstances;
- the following conditions are met: (i) the custodian is a prescribed entity in connection with planning the administration of the health system; (ii) the disclosure is for the purpose of health planning or health administration; (iii) the information relates to health care provided in Ontario to a person who is a resident of another province or territory in Canada; and (iv) the disclosure is made to the government of that province or territory;
- the disclosure is reasonably necessary for the provision of health care to the Data Subject, but not if the Data Subject has expressly instructed the custodian not to make the disclosure; or
• the disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the Data Subject or for contractual or legal requirements in that connection.

12. Security Requirements
An organization is required to ensure that Personal Data in its possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and must comply with sector-specific requirements.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
Subject to certain exceptions, a health information custodian that has custody or control of Personal Health Information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost or accessed by unauthorized persons. In certain cases, the custodian may also be required to notify the Information and Privacy Commissioner of Ontario.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, an administrative fine, penalty or sanction, civil actions and/or class actions, and/or a criminal prosecution.

16. Accountability
There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.
18. E-Discovery

To the extent that Personal Data is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with PHIPA. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation.

Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that Personal Information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering

Section 184(1) of the Criminal Code sets out the general rule that it is illegal to willfully intercept a private communication: “Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”.

Therefore, an organization should ensure that the introduction and implementation of a spam-filtering solution are in compliance with PHIPA and the Criminal Code.

20. Cookies

There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is generally required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Quebec, Canada

1. Recent Privacy Developments

*Update on Quebec Class Action Involving Data Breach in the United States*

In a 2015 case involving a large United States retailer, the plaintiff proposed a class action in Quebec arising from a large-scale data breach that occurred in the United States. The Superior Court of Quebec (“QCCS”) dismissed the plaintiff’s class action certification motion for lack of jurisdiction, however the Quebec Court of Appeal (“QCCA”) overturned the decision and the matter was sent back to the QCCS for re-consideration.

In 2017, the QCCS certified the class action citing reasons consistent with the QCCA’s earlier decision. That is, a number of factors, including inconvenience, loss of time and expenses dealing with issues stemming from a data breach, were potentially compensable and sufficient allegations of damages occurring in Quebec to establish jurisdiction in Quebec. However, the QCCS limited the class to Quebec residents only.

2. Emerging Privacy Issues and Trends

*Quebec Parliamentary Committee Holds Public Hearings on CAI 2016 Five-Year Report*

In August 2017, the Quebec Committee on Institutions held a general consultation and public hearings on the *Commission d’accès à l’information du Québec* (“CAI”) 2016 Five-Year Report, entitled “Restoring Balance”, concerning the application of Quebec’s public and private sector privacy laws. Key issues that were discussed in the Report and the public hearings include:

- addressing the increasing number of provincial statutes that exclude or create exceptions to the application of public and private sector privacy laws;
- introducing various measures to increase the transparency of public bodies;
- amending public and private sector privacy laws to strengthen the protection of personal information; and
- addressing various issues concerning the dissemination of open data.

3. Law Applicable

An Act respecting the protection of Personal Information in the private sector, RSQ, c P-39 (“Quebec Act”).
4. Scope of the Law

a. Personal Data

Personal Information is any information which relates to a natural person ("Data Subject") and allows that person to be identified ("Personal Information" or "Personal Data"). The Quebec Act applies to such information whatever the nature of its medium and whatever the form in which it is accessible, whether written, graphic, taped, filmed, computerized or other. However, the Quebec Act does not apply to oral disclosures of Personal Information. The Personal Information must be in an accessible recorded form. The expression of an opinion about a Data Subject is a description of that Data Subject and, therefore, qualifies as his or her Personal Information. It is the nature of the information that characterizes it as Personal Information under the Quebec Act.

The Quebec Act, which has been in force since 1994, deals with the protection of Personal Information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise. The Quebec Act applies to both natural and legal persons carrying on an enterprise.

b. Data Processing

Processing is not expressly defined in the Quebec Act but is a broad concept that encompasses an operation or set of operations performed on Personal Information pursuant to guidance or instruction of the Data Controller, including the handling, collecting, recording, disclosing, storing, correcting, amending, organizing, communicating or deleting of Personal Information – whether on a manual or automated basis.

c. Processing by Data Controllers

A "file" (which is broadly defined as a group of organized data elements in some form of media – e.g., in writing, electronic media) may only be established when there is a serious and legitimate reason for doing so. The purpose/object of a file must be determined when the file is first established. Personal Information for a file (described above) may be collected only as necessary for the object of the file.

A Data Controller cannot deny a Data Subject goods or services based only on the Data Subject’s refusal to disclose his or her Personal Information, unless:

- it is necessary for the conclusion or performance of a contract;
- it is authorized by law; or
- there are reasonable grounds to believe that the request is not lawful.
The Quebec Act expressly extends the foregoing prohibition to the employment context. An enterprise cannot refuse a Data Subject’s request for employment by reason only that the Data Subject has refused to disclose Personal Information, unless the information is necessary for determining whether the Data Subject is a suitable employment candidate.

d. Jurisdiction/Territoriality

All persons carrying on an enterprise in Quebec are subject to the Quebec Act, even if the enterprise’s head office is elsewhere. An enterprise cannot avoid the application of the Quebec Act by transferring files containing Personal Information collected, held and used in Quebec to a location outside the province.

The federal PIPEDA does not apply to those organizations in the province of Quebec that are subject to the Quebec Act with respect to their collection, use and disclosure of Personal Information within the province. PIPEDA applies to: (i) federal works, undertakings and businesses in the province of Quebec; and (ii) all transborder collections, uses and disclosures of Personal Information in the course of commercial activity.

Federal and provincial public sector privacy statutes apply to Personal Information in records held by government and other public sector entities. While these laws do not apply directly to commercial businesses, they can be relevant to private sector companies that supply or otherwise transact business with government and other public sector entities in Canada.

e. Sensitive Personal Data

The Quebec Act does not include a definition of Sensitive Personal Information.

f. Employee Personal Data

The Quebec Act does not include a definition of Employee Personal Information.

5. Consent

a. General

Consent to the communication or use of Personal Information must be manifest, free and enlightened, and must be given for a specific purpose. A consent that does not meet these requirements is without effect. A valid consent need not be in writing, but it must be precise and given for particular purposes. The Quebec Act prohibits the use of overly broad forms of consent. A new consent is required for each new purpose. While the Quebec Act does not define “manifest, free and enlightened”, these terms suggest that consent must be evident, uncoerced and informed.
An enterprise must provide Data Subjects with an opportunity to opt out of using their Personal Information for internal marketing purposes.

b. **Sensitive Data**
An organization should seek express consent when Personal Information is likely to be considered sensitive, having regard to the reasonable expectations of the Data Subject. This is intended to ensure that the consent is given freely and is provided on an informed basis. The more sensitive the Personal Information is, the greater likelihood that express consent is required for its collection, use and disclosure.

c. **Minors**
The Quebec Act does not include any unique consent requirements applicable specifically to minors.

d. **Employee Consent**
The CAI may, on written request and after consulting the professional orders concerned, grant a person authorization to receive communication of Personal Information on professionals regarding their professional activities, without the consent of the professionals concerned, if it has reasonable cause to believe:

- that the communication protects professional secrecy, especially in that it does not allow the identification of the person to whom the professional service is rendered, and does not otherwise invade the privacy of the professionals concerned;
- that the professionals concerned will be notified periodically of the intended uses and the ends contemplated and will be given a valid opportunity to refuse to allow such information to be preserved or to allow such information to be used for the intended uses or the ends contemplated; and
- that security measures have been put into place to ensure the confidentiality of Personal Information. Such authorization shall be granted in writing. It may be revoked or suspended if the CAI has reasonable cause to believe that the authorized person is not complying with the above prescriptions, the intended uses or the ends contemplated.

The authorized person may communicate such Personal Information if:

- the information is communicated in a combined form that does not allow the identification of a specific professional act performed by a professional;
- the professionals concerned are periodically given a valid opportunity to refuse to be the subject of such a communication of information; and
• the person receiving communication of such information undertakes to use the information only for the intended uses and the ends contemplated.

e. Online/Electronic Consent
The Quebec Act does not include any provisions concerning written versus electronic consents. However, electronic consent will suffice if appropriate steps are taken to ensure a Data Subject is aware of the Data Controller’s data processing practices and policies (e.g., an appropriately accessible hyperlink – directly above a consent button).

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) its privacy practices (which must be given in a clear and transparent way); (v) third parties to which the organization will disclose the Personal Data; (vi) the rights of the Data Subject; (vii) how the Personal Data is to be retained; (viii) where the Personal Data is to be transferred; (ix) where the Personal Data is to be stored; (x) how to access and/or correct the Data Subject’s Personal Data; and (xi) the duration of the proposed processing.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
An organization that collects and processes Personal Data is not required to register, file and notify the appropriate data authority.
10. Data Protection Officers
Organizations may be required to designate a privacy officer or other individual(s) who will be responsible for the privacy practices of the organization.

11. International Data Transfers
An enterprise subject to the Quebec Act, which either communicates Personal Information outside Quebec about Quebec residents or gives a person outside Quebec the authority to hold, use or communicate the information on his or her behalf, is still accountable for that information and must take all reasonable steps to ensure that the information is not used for purposes irrelevant to the object of the file, nor communicated to third parties without consent of the Data Subject to whom the information relates.

12. Security Requirements
A person carrying on an enterprise must take the security measures necessary to ensure the protection of the Personal Data collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and must comply with sector-specific requirements.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
There are no explicit security breach notification requirements in the Quebec Act. Nevertheless, an organization is generally required to take reasonable security measures to protect Personal Information under its control, and take appropriate action to address security breach situations that may arise, which action may include notification of Data Subjects, data authorities and/or other parties.

An organization that is involved in a data breach situation may be subject to: a suspension of business operations, closure or cancellation of the file, register
or database, an administrative fine, penalty or sanction, civil actions and/or class actions and/or a criminal prosecution.

16. Accountability
There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Canada provided that they are in compliance with local laws.

18. E-Discovery
To the extent that Personal Information is to be collected, used and disclosed during an e-discovery process, such activity must be in compliance with the Quebec Act. An organization should take privacy-related issues into consideration prior to the commencement and during the course of litigation. Courts will often limit the scope of e-discovery by imposing privacy-protective measures to ensure that any invasion of privacy is kept to a minimum.

Furthermore, if a third-party provider is involved in the hosting of an e-discovery system, the organization shall use contractual or other means to ensure that Personal Information and such system are protected while being processed by the third party.

19. Anti-Spam Filtering
Subsection 184(1) of the Criminal Code (Canada) (“Criminal Code”) sets out the general rule that it is illegal to wilfully intercept a private communication: “Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”.

Therefore, the organization shall ensure that the introduction and implementation of a spam-filtering solution are in compliance with the Quebec Act and the Criminal Code.

20. Cookies
There are specific laws/rules in Canada that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.
21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent is not considered valid consent.
Chile

Diego Ferrada
Santiago
Tel: +56 2 2367 7043
diego.ferrada@bakermckenzie.com

Antonio Ortuzar Jr.
Santiago
Tel: +56 2 2367 7043
antonio.ortuzar.jr@bakermckenzie.com
1. Recent Privacy Developments

The current government has rejected the idea of the “consolidated bill” and has presented for public comments an entirely new bill (the “New Bill”), which will wholly replace the current Personal Data Protection Act. The New Bill was presented to Congress in March 2017 but has not made major progress. The New Bill seeks to introduce the following main changes to the current Personal Data Protection Act:

a. The creation of a Data Protection Council, which will be in charge of enforcing the Personal Data Protection Act and will have powers to impose important fines against violators.

b. The introduction of fines for the first time, which are expected to reach USD 700,000.

c. In case of serious and repeated offenses, the prohibition of Data Controllers from processing Personal Data.

d. The New Bill will incorporate most OECD Personal Data protection principles.

e. A requirement for databases to be registered with the data protection authority.

f. There is also discussion about Personal Data of minors and Personal Data of deceased individuals.

2. Emerging Privacy Issues and Trends

With the New Bill, the Chilean government intends to bring the Chilean legislation to a higher standard. Whether or not it will become an actual law depends on the new elected government, which will come into power in March 2018.

3. Law Applicable

The Personal Data Protection Act No. 19,628 (the “Act”) came into force on 28 October 1999, and was amended by Act No. 19,812 of 13 June 2002, Act No. 20,463 of 25 October 2010 and Act No. 20,575 of 17 February 2012.

4. Key Privacy Concepts

a. **Personal Data**

“Personal Data” is defined as any information relating to identified or identifiable individuals.

b. **Data Processing**

Generally, Personal Data may be processed only when the Act or other legal provisions allow such processing, or if the Data Subject has expressly
consented after being duly informed of the collection of his/her Personal Data and the purpose thereof.

c. **Processing by Data Controllers**
The Act does not provide for a data protection authority or require that private enterprises register Data Controllers or databases. The Act is a self-assessment compliance regime and regulates the processing of Personal Data in databases (whether automated or not).

d. **Sensitive Personal Data**
“Sensitive Data” is defined as Personal Data that refers to the physical or moral characteristics of Data Subjects or to facts or circumstances of their private life such as personal habits, racial origin, political ideologies and opinions, religious beliefs, the status of their physical and mental health, and their sexual life.

e. **Employee Personal Data**
With respect to employees, the law prohibits setting as a condition for hiring the absence of negative commercial information, or to require any statement or certificate on the same. The law exempts from this prohibition the case of hiring employees who will have the authority to represent their employer (managers, agents, etc.) and those who will work in the collection, administration or custody of funds or securities.

5. **Consent**

a. **General**
Data Subjects should be informed about the purpose of the collection, processing and storage of Personal Data. According to the Act, the consent of the Data Subject should be voluntary, informed, and unambiguous, and must be in writing. Consent is not required where: (i) the Personal Data comes from sources available to the public; or (ii) the Personal Data is processed for the exclusive use and general benefit of private legal entities, their members or affiliated entities, for statistical purposes, price setting or other purpose of general benefit. Personal Data should only be used for the purposes for which it was obtained.

b. **Sensitive Data**
Sensitive Data cannot be processed except when the Act allows for such processing; the Data Subject has given consent; or the Personal Data is necessary to determine or grant medical benefits that belong to the Data Subject.

c. **Minors**
There are no specific rules for minors.
d. Employee Consent

Section 4 of the Act unambiguously requires express written consent by the Data Subject for the processing of any Personal Data. If such Data Subject is an employee of the Data Controller/Data Processor, from a practical point of view, the easiest way to obtain consent from employees is to include a special clause in the standard format of employment agreements and the company’s internal regulations. This practice ensures that all employees will provide their consent prior to the data collection.

The Data Subject must have authorized the transmission of Personal Data. Authorization to collect and process Personal Data does not serve as authorization to transmit. Therefore, special language must be included in the authorization to collect and process which explicitly sets out the intention to transmit the Personal Data. Further, the general rule in the case of Sensitive Data is that a special authorization must be provided. To satisfy such requirement, it would be advisable to alert the Data Subject in the transmission authorization that Sensitive Data could be transmitted.

e. Online/Electronic Consent

Electronic consent is permissible and can be effective if properly structured and evidenced.

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; third parties to which the organization will disclose the Personal Data; where the Personal Data is to be transferred; and the means of transmission of the Personal Data.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.
9. Registration/Notification Requirements
There are no requirements for organizations that collect and process Personal Data to register, file or notify the local data authority.

10. Data Protection Officers
There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
The Act does not contain any special restrictions on the transfer of Personal Data to third countries. The New Bill (as discussed in Section 1) intends to establish territorial restrictions.

12. Security Requirements
The Act does not contain any specific security requirements.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Generally, the party responsible for the database will remain liable for the acts of the third-party provider. The outsourcing services agreement must be in writing and must clearly indicate the scope of the services and liability of the third parties. Should the third-party provider breach the contract, it may be subject to an independent liability under the Act.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, civil actions, class actions, or private rights of action.

15. Data Security Breach
There are no specific rules addressing data security breaches. Organizations that are involved in a data breach situation may be required to gather information about the breach; take steps to mitigate the harm to impacted Data Subjects; take steps to contain the breach and prevent future similar breaches; assist authorities with any investigation relating to the breach; and comply with court orders.

An organization that is involved in a data breach situation may be subject to civil actions and/or class actions.
16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
There are no laws/rules regulating whistle-blower hotlines in Chile.

18. E-Discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of such system, the monitoring of work tools and the storage of Personal Data.

19. Anti-Spam Filtering
Generally, when a spam filtering solution is an automated process, it does not create privacy issues.

20. Cookies
The use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.
China

Nancy Leigh
Hong Kong
Tel: +852 2846 1787
nancy.leigh@bakermckenzie.com

Howard Wu
Shanghai
Tel: +86 21 6105 8538
howard.wu@bakermckenzie.com

Zhenyu Ruan
Shanghai
Tel: +86 21 6105 8577
zhenyu.ruan@bakermckenzie.com

Cathy Zhai
Shanghai
Tel: +86 21 6105 8545
cathy.zhai@bakermckenzie.com
1. Recent Privacy Developments

**Cybersecurity Law**

The Chinese legislature passed the *Cybersecurity Law* on 7 November 2016, and it came into legal effect on 1 June 2017. As China’s first law specifically regulating activities in cyberspace, the Cybersecurity Law contains a number of provisions devoted to Personal Data protection. While many of these provisions restate the Personal Data protection requirements already in place governing the telecommunications sector, the law could have a much wider scope of application – it applies to all “network operators”, which is defined broadly to include owners and administrators of computer information networks, as well as network service providers. In addition, the Cybersecurity Law introduces the concept of “Critical Information Infrastructures ("CII") and operators of CII are specifically required to store personal information and other “important data” (undefined) collected and generated during operations within China. If a CII operator seeks to store or transfer such data overseas for business reasons, it must undergo a security assessment process.

Violations of the Personal Data protection provisions may lead to the confiscation of the illegal gain and a fine of up to 10 times the illegal gain or RMB 1 million (in case there is no illegal gain), and in serious cases, suspension of business or revocation of business license. Responsible individuals may be subject to fines of up to RMB 100,000. For CII operators, unauthorized cross-border transfers of data may result in the confiscation of the illegal gain and a fine of up to RMB 500,000, as well as suspension of business or revocation of business license and a fine of up to RMB 100,000 for responsible individuals.

**Draft implementation regulations of the Cybersecurity Law**

Following the promulgation of the Cybersecurity Law, the Cybersecurity Administration of China ("CAC") released a draft of the *Measures for Security Assessment of Outbound Transmission of Personal Information and Important Data* ("Draft Security Assessment Measures") to implement the security assessment requirement under the Cybersecurity Law for cross-border data transfers. Under the Draft Security Assessment Measures, network operators (and not just CII operators) have a general obligation to assess the necessity for and security of their cross-border data transfers. In some situations, including where personal information of 500,000 or more Data Subjects is to be transferred overseas, a government-administered security assessment will be triggered.

In addition, the CAC released a draft of the Regulations for the Security Protection of Critical Information Infrastructure ("Draft CII Regulations"). Once finalized, the Draft CII Regulations should provide more detailed guidance on
the scope of CII operators. According to the current draft, further CII identification guidelines and industry-specific guidelines will also be issued.

All of the draft regulations mentioned above are still under deliberation by the Chinese government, and are expected to be issued within a 12-month time period from 1 June 2017. Furthermore, according to an official statement made by the CAC, the security assessment regime will not be implemented until 31 December 2018.

General Provisions of the Civil Law

The General Provisions of the Civil Law of the People’s Republic of China were promulgated on 15 March 2017 and became effective on 1 October 2017. The General Provisions of the Civil Law formally recognize the right to one’s personal information as a civil right. Each organization or individual must obtain the personal information of another person through legitimate means and ensure the security of such personal information. No one (whether an organization or an individual) is allowed to illegally collect, use, process, transmit, purchase, sell, provide or publish personal information of another person.

As such, the General Provisions of the Civil Law have established a private right of action for infringement of one’s right to personal information. The infringed party may seek compensation for actual losses (or profits arising from the infringement if actual losses cannot be determined) and where applicable, damages for emotional distress, in addition to other remedies provided under the law (e.g., cessation of infringement, return of property, apology from the infringer, restoration of reputation, etc.).

Clarification on scope and liabilities of the criminal offense of infringement of personal information

On 9 May 2017, the Supreme People’s Court and the Supreme People’s Procuratorate of China issued the Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens’ Personal Information (“Judicial Interpretation”), which became effective on 1 June 2017. The Judicial Interpretation clarifies the scope and liabilities of the criminal offense of infringement of personal information under the Criminal Law. Most notably, the Judicial Interpretation provides: (i) a detailed definition of “personal information”, which appears broader than the one stipulated under the Cybersecurity Law; (ii) specific examples of illegal use and disclosure of personal information punishable by the Criminal Law; and (iii) criteria for the imposition of criminal penalties.

2. Emerging Privacy Issues and Trends

2017 has witnessed the passage of several legislative milestones in China. These demonstrate the Chinese government’s ongoing focus on protecting
personal information and data security through the use of civil, administrative and criminal sanctions.

The provisions of the Cybersecurity Law and the General Provisions of the Civil Law contain broad terms which are subject to further clarification and interpretation. Business operators are advised to closely monitor relevant legislative developments and undertake further analysis as and when the implementation regulations and judicial interpretations are issued.

3. Law Applicable

While there is wide recognition in China of the need to protect privacy, as of yet there is no specific legislation for the protection of Personal Data or privacy in China.

The General Principles of the Civil Code of the People’s Republic of China (effective as of 1 January 1987), the Opinion of the Supreme People’s Court on Several Problems in the Implementation of the General Principles of the Civil Code (issued in 1988 and revised in 1990), and the Answers of the Supreme People’s Court to Several Questions on Trying Cases Concerning the Right to Reputation (effective on 7 August 1993) (collectively the “Opinions”) address several issues relating to “privacy”.

This changed when the Law of the People’s Republic of China on Tortious Liability (the “Tortious Liability Law”) came into effect on 1 July 2010 and privacy rights were formally recognized as a form of civil rights and interests.

Under the current legal framework, the following laws and regulations are also relevant to privacy protection:

- the General Provisions of the Civil Law of the People’s Republic of China, promulgated on 15 March 2017 and effective on 1 October 2017;
- the Cybersecurity Law, promulgated on 7 November 2016 and effective on 1 June 2017;
- the Criminal Law, as amended by its Ninth Amendment and effective on 1 November 2015;
- the Decision on Strengthening the Protection of Network Information, passed by the Standing Committee of the National People’s Congress on 28 December 2012;
- the amended Consumer Protection Law, effective from 15 March 2014; and
- industry-specific regulations governing telecommunications, banking, insurance, real estate brokerage, post and courier, health and other sectors (collectively, the “Data Protection Regulations”).
4. Key Privacy Concepts

a. Personal Data

There is no uniform definition of “Personal Data” under the Data Protection Regulations. The scope of Personal Data varies among different Data Protection Regulations.

Examples of privacy and personal information given by the Supreme People’s Court include genetic information, medical history, medical check-up records, criminal records, home address and private activities of a natural person.

Following the amendments to the Consumer Protection Law, the State Administration for Industry and Commerce promulgated the Measures for Punishments against Infringements of Consumer Rights and Interests ("Measures"), which came into effect on 15 March 2015. The Measures define “consumer personal information” as “information collected by a business operator during the provision of goods or services that may, independently or in combination with other information, ascertain the identity of a consumer such as the consumer’s name, gender, occupation, date of birth, identity document number, residential address, contact details, income and financial position, health information, and consumption habits, etc”.

The scope of Personal Data in the context of cybersecurity laws and regulations typically includes the name, birth date, identity document number, residential address, phone number, account number and password, activity log, etc. of internet users collected by telecommunications and internet service providers.

Industry-specific regulations typically set out their own definitions of “personal information” that is protected under the regulations. Although the definitions of Personal Data tend to be sector specific, what they have in common is the general principle that any information that alone or in combination with other information may identify an individual can be regarded as Personal Data.

b. Data Processing

The Cybersecurity Law stipulates the general principles of legitimacy, reasonableness and necessity for collecting and processing Personal Data by network operators (as very broadly defined). More specifically, when collecting and processing Personal Data, a network operator must:

- explicitly inform the Data Subjects of the purposes, scope and manner of data collection and use, and must obtain the Data Subjects’ consent to the same;
- only collect and use the Personal Data collected in compliance with the law and as agreed with the Data Subjects;
• keep the Personal Data collected strictly confidential, and must not disclose, tamper with, damage, sell or unlawfully provide the same to a third party;

• refrain from collecting Personal Data which is not relevant to the services it provides to the Data Subjects; and

• adopt technical and other necessary measures to ensure that the data is secure, and must take remedial steps immediately where data disclosure, damage or loss occurs or may occur.

There are very similar provisions under the amended Consumer Protection Law, which impose obligations on business operators that provide goods or services to PRC consumers. Furthermore, under the Consumer Protection Law, business operators may not send commercial messages to a recipient’s email address, landline or mobile number without the recipient’s consent or request, or where the recipient has not expressly declined the receipt of the same.

Industry-specific regulations raise additional considerations with respect to data privacy in the relevant service sectors (e.g., telecommunications, insurance, post and courier, health, etc.). For instance, banking institutions in China must comply with the relevant rules issued by the China Banking Regulatory Commission in respect of cross-border transfer of Personal Data. Another example is that medical institutions in China are not allowed to store population health data (such as electronic medical records of patients) on servers located outside China.

A business operator is also advised to check the relevant industry-specific regulations and guidelines for specific requirements or recommendations on data processing.

c. Processing by Data Controllers
See Section 4(b) above. No distinction has been drawn between a Data Controller and any other user/processor of Personal Data.

d. Jurisdiction/Territoriality
Chinese laws and regulations concerning Personal Data protection and security do not have any extraterritorial effect.

e. Sensitive Personal Data
No such term is defined under current Chinese laws and regulations.

In the absence of clear legal guidance, the General Administration of Quality Supervision, Inspection and Quarantine and the State Standards Commission published non-binding guidelines, i.e., Information Security Technology Guidelines for Personal Information Protection within Information System for
Public and Commercial Services (the “Personal Information Protection Guidelines”), which define sensitive personal information as an individual’s personal information that may have adverse effects on the individual once it is leaked or modified. Examples of sensitive personal information include identification numbers, mobile phone numbers, racial or ethnic origin, political opinions, religious beliefs, DNA and fingerprints.

Please note that the Personal Information Protection Guidelines are not mandatory, and are for the relevant industry players’ reference only and have no legally binding effect.

f. Employee Personal Data

The Administrative Regulations for Employment Services and Employment (effective as of 1 January 2008) (the “Employment Management Regulations”) use the term “Personal Data”, but this term is not further defined in the regulations.

Although there is no definition under Chinese law of “Employee Personal Data”, general rules governing record retention of enterprises refer to special retention and local government/trade union consent requirements for documents and materials that arise from the operation and management of an enterprise whose preservation is of “value to the State, society and the enterprise”. Discussions with selected government officials indicate that such materials could include the Personal Data of employees, and it is recommended that local authorities be consulted regarding certain categories of data (e.g., health records, disciplinary actions, pensions, social security information, etc.).

5. Consent Requirements

a. General

Under the Cybersecurity Law, network operators (as very broadly defined) must obtain the consent of Data Subjects for the collection and use of their Personal Data. Under the amended Consumer Protection Law, the collection and use of consumer Personal Data, and the sending of unsolicited commercial messages are subject to consumer consent.

b. Sensitive Data

Chinese law does not explicitly distinguish between personal information and sensitive personal information.

c. Minors

The Law of the PRC on the Protection of Minors (effective from 1 June 2007) provides that no person may disclose the private matters of PRC citizens under the age of 18. There is no guidance on the application of the requirements, however, and the general view is that the collection and lawful
use of the Personal Data of minors with the consent of their parents or guardians is acceptable.

d. **Employee Consent**

Under the Employment Management Regulations, employers should keep their Employee Personal Data confidential, and must obtain an employee’s written consent before publicizing his or her Personal Data.

In addition, if an employer has formulated a data processing policy, and such policy forms part of the employer’s company rules, the employer is required to consult the employees through the trade union, the employee representatives’ congress or other means.

e. **Online/Electronic Consent**

Electronic signatures are valid under PRC law. In addition, data messages shall be deemed to be written and original documents if their contents can be exhibited in tangible form, be retrieved and be consulted, and if it can be verified that their contents have maintained their integrity without modification since their finalization. Though PRC law provides that the use of a data message as evidence may not be refused solely on the grounds of its creation, sending, receipt or storage in electronic form, in practice, it is generally much more difficult to submit an electronic contract/data message as evidence as opposed to a hard copy signature.

6. **Information/Notice Requirements**

Under the Cybersecurity Law, Data Subjects should be informed of the purpose, scope and manner of data collection and use of Personal Data.

Similar requirements are imposed pursuant to various industry-specific Data Protection Regulations. In the telecommunications and internet sector, the relevant Data Protection Regulations further require telecommunications operators and ISPs to advise users of the ways to inquire or correct information, as well as the consequences of refusal to provide such information.

7. **Processing Rules**

A business operator is advised to check the relevant industry-specific Data Protection Regulations for specific rules or recommendations on data processing. Please also refer to Section 4(b) above and Section 13 below.

8. **Rights of Individuals**

Under the Tortious Liability Law, “civil rights and interests” of natural and legal persons are protected, where the term “civil rights and interests” is broadly defined to include, among other things, the right to one’s name, reputation, honor, image and privacy. Further, the General Provisions of the Civil Law
formally recognize the right to one’s personal information as a civil right which shall be protected by law. A person whose civil rights and interests have been infringed has the right to demand that the infringer bear tortious liability by ceasing the perpetration of the act, returning property or restoring it to the original state, paying compensation for loss, making an apology and/or elimination of the effect and restoration of reputation.

Under the Cybersecurity Law, network operators that collect and use Personal Data in their business operations must expressly inform the Data Subjects of the purposes, scope and manner of data collection and use and obtain their consent to the same.

Similar requirements are imposed under various sector-specific Data Protection Regulations. In the telecommunications and internet sector, the relevant Data Protection Regulations also require telecommunications operators and ISPs to inform Data Subjects of the channels through which they may make data access and correction requests, and lodge data privacy complaints.

9. Registration/Notification Requirements

See Section 15 below. The Cybersecurity Law imposes a general data breach notification obligation on all network operators. In addition, if an information safety incident (such as a massive data breach) occurs, the affected entity is generally required to report the incident to the industry regulator.

10. Data Protection Officers

No specific requirements apply. However, the Cybersecurity Law requires network operators to designate personnel to be responsible for cybersecurity-related compliance work.

11. International Data Transfers

Transfers of Personal Data out of China are generally permitted so long as the consent of the Data Subject has been obtained. However, there are restrictions on certain types of entities for transfer of Personal Data or other information to places outside of China.

Under the Cybersecurity Law, CII operators are required to store personal information and other “important data” collected and generated during operations in China within the territory of China. If truly necessary for business reasons, the CII operator needs to provide such information or data overseas, it must undergo a security assessment process. CII is defined broadly as “infrastructure that, in the event of damage, loss of function, or data leakage, might seriously endanger national security, national welfare or the livelihood of the people, or public interest”, and specific reference is made to key sectors such as public communications and information services, energy,
transportation, water resources, financial services, public services and e-government. The exact scope of CII operators is not entirely clear under the Cybersecurity Law, and it is expected to be further clarified in implementation regulations issued by the Chinese government.

Certain industry sectors are also subject to specific restrictions. For example, according to rules issued by the People’s Bank of China, personal financial information collected within China must be stored, processed and analyzed in China unless otherwise exempted. Similarly, medical and health institutions are prohibited from storing "population health information" on overseas servers.

Selected regulations also suggest that local government authorities in charge of archives should be consulted before the implementation of international data transfers.

Furthermore, production, reproduction, access and dissemination (including by means of cross-border transfer) of prohibited information is strictly forbidden under Chinese law. Prohibited information generally includes information which may harm the interests of the State, cause social instability or infringe another person’s rights.

12. Security Requirements

The Cybersecurity Law requires that network operators adopt technical and other necessary measures to ensure that the data collected is secure, and take remedial steps immediately where data disclosure, damage or loss occurs or may occur. The Consumer Protection Law also imposes similar obligations on business operators that provide goods or services to PRC consumers.

Certain industry-specific regulations contain detailed security requirements. For example, the Regulations on Telecommunications and Internet User Personal Data Protection impose specific security requirements on telecommunications business operators and internet service providers.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

The consent of Data Subjects is required for data outsourcing arrangements with third parties. Certain sectors such as the financial sector may impose specific requirements.

14. Enforcement and Sanctions

Any infringement of privacy rights (as described in Section 4 above) will give rise to claims for injunctive relief and compensatory damages under the Tortious Liability Law.
Administrative penalties (e.g., issuing a warning, confiscating illegal income, imposing a fine, revoking a business license, etc.) may be imposed for violation of the data privacy requirements set out in the Cybersecurity Law.

In serious cases, the above-mentioned activities may amount to a violation of the Law of the PRC on the Imposition of Penalties in Connection of the Administration of Law and Order (effective from 1 March 2006) (the “Penalties Law”). The Penalties Law is applicable to cases where the circumstances are not serious enough to amount to a crime but the administrative penalties are insufficient. Penalties imposed by the Public Security Bureaus under the Penalties Law include detention of up to 20 days.

Under the Amendment to Criminal Law:

- anyone who unlawfully sells or provides personal information to third parties and causes serious results may be sentenced to up to three years of imprisonment or criminal detention and/or subject to a fine in serious cases, or be sentenced to three to seven years of imprisonment and/or subject to a fine in very serious cases;

- anyone who unlawfully sells or provides to third parties the personal information acquired in the course of providing the relevant services or fulfilling his or her duties and causes serious results shall be sentenced to three to seven years of imprisonment and/or subject to a fine in serious cases;

- for those stealing or illegally obtaining the aforesaid information, the same sanctions above will apply; and

- if any of the above offenses is committed by an organization, it will be subject to a fine and all management and officers who are directly responsible will be subject to the sanctions stated above.

15. Data Security Breach

The Cybersecurity Law imposes a general obligation on all network operators to promptly notify Data Subjects and the relevant authorities in the event of a data breach. However, the Cybersecurity Law does not provide further detail on the notification requirement. Actual enforcement of such data breach notification requirement will be dependent on implementation legislation that is yet to be issued.

There are also a number of “information safety/security” regulations, which were promulgated, not particularly for the protection of Personal Data, but more out of concern for preserving State secrets and preventing data loss and business disruption which are considered harmful to the “public interest” in general. In that regard, government organizations and sensitive industries are required to install security systems, take preventive measures, and when any
“information safety/security incident” occurs, report in a timely manner to the authorities and take emergency measures.

“Information safety incidents” is a very broad concept, and generally covers all malicious attacks, equipment malfunctions or natural disasters which result in a massive breakdown of an information system and/or data loss or theft (it is a broader concept than that of “security breach”). These regulations do not include specific requirements for notifying the affected individuals, as they were drafted mainly from the perspective of State supervision and maintenance of order, instead of mitigating the impact on individuals.

In addition, there are industry-specific regulations that impose special duties on certain types of data carriers, including telecommunications service providers as well as companies in the financial and securities industries.

Failure to comply with the notification requirements as discussed above may lead to investigations and queries from the relevant authority and ultimately result in the imposition of administrative penalties.

16. Accountability
An organization has no legal obligation to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. That being said, under the Cybersecurity Law, network operators may need to undergo a security assessment or approval process (details of which are not available yet and are subject to further legislation) for cross-border transfer of Personal Data and other important data.

17. Whistle-Blower Hotline
There are no laws/rules that govern whistle-blower hotlines in China.

18. E-Discovery System
The implementation of an e-discovery system within an organization will not specifically raise any privacy issues in China.

19. Anti-Spam Filter
The introduction of a spam-filtering solution in an organization will not raise privacy issues in China.

20. Cookies
There is no specific law/rule that governs the use and deployment of cookies in China.
21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent.

Under the amended Consumer Protection Law and the amended Advertising Law, a business operator is prohibited from sending unsolicited commercial information to consumers who have not consented to receiving such information or who have expressly refused to receive the same.
Colombia

Sandra Castillo
Bogota
Tel: +57 1 644 9595 Ext. 2756
sandra.castillo@bakermckenzie.com

Carolina Pardo
Bogota
Tel: +57 1 644 9595 Ext. 2603
carolina.pardo@bakermckenzie.com
1. Recent Privacy Developments

_Adequacy for the cross-border transfer of Personal Data_

On 10 August 2017, the Colombian data protection authority, the Superintendence of Industry and Commerce (SIC), published External Circular number 5 of 2017 ("Circular No. 5"). Circular No. 5 which:

- establishes the standards with which a country must comply for it to have adequate levels of protection to receive Personal Data transferred from Colombia.

- includes an initial list of countries that comply with such standards.

- provides for some alternatives for the cross-border transfer of Personal Data to countries that do not meet the required adequate levels of protection.

_Standards to determine if a country has adequate levels of protection_

In accordance with the provisions of Circular No. 5, a country shall be deemed to offer adequate levels of protection for the transfer of Personal Data of individuals residing in Colombia, if it meets all of the following criteria:

- Existence of rules applicable to the processing of Personal Data.

- Express inclusion in the country’s rules and laws, of principles applicable to data processing, in others: legality, purpose, freedom, veracity or quality, transparency, access and restricted circulation, security and confidentiality.

- Express inclusion in the country’s rules and laws, of rights of the Data Subjects.

- Express inclusion in the country’s rules and laws, of duties of the Data Controllers and Processors.

- Existence of judicial and administrative means and channels to guarantee the effective protection of the rights of the Data Subjects and law enforcement.

- Existence of public authority or authorities responsible for the supervision of the processing of Personal Data, enforcement of applicable legislation and the protection of the rights of Data Subjects, effectively exercising its/their functions.
Initial list of countries considered to have adequate levels of protection for international transfers of Personal Data

The following countries have been included in the initial list of jurisdictions considered by the SIC to have adequate levels of protection for international transfers of Personal Data, based on the criteria listed above:

Germany; Austria; Belgium; Bulgaria; Cyprus; Costa Rica; Croatia; Denmark; Slovakia; Slovenia; Estonia; Spain; United States of America; Finland; France; Greece; Hungary; Ireland; Iceland; Italy; Latvia; Lithuania; Luxembourg; Malta; Mexico; Norway; Netherlands; Peru; Poland; Portugal; United Kingdom; Czech Republic; Republic of Korea; Romania; Serbia; Sweden; and countries that have been declared with adequate level of protection by the European Commission.

Circular No. 5 stresses that, even though a country is included in the list of adequate jurisdictions, Data Controllers must be able to demonstrate to the SIC that they have taken effective measures to properly process Personal Data in a responsible manner, applying the accountability principle, which is expressly developed in the Colombian data protection legislation.

International transfers of Personal Data to countries that do not have adequate levels of protection

Circular No. 5 reiterates alternatives to lawfully transfer Personal Data even to jurisdictions not listed as adequate. These are already provided in the Law and consist of obtaining prior, express and informed consent and situations in which ulterior rights such as life and health of Data Subject (among others) allow for data transfers without consent or to jurisdictions not listed as adequate.

Circular No. 5 also refers to the possibility of obtaining declarations of conformity from the SIC for specific cross-border transfer projects on a case by case basis, for which the Data Controller must file a petition with the SIC providing the information and documentation described in the “Guide to Requesting the Declaration of Conformity on International Transfers of Personal Data”.

Finally, Circular No. 5 includes a novelty consisting in that if the Data Controller enters transfer agreements or other legal instruments that encompass the conditions ruling the transfer and the principles ruling the processing, it shall be presumed that the transfer is valid. This alternative will require that the Data Controller submits a notification of the transfer to the SIC and acknowledges that an agreement has been subscribed and leaves to SIC the discretion to initiate an investigation if said entity verifies that Colombian data protection laws are being breached as a result of the transfer.
The Circular, which issuance process and initial drafts were very controversial, represents a groundbreaking development in Colombian data protection laws, which facilitates the cross-border transfers of Personal Data to certain countries but also calls for a more active application of the accountability principle by Data Controllers.

2. Emerging Privacy Issues and Trends

The enforcement of Colombian Data Protection Laws remains very focused on requirements of express consent. Pursuant to Article 9 of Law 1581, the processing of any Personal Data – not just sensitive data – requires prior, express and informed consent from the Data Subject, which must be obtained by means that can be subsequently consulted. In furtherance of this provision, the secondary regulation issued by the Colombian government provides that valid consent can be granted by the Data Subject through unequivocal behaviors that lead to the reasonable conclusion that authorization was granted. With the increase of e-commerce activity in Colombia, it is expected that some cases related to the interpretation of the law on consent granted through unequivocal behaviors may be discussed in the near future.

Another aspect which will probably result in increased enforcement actions is the deadline of 8 November 2016 for controllers to register databases in the NDR. The information included in such registry should provide the DPA with information that allows it to monitor the processing of Personal Data. Such registry is also the mechanism through which data breaches must be reported to the DPA in Colombia.

Some of the highlights of Decree 1377 of 2013 (“Decree 1377”), supplementary regulation of Law 1581, include the following:

- Decree 1377 introduces the concept of “transmission”, which differs from that of “transfer”. The transfer of Personal Data requires prior, express and informed consent of the Data Subject (unless said transfer is subject to the exceptions provided by Law 1581). On the other hand, transmission is understood as the circulation of Personal Data from Data Controllers to Data Processors. Transmissions will no longer require prior and informed consent of the Data Subjects if the Data Controller and the Data Processor enter into a transmission agreement. Furthermore, the transmission will be upheld if the parties sharing the data have all adhered to the same privacy policy accepted by the Data Subjects.

- Decree 1377 also develops the concept of “prior, express and informed consent” – See Section 5(a).

- Processing of Personal Data of minors – See Section 5(c).

- Decree 1377 introduces the concepts of “privacy policy” and “privacy notice” – See Section 6.
- Obligation of Data Controllers and Data Processors to appoint a Data Protection Officer – See Section 10.
- Data breach obligations – See Section 15.
- Introduction of the accountability principle – See Section 16.
- Do not call approaches and developments – See Section 21.

3. Law Applicable and Data Protection Authorities

a. Law Applicable

The Colombian Constitution introduced the fundamental right to habeas data, which is the right that every person has to self-determine the collection, use, storage, processing and transfer of his or her Personal Data, granting it special protection.

The Constitution mandates that the protection of fundamental rights must be detailed and ratified by one or more Statutory Laws. Statutory Laws require absolute majorities and a special proceeding within the Colombian Congress to be approved, and must be signed into law by the President before they come into force.

In Colombia, the protection of the habeas data right is currently based on the provisions of the Constitution, and the following laws that regulate the right:

- Statutory Law 1581 of 2012, which regulates privacy rights in respect of Personal Data collected and processed in any type of database (“Law 1581”).
- Statutory Law 1266 of 2008, which regulates data privacy rights related to commercial and financial data for credit rating purposes (“Law 1266”).
- Statutory Law 1273 of 2009, which provides that certain actions undertaken in managing and processing Personal Data are inappropriate and qualify as felonies under the Colombian Criminal Code (“Law 1273”).

The abovementioned statutes have been subject to interpretation by the Constitutional Court (the “Constitutional Rulings”). These Constitutional Rulings should be referred to in clarifying and understanding the context and rights under the relevant statutes.

Although data protection rules are generally applicable across all databases, the SIC, the Ministry of Communications and Information Technology, and the Ministry of Commerce, Industry and Tourism, issued a supplementary regulation through Decree 1377, to develop further specific issues already covered by Law 1581 and more recently, Decree 866 in relation to the National Database Registry.
4. Key Privacy Concepts

a. Personal Data

Law 1266 regulates the collection, processing, storage, transfer and use of Personal Data related to credit rating activities. This Law defines Personal Data as any piece of information linked to one or more identifiable individuals or legal entities or to information which may be associated with a certain individual or legal entity.

Under Law 1266, Personal Data is classified into three different categories: (i) private data, which has a reserved and intimate nature that concerns a Data Subject; (ii) semi-private data, which is data that refers to an individual or person and is required by third parties (e.g., financial entities) to make certain assessments with respect to a person; and (iii) public data, which refers to information of a determined person, that has been validly recorded in public registries, judicial rulings or public documents, and all other data that is not private or semi-private in nature.

On the other hand, Law 1581 provides for a general framework related to the protection of data privacy rights. Hence, this Law regulates the collection, processing, storage, transfer and use of Personal Data, when such treatment occurs in any database in Colombia or with respect to Data Subjects domiciled in Colombia, where such data is susceptible to treatment by public or private entities.

Law 1581 only applies to individuals. According to the Constitutional Ruling of 2011, Law 1581 could apply to the protection of data privacy rights of legal entities when there is an infringement to the rights of individuals who are part of such entity.

For the purpose of this document, “Personal Data” and “Data Subject” should be understood as defined in Law 1581, unless otherwise stated or when specifically making reference to Law 1266.

According to the Rulings of the Constitutional Court referring to Law 1581 and Law 1266, the right of a person to authorize the processing of his Personal Data is not transferable. However, Law 1581 makes reference to some cases where a legal representative or a third party representing the Data Subject can validly grant consent. This is the case, for example, when the life or health of the Data Subject is at risk.

b. Data Processing

Law 1581 defines Data Controller as “an individual or legal entity, public or private, that either alone or in association with others, decides over the data base and/or on processing of the data” and Data Processor as “an individual or legal entity, public or private, that either alone or in association with others, processes Personal Data on behalf of the Data Controller”. Any processing of
Personal Data governed under Law 1581 has to be done in accordance with the obligations that Data Controllers and Data Processors have under said Law.

According to the Constitutional Ruling of 2011, Law 1581 is applicable to residents in the territory of Colombia. It is also applicable to processing that takes place outside of Colombia but in relation to residents within the Colombian territory. This is especially relevant to cloud computing and online processing of Personal Data.

c. Processing by Data Controllers

A Data Controller or information operator can only process Personal Data within the scope of the prior, express and informed consent granted by the Data Subject, unless one of the exceptions established in Law 1581 or in Law 1266 applies.

According to Law 1266, prior, express and informed consent is required to report credit history of individuals and legal entities to financial databases. The databases are subject to registration and rules relating to the management of the data and the publication of reports regarding such credit history. Failure to abide by such rules, triggers fines and sanctions.

According to Law 1581, prior and informed consent of the Data Subject will be required except for the following circumstances:

- when the processing is authorized by a Law for historic, statistical, scientific, or other purposes;
- when the information is of a public nature;
- when the information is required by a government authority exercising its duties, as explicitly conferred by law;
- when the circulation of Personal Information is necessary in the event of a medical or sanitary emergency; and
- information regarding the civil registry.

d. Jurisdiction/Territoriality

Law 1266 applies equally to individuals and legal entities, in connection with data privacy rights related to credit rating activities in Colombia or related to Colombian persons.

Law 1581 establishes that its provisions are applicable to Data Subjects in the following cases:

- all data processing carried out in Colombia; and
• all data processing carried out abroad but performed by a Data Processor or Data Controller whose acts are ruled by Colombian provisions according to international treaties. This means that activities of a Data Processor or a Data Controller that refer to individuals domiciled in Colombia, are subject to the provisions of Law 1581.

e. Sensitive Personal Data
The concept of Sensitive Personal Data includes, but is not limited to, any racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual preferences or habits and behavior. In general, Law 1581 defines Sensitive Personal Data as that which can affect the privacy of the Data Subject or the misuse of which can lead to discrimination.

f. Employee Personal Data
Employees’ Personal Data is likely to include Sensitive Personal Data (e.g., health-related information) and non-Sensitive Personal Data.

Employees’ Sensitive Personal Data should be processed in accordance with the applicable laws mentioned in Section 4(e) and the Constitutional Rulings.

5. Consent
a. General
Under Law 1581, any collection, use, transfer, storage and processing of Personal Data requires prior, express and informed consent from the Data Subject, except as provided for in Section 4(c).

In the Constitutional Ruling of 2011, the court stated that consent can be granted through a "specific indication". Hence it is possible to consider that an affirmative action will be construed as express consent, and thus if the elements of a prior and informed authorization from a Data Subject are also met, this should amount to adequate consent. In many Constitutional Rulings and, in particular, the Constitutional Ruling of 2011, the Court has confirmed that silence, tacit consent and blanket consents are not acceptable.

Data Subjects have the right to revoke or request the suppression of their Personal Data at any time, except for certain instances in which the Data Controller must preserve the Personal Data (i.e., fraud prevention, etc.)

b. Sensitive Data
Law 1581 specifically establishes that processing of Sensitive Personal Data is unlawful unless the Data Subject has given his or her explicit consent or the processing is within the following exceptions:

• the processing is necessary to protect the life and health of the Data Subject and he or she is not legally or physically able to express his or
her consent (in these cases, their representative must grant the authorization);

- if the processing corresponds to legitimate activities carried out with the appropriate guarantees by foundations, NGOs, associations or any other non-profit organization with a political, philosophical, religious or trade union purpose, if such data processing is only related to the members of the association or persons with whom the association is in recurrent contact because of its objective (in these events, the data may not be provided to third parties without the permission of the Data Subject);

- the processing refers to data that is necessary for the recognition, exercise or defense of a right under a judicial proceeding; and

- the processing has a historical, statistical or scientific purpose (in this event, measures must be taken for suppression of the Data Subject can be identified).

c. Minors

Minors are children and adolescents under the age of 18. In the Constitutional Ruling of 2011, the Court brought up the definition of minor from the Code of Infancy and Adolescents, indicating that for purposes of Law 1581, children are individuals between 0 and 12 years old and adolescents are individuals between 12 and 18 years old.

However, the Constitutional Ruling of 2011 established that the prohibition of the processing of data of Minors does not apply when such processing of data guarantees that the fundamental rights of Children and Adolescents will be safeguarded, which implies that any processing of Personal Data of Minors should strictly comply with the Constitution and Law 1581, and other provisions as applicable.

Although Law 1581 does not contemplate explicitly the need for consent from minors, the Constitutional Ruling of 2011 has included some guidelines that must be followed for the processing of minors’ Personal Data to be lawful: (i) the treatment shall respond to and comply with the highest interests of the children and adolescents; (ii) it shall be compliant with the minors’ constitutional rights; and (iii) as far as possible, the treatment shall be made taking into account the opinion of the minor to whom the Personal Data refers, in consideration of their maturity, autonomy and capacity to understand the situation referred to such processing of their Personal Data and the consequences that this entails. The evaluation of these factors must be made on a case-by-case basis. These guidelines inspired Article 12 of Decree 1377 and, therefore, they are no longer mere guidelines but current regulation that must be followed whenever the processing of data of minors is required.
d. Employee Consent

Law 1581 and Decree 1377 do not provide for a specific provision on the requirements to implement monitoring mechanisms on employees (i.e., through their computers, surveillance cameras, telephones and cellphones, among others). However, multiple Constitutional Rulings have established that the employer should seek prior, express and informed consent from employees to collect and process their Personal Data through such monitoring devices, even though the devices belong to the company.

In addition, in Colombia, employee consent is required when implementing a “Bring Your Own Device” program in the workplace.

e. Online/Electronic Consent

Consent can be obtained electronically since electronic contracts are valid and binding in Colombia. The foregoing is based on the rules established in Law 527 of 1999 (“Law 527”), which indicate that unless otherwise required by law, the parties are free to enter into any contract by any means and express their will to bind themselves in any way they choose and to the extent permitted by law. Electronic messages have the same legal effects as written documents and therefore in principle they can replace the requirement of the written document as per Law 527.

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

Decree 1377 introduces the concept of a “privacy policy” and the obligation of its implementation by Data Controllers. It also specifies the content required to appear in the said policy. In addition, Decree 1377 states that a “privacy notice”, which contains the organization’s “privacy policy”, should be made available, especially in cases where information of said policy cannot be provided to the Data Subject. In any case, the privacy notice must contain a link or a reference indicating where to access and consult the privacy policy. Decree 1377 provides a description of the information that the privacy notice must contain.
7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met. One of the obligations that Data Controllers and Processors have is to adopt an internal manual of policies and procedures that are followed to guarantee that the provisions contained in Law 1581 and its applicable regulations, are effectively followed.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

Law 1581 created the National Database Registry (the “NDR”), which is a public list of databases operating in Colombia. The registration of the databases will be administered by the SIC and specifically by the DPA.

On 12 May 2014, the Colombian government issued Decree 886, which regulates Article 25 of Law 1581 on the creation of the NDR.

Decree 886 extensively regulates the obligation that Data Controllers have under Article 25 of Law 1581 of 2012 to record with the NDR, information on certain characteristics of their databases containing Personal Data and which processing is subject to Colombian laws.

External Circular No. 002 of 2015, issued by the DPA, provided that as of 9 November 2015, all entities incorporated in Colombia and registered with the local Chambers of Commerce that act as Data Controllers, must record certain aspects of how they process Personal Data in each of the databases they control, before the NDR, managed by the DPA.

The main highlights of Decree 886 include:

- **No recordal of the database itself.** Decree 886 does not require the recordal of the database itself. The purpose of the NDR is more focused on informing Data Subjects and the SIC of the databases that Data Controllers have and the conditions on which Data Controllers process Personal Data.
• **Separate filings must be made per database.** Data Controllers will have to make separate filings with the NDR for each database in which they hold Personal Data that they collect and process.

• **Database information that must be recorded with the NDR.** For each database that is recorded with the NDR, Decree 866 requires specific information and documentation to be detailed and uploaded.

In accordance with Decree 886, the following information must be submitted when recording each database with the NDR:

- identification information, location and contact information of the Database Controller;
- identification information, location and contact information of the Database Processor or Processors;
- channels through which the Data Subjects may exercise their rights;
- name and purpose of the database;
- form of processing of the database (manual and/or automated); and
- policy for the processing of Personal Data.

Additionally, with the External Circular No. 002 of 2015, entities that act as Data Controllers shall record the following information before the NDR:

- information stored in the databases;
- respond affirmatively or negatively to whether certain security measures for protecting the information have been implemented;
- origin of the Personal Data;
- information related to the international transfer of Personal Data;
- information related to the international transmission of Personal Data; and
- information related to the assignment of databases.

Likewise, External Circular No. 002 of 2015 establishes the permanent obligation of maintaining the NDR updated with any modification of the aforementioned information. The same platform was enhanced in order to allow for the recording of all the complaints submitted by the Data Subjects and for the fulfillment of the obligation of reporting data breaches over the databases in which Personal Data is stored. As of 9 November 2015, access to the NDR was made publicly available for Data Subjects to consult the registries made by Data Controllers in the platform.
Failure to comply with the obligation of recording databases with the NDR may trigger the same sanctions for breach of other obligations under Law 1581.

10. Data Protection Officers
Organizations are required to designate a privacy officer or individual who will be responsible for the privacy practices of the organization. The duties of this officer can be exercised either by a specific individual or by an area or division within the organization. While Colombian laws do not require the privacy officer to be located in Colombia, such privacy officer is obliged to respond in a timely manner to all queries and complaints in Spanish, and must be fully knowledgeable of the organization’s operations and privacy policies.

11. International Data Transfers
The general rules established by Law 1266/08 and the Constitutional Court require that any transfer of private or semi-private Personal Data should be previously authorized by the Data Subject. Personal Data that originates from a foreign country does not require the Data Subject’s prior consent.

Law 1581 prohibits the transfer of any Personal Data to countries that do not provide adequate levels of protection. Law 1581 provides that there is an adequate level of protection if the regulations of said country meet the standards set by the SIC on the subject, which in no case can be lower than the standards established by Law 1581. These adequate levels have been established by the SIC’s Circular No. 5 of 2017 discussed in section 1.

The prohibition for the international transfer of Personal Data has the following exceptions, as described in Law 1581: (i) prior authorization from the Data Subject; (ii) exchange of medical information for reasons of health and public hygiene; (iii) exchange of financial information in connection with transfers or banking operations, according to the applicable legislation; (iv) transfer of data in compliance with an international treaty to which Colombia is a party; (v) necessary transfer of Personal Data for the execution of a contract between the Data Subject and the Data Controller; and (vi) transfers of data legally required to protect the public interest.

The Constitutional Ruling of 2011 provided some guidelines on the international transfer of Personal Data.

Law 1581 gave the Colombian government the authority to issue: a supplementary regulation on binding corporate rules (“BCRs”); the certification of good practices in data protection; and a list of countries with adequate levels of protection for the cross-border transfer of Personal Data.

To date, the Colombian government has not yet issued a list of countries that are deemed to have adequate levels of protection. Nor has it issued a regulation governing BCRs. In effect, even if an organization has BCRs in
place, they are not deemed useful for the purposes of international transfers of data, where processing of data is subject to Colombian laws.

12. Security Requirements

Organizations are required to take steps to: ensure that Personal Data in their possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations shall be liable together with third-party providers in case of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings, and/or private rights of action. Sanctions and penalties will be subject to reduction if Data Controllers and Processors apply the accountability guidelines issued by the DPA.

15. Data Security Breach

Pursuant to Law 1581, both Data Controllers and Data Processors have a duty to notify the Data Deputy of any breach to security codes and risks in the management of Data Subjects’ Personal Data, regardless of the nature and scope of the breach.

There is no obligation under Law 1581 to report the security breach to the Data Subject. However, the accountability principle guidelines include a recommendation on notifying Data Subjects, which is deemed by the DPA as an advisable practice that will be seen in a favorable light in case any investigations are initiated pursuant to a data breach report.

An organization that is involved in a data breach situation may be subject to a suspension of business operations; closure or cancellation of the file, register or database; administrative fine, penalty or sanction; civil actions and/or class actions, or a criminal prosecution.

The NDR platform (see Section 9) includes a module to notify data breaches. Until further regulation is issued, the obligation for Data Controllers to notify data breaches through this platform, only applies entities incorporated in
Colombia and registered with the local Chambers of Commerce acting as Data Controllers. No further regulation has been issued as to how other Data Controllers should make the notification of data breaches. In the absence of specific instructions for other parties, it is prudent to make the notification – when necessary – through a written brief submitted to the NDA.

16. Accountability

The DPA issued the document Guidelines for the Implementation of the Accountability Principle (hereinafter referred to as the “Guidelines”).

This document was issued by the DPA to help Data Controllers and Processors of Personal Data of Colombian individuals to implement within the organizations the accountability principle, which was introduced in the Colombian legislation.

According to the Guidelines, Data Controllers collecting and processing Personal Data of individuals who reside in Colombia must adopt measures that reflect its commitment to an accountability culture in the processing of such data. Hence, such Data Controllers should be capable to demonstrate to the DPA that they have adopted effective and appropriate internal measures to comply with the obligations set forth in the law.

Accordingly, internal measures adopted by Data Controllers must guarantee that (i) that there is an administrative structure directly proportional to the structure and size of the Data Controller within the organization; (ii) that there are internal mechanisms adopted to put into practice policies that include tools to implement and train personnel in the processing of data and in the policies related thereto; and (iii) adopt procedures to attend to consultations and claims from Data Subjects.

The Guidelines are aimed at explaining and detailing to Data Controllers the specific measures available to comply with their legal obligations. It is worth highlighting that the measures and mechanisms described in the Guidelines are not mandatory.

Nevertheless, organizations that undertake the commitment to protect Personal Data by adopting measures described in the Guidelines, can request a lenient application of fines and sanctions when investigated for violation of their obligations under the law.

This approach is consistent with the principles of data protection established under Law 1581, and therefore, if a Data Controller is able to demonstrate that it has adopted the measures similar or identical to those described in the Guidelines and that the infringement was isolated, the DPA may even refrain from opening a formal investigation in case of a non-material breach.

The Guidelines introduced the concept of an Integral Personal Data Management Program (hereinafter referred to as the “Program”) aimed at
applying the accountability principle. Some highlights of the suggested actions in the Guidelines are the following:

- **Tone at the top**, which requires active involvement of the company’s top management in developing, implementing and verifying compliance at all areas of the company.

- **The duties of the data protection officer (or division) include commitments to:**
  - Actively contribute in the development and implementation of the Program and the drafting of policies for the processing of Personal Data;
  - Develop a Personal Data risk assessment system;
  - Be the liaison between top management and all areas of the company for data processing and any projects that entail processing of Personal Data;
  - Promote a culture of Personal Data protection within the company;
  - Keep an inventory of all databases of the company that contain Personal Data;
  - Conduct the registration of databases with the DPA once the NDR is implemented;
  - Process and obtain the corresponding declarations of conformity with the DPA for specific data processing and sharing projects,
  - Review, amend and approve data transmission agreements;
  - Conduct internal trainings related to the effective compliance with the Program and with the internal policies adopted by the company to effectively and lawfully process Personal Data;
  - Attend and respond within the standards adopted by the Program and the time frames provided for in Law 1581 to claims and consultations made by Data Subjects regarding the processing of their Personal Data; and
  - Actively cooperate with the DPA whenever said entity opens an investigation to the company or makes any information request regarding the processing of Personal Data by the company.

- **Internal report and auditing mechanisms for data processing and management.**

- **Effective control systems for compliance of the Program and policies for the processing of Personal Data.**
• Effective administrative and operation protocols.

• Adequate database inventory.

• Adoption of data processing policies and manuals consistent with the content requirements of Decree 1377 and with the realities of the company’s data flows.

• Adoption of privacy impact assessment mechanisms that have the following phases: (i) identification; (ii) measurement; (iii) control; and (iv) monitoring.

• Robust internal training programs for all employees to guarantee knowledge, awareness and compliance with the law, the Program and the company’s internal policies and procedures.

• Adopt a robust methodology to receive and attend claims and consultations from Data Subjects.

• Adequately manage the relationship with Data Processors and the cross-border circulation of data in the way in which they handle, process and circulate Personal Data, which includes having robust contracts with them regulating the circulation of data in compliance with Law 1581 and Decree 1377.

• Appropriate communication strategies to ensure internal and external Data Subjects are duly informed and become aware of their rights, how to exercise them and the company’s policies in relation to the processing of Personal Data.

• Periodical supervision, evaluation and assessment of effective compliance of the law and the Program.

• Adopt protocols to adequately attend and respond to data breaches, conduct internal audits and adequately notify Data Subjects and the DPA of the same.

The Guidelines extensively comment on and develop all of the abovementioned recommendations, which evidences an effort from the DPA to put together an informative document that should help to understand the implications that handling Personal Data has.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Colombia as long as they are in compliance with local laws.
18. E-Discovery

The process by which electronically stored information is reviewed, processed and presented for the purposes of litigation or regulatory requests is valid under Colombian law. Electronic information can be stored in databases as structured content, in emails or instant messages as semi-structured content, and in documents or files as unstructured content. Nevertheless, employers should advise employees of the implementation of an e-discovery system and also that the use of work tools (e.g., email, Internet) is being monitored and information such as emails will be stored. Nevertheless, employees may request the employer to destroy any Private Information stored as a consequence of the implementation of the e-discovery system. The employer may justify his position by alleging that such information is crucial for complying with regulations and/or for the purposes of litigation.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

There are no specific laws/rules in Colombia that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. The consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. The consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid.

The Communications Regulation Commission (a special government agency) has developed the Excluded Numbers Registry, in which consumers can sign up their mobile numbers to stop receiving advertising text messages. This registry was created by Resolution No. 2229 of 2009. Despite this specific regulation, Law 1581 requires the Data Subjects’ prior, express and informed consent when any contact is made for advertising purposes; otherwise, such contact would be deemed as illegal.
Czech Republic

Jiri Cermak
Prague
Tel: +420 236 045 001
jiri.cermak@bakermckenzie.com

Milena Hoffmanova
Prague
Tel: +420 236 045 001
milena.hoffmanova@bakermckenzie.com

Martin Lazár
Prague
Tel: +420 236 045 001
martin.lazar@bakermckenzie.com
1. Recent Privacy Developments

**Opinion of the Office for Personal Data Protection on the collection and copying of certain visitor information for identification at the entrances to buildings**

The new draft law on Personal Data processing, which is supposed to replace the Act No. 101/2000 Coll., on the Protection of Personal Data once the EU General Data Protection Regulation (the “GDPR”) starts to apply, has been proposed by the Czech Ministry of the Interior. It has already been approved by the Government of the Czech Republic and is expected to be submitted to the Chamber of Deputies of the Parliament of the Czech Republic for the further discussions and approval.

2. Emerging Privacy Issues and Trends

The new draft law on Personal Data processing described above does not go beyond the provisions of the GDPR, however, in connection with the authorization given to the national legislators, provides certain derogations and specifications. The following important areas are worth mentioning:

- with respect to particularly important cases of processing of Personal Data in the public interest, the possibility of further processing without the requirement of reviewing the compatibility of the purpose of the original and subsequent data processing is established;

- reduction of age limit for granting of online consent to data processing to 13 years;

- in cases where a Data Controller carries out processing of Personal Data necessary to fulfil its legal obligation or a task carried out in the public interest or within the exercise of its authority, such controller may inform Data Subjects of the processing also by disclosing the information in a manner allowing remote access;

- introduction of a possibility of Data Controller to inform the recipients to whom Personal Data has been made available of any corrections, limitations or deletions of such Personal Data also by means of change of the respective Personal Data in the records, provided that valid contents of such records are regularly made available to the recipient;

- exception to obligation to carry out data protection impact assessment where certain data processing is regulated by specific legal regulations;

- limitation of Data Controllers’ obligations as set out in Articles 12 – 22 of GDPR, and also establishment of possibility of Data Controller to limit or postpone notification of a Personal Data breach to the regulatory authorities in cases of data processing for the purpose of: (i) defense or security of the Czech Republic; (ii) public order or internal security; (iii)
prevention, search for or detection of criminal activities, prosecution of
criminal offenses or enforcement of criminal penalties; (iv) another
important public interest objective of the European Union or a Member
State of the European Union, in particular an important economic or
financial interest of the European Union or a Member State of the
European Union, including monetary, budgetary and fiscal matters, public
health and social security; (v) protection of the independence of the
judiciary and of judicial proceedings, or (vi) monitoring, inspection or
regulatory functions related, even occasionally, to the exercise of official
authority in the cases referred to in points (i) to (v).

Please note that since such proposed draft law has not been approved yet by
the Czech legislative bodies, it is subject to possible amendments and its
wording should be deemed neither final nor binding at this stage.

3. Law Applicable

The Czech Data Protection Act No. 101/2000 Coll. (“CDP”), effective as of 1
June 2000, which implements the Data Protection Directive (95/46/EC); and
Regulation 2016/679 on the protection of natural persons with regard to the
processing of Personal Data and on the free movement of such data, and

4. Key Privacy Concepts

a. Personal Data

The CDP applies to the processing of any information relating to natural
persons (“Data Subjects”) who can be identified either directly or indirectly
from that information, in particular by reference to a number, code or to one or
more factors specific to their physical, physiological, mental, economic,
cultural or social identity (“Personal Data”).

Personal Data is defined accordingly in GDPR.

b. Data Processing

According to the CDP, processing of Personal Data means any operation or a
set of operations, systematically executed by a Data Controller (see Section
4(c) below) in an automatic or other manner. Processing means, in particular,
the collection of Personal Data, as well as its storage on data carriers,
retrieval, modification or alteration, searching, using, transferring, distributing,
publishing, preserving, exchanging, sorting or combining, blocking or
liquidating (i.e., deleting or destroying).

The CDP applies to any processing of Personal Data, whether executed
automatically (e.g., electronically) or otherwise and thus both hard and
soft/electronic copy of records of Personal Data are covered by the CDP and
considered data carriers.
The CDP does not apply to Personal Data processed for purely personal purposes or the occasional collection of Personal Data which is not subsequently processed any further.

Data Processing is defined accordingly in GDPR.

c. Processing by Data Controllers
Any person or entity (e.g., an employer) who specifies the purpose and the means of the processing of Personal Data, and who executes such processing and is responsible for it, is viewed as a Data Controller (“Data Controller”) for the purposes of the CDP.

Data Controller is defined accordingly in GDPR.

d. Jurisdiction/Territoriality
The CDP applies to processing carried out by Data Controllers established in the Czech Republic as well as foreign-established Data Controllers that process Personal Data in the Czech Republic, except for the transfer of Personal Data through the territory of the European Union (including the Czech Republic).

The GDPR will have a considerably broader territorial scope.

e. Sensitive Personal Data
The CDP imposes additional requirements for the processing of Sensitive Personal Data – that is, data relating to nationality, racial or ethnic origin, political attitudes, membership of trade unions, religious and philosophical beliefs, criminal convictions, health conditions and sexual life, genetic data of the Data Subject, or biometric data, which enables the Data Controller to directly identify or authenticate the Data Subject.

The GDPR uses the term “special categories of Personal Data” rather than Sensitive Personal Data. In contrast with CDP, processing of Personal Data regarding criminal convictions and offenses or related security measures under GDPR may only be carried out under the control of official authority or when the processing is authorised by the EU or a Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

Sensitive Personal Data may be processed only if the Data Subject has given explicit consent (in writing) to such processing. However, the CDP stipulates that the consent is generally not required if:

• the processing is necessary to protect the vital interests of the Data Subject, or to address an immediate danger threatening his/her property, and where the Data Subject is physically, mentally, or legally incapable of giving consent, or is missing, or because of any similar reason;
• the processing is necessary for providing health care, public health protection, health insurance, public administration in the area of health care, or examination of health conditions pursuant to a specific law;

• the processing is necessary to fulfill the obligations and rights of the Data Controller in the field of employment or labor law (arising under a specific law);

• the processing (i) is carried out in the course of legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade union aim, (ii) is duly authorized, and (iii) relates only to the members of such a body, and the Personal Data is not disclosed without the consent of the Data Subject;

• the processing of Personal Data is required to provide health insurance, social security insurance, old age pension security, state social subsidy and other social care according to specific laws;

• the processing relates to Personal Data that is made public by the Data Subject;

• the processing is necessary for the establishment or exercise of legal claims;

• Personal Data is processed only for archiving purposes pursuant to a special law; or

• the processing is carried out according to special laws in the course of prevention, investigation, or detection of criminal activity, prosecution of criminal offenses and searching for individuals.

The GDPR contains a general prohibition on processing of special categories of Personal Data and only allows it in certain exceptional circumstances expressly listed.

f. Employee Personal Data

The CDP does not recognize a special category of Employee Personal Data and, therefore, the general rules for processing set forth in the CDP apply. However, in the case of an employment relationship, if the scope of Personal Data collected does not exceed the scope of data required for concluding or performing an employment agreement under the Czech Labor Code, employee consent (as described in Section 5(a) below) and notification to the Office would not be required. However, the Labor Code does not specifically state what Personal Data is necessary for concluding or performing an employment relationship.

Sensitive Personal Data, by its definition, does not fall within the scope of Employee Personal Data which can be collected and processed without the
employee’s consent. Nevertheless, it is generally acknowledged by the Office that any Personal Data collected for the purpose of an employment agreement and granting of additional employee benefits can be collected without the employee’s consent (e.g., data regarding name, address, date of birth, citizenship, phone numbers, education, salary, bonus, social security, bank account, etc.).

A fallback justification for processing both Personal Data and Sensitive Personal Data in an employment context is when the employee, as the Data Subject, provides consent.

According to the CDP, the fact that Sensitive Personal Data belongs to an employee is not relevant in respect of the rules for processing of such Personal Data. Accordingly, the processing of Sensitive Personal Data in excess of the scope permitted under the Labor Code must be justified by the employee’s consent or another ground in Section 4(e).

Same as CDP, the GDPR does not distinguish a special category of Employee Personal Data, thus general rules for data processing set forth in the GDPR apply. But it does allow Member States to provide for more specific rules for the processing of employee’s Personal Data in the employment context.

5. Consent

a. General
Under the CDP, the general rule is that a Data Controller may process Personal Data as long as the consent of the Data Subject is obtained. However, the CDP provides for a number of exceptions.

Consent must be voluntary, informed, explicit and unambiguous, and must be obtained prior to or at the time of collection of data. Consent only covers identified purposes, and hence, fresh consent is needed for purposes not previously identified and consented to. The Data Subject can revoke the consent at any time.

The CDP does not stipulate in what language consent must be given. The Office regularly communicates in the Czech language; however, in practice, the Office is flexible in this area and usually accepts documents in the English language as well. In addition, consent can be translated into the Czech language should the Office so require.

Additionally, according to the GDPR, if the Data Subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters. Revocation of consent must be as easy as it is to give the consent. The withdrawal of consent does not affect the
lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the Data Subject must be informed thereof.

GDPR also provides that where data processing is based on consent, the Data Controller must be able to demonstrate that the Data Subject has consented to processing of his or her Personal Data.

When assessing whether consent is freely given under GDPR, utmost account is taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of Personal Data that is not necessary for the performance of that contract.

The GDPR does not stipulate in what language consent must be given (of course, Data Subjects have to understand the language).

b. Sensitive Data

Subject to specific exceptions stipulated in the CDP, Sensitive Personal Data may be processed only if the Data Subject has given explicit consent (in writing) to such processing. Prior to giving consent to the processing of Sensitive Personal Data, the Data Subject must be informed of (i) the purpose(s) of processing for which the consent is given, (ii) the scope of the Personal Data being processed, (iii) the Data Controller to which the consent is given, and (iv) the period of time for which the consent is given. The Data Controller must be able to prove the existence of the consent during the entire period of the processing of Personal Data and the Data Subject can revoke the consent at any time.

Under GDPR, the processing of special categories of Personal Data is also subject to additional consent requirements.

c. Minors

According to the Czech Civil Code, a person becomes fully competent to acquire and assume rights and obligations through legal acts upon reaching the age of 18 years. However, the Civil Code also stipulates that minors (i.e., persons below 18 years of age) can execute such legal acts in law which correspond to the level of their mental and moral maturity. In addition, the Civil Code regulates certain specific rights of minors who have reached the age of 15 years (e.g., right to express a last will).

In light of this, it has been generally acknowledged by the Office that minors between 15 and 18 years of age can execute legal acts in relation to their Personal Data (i.e., can provide consent to the Data Controller). The statutory representatives (e.g., parents) of a minor shall represent and act on behalf of minors that are below 15 years of age.

Under the GDPR, in relation to the offer of information society services directly to a child, the processing of the Personal Data of a child shall be lawful where the child is at least 16 years old. If a minor is under 16 years of age, such
processing is lawful only and to the extent that such consent has been expressed by a person who exercises parental responsibility for the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

d. Employee Consent

There are no special rules or limitations stipulated in the CDP in relation to consent granted by an employee to the employer. Therefore, the general consent rules apply to Employee Personal Data. Likewise, GDPR does not provide specific rules for consent of the employee, thus the general rules apply.

e. Online/Electronic Consent

Consent can also be given electronically, provided the Data Controller assures that each consent can be unequivocally assigned to a particular identified Data Subject, and the consent includes all required information. An electronic signature that meets the requirements set forth in the Czech Act on Electronic Signatures (implementing EU Directive 1999/93/EC) provides the highest standard of legal certainty with respect to identification of the acting person. It is therefore advisable to comply with these requirements wherever possible.

According to the GDPR, consent can also be given electronically by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the Data Subject’s agreement to the processing of Personal Data. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the Data Subject’s acceptance of the proposed processing of his or her Personal Data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes.

If the Data Subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity, (ii) the types of Personal Data being collected, (iii) the purposes for collecting Personal Data, (iv) third parties to which the organization will disclose the Personal Data, (v) the consequences of not providing consent, (vi) the rights of the Data Subject, (vii) where the Personal Data is to be transferred, (viii) how to make an inquiry or
file a complaint, (ix) how to access and/or correct the Data Subject’s Personal Data, and (x) the duration of the proposed processing.

Under the GDPR, similar requirements are established for information obligatorily provided to Data Subjects; apart from the information listed by CDP, it is also required under the GDPR to inform a Data Subject of the identity and contact information of the Data Protection Officer (if applicable). Additionally, and, if necessary for fair and transparent data processing, also about the existence of right to data portability (as these are the rights that are not recognized under CDP), and the fact that Personal Data are subject to automated decision-making, including profiling.

Additionally, in case Personal Data is not obtained directly from the Data Subject, it is also required under the GDPR to inform a Data Subject of the categories of Personal Data concerned, and, if necessary for fair and transparent data processing, also the information on from which source the Personal Data originate, and if applicable, whether it came from publicly accessible source.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

GDPR recognizes such principles as stated by CDP.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Data.

In addition to the abovementioned information, GDPR introduces a completely new right, right to data portability. More specifically, the Data Subject will have the right to receive his/her Personal Data, which he/she has provided to the controller and will have the right to transmit those data to another controller without hindrance from the former controller. This has to be done in a structured, commonly used and machine-readable format.

However, this only applies within specific situations, when (i) the Data Subject has given consent to the processing of his/her Personal Data for one or more specific purposes; (ii) the processing is necessary for the performance of contract to which the Data Subject is party or in order to take steps at the
request of the Data Subject prior to entering into a contract; (iii) the Data Subject has given explicit consent to the processing of special categories of Personal Data for one or more specified purposes; or (iv) the processing is carried out by automated means.

Furthermore, under GDPR, it is explicitly stated that Data Subjects have the right for deletion if Personal Data concerning them. This right was previously merely judicated by the Court of Justice of the European Union.

9. Registration/Notification Requirements

Generally, the processing of Personal Data requires registration with the Office. Registration is not required if (i) only publicly available Personal Data is being processed, (ii) the processing is carried out on the basis of a special law or is necessary to fulfill the legal obligations and rights of the Data Controller, or (iii) the processing is carried out in the course of legitimate activities by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade union aim, and the processing is duly authorized and relates only to the members of such a body.

Given the foregoing, before commencement of the processing of Personal Data, the Data Controller needs to notify the Office. The notification is carried out by filling in an online notification form available on the website of the Office.

Under the GDPR, data processing activities are not subject to registration obligation with the Office. However, the obligation to keep records of data processing activities and to evidence such records upon request of the Office is introduced instead, applying to each Data Controller, with an exception of an enterprise or an organization employing less than 250 persons, unless the processing it carries out is likely to result in a risk to the rights and freedoms of Data Subjects, the processing is not occasional, or the processing includes special categories of data or Personal Data relating to criminal convictions and offenses.

10. Data Protection Officers

In the Czech Republic, there is no requirement for organizations to appoint a data protection officer or other individual who will be accountable for the privacy practices of the organization.

However, under GDPR, in several situations it will be mandatory to appoint such officer, namely in instances when (i) the processing is carried out by a public authority or body; (ii) the core activities of the controller consist of regular and systematic monitoring on a large scale; or (iii) the core activities of the Data Controller consists of processing of special categories of data on a large scale.
GDPR further provides for a possibility for a group of undertakings to appoint a single data protection officer provided that this officer is easily accessible from each establishment, and further specifies the obligations and the role of data protection officer.

11. International Data Transfers

According to the CDP, Personal Data can be transferred:

- to EEA Member States without any limitation; and
- to third countries (i.e., non-EEA countries) if (i) such transfers are permitted under a ratified international treaty binding on the Czech Republic or (ii) Personal Data is transferred on the basis of the decision of an EU authority.

If the above-mentioned conditions are not met, Personal Data can only be transferred to recipients outside the Czech Republic if:

- the Data Subject has given consent to or instructions for the transfer;
- the recipient’s country provides sufficient special safeguards for the protection of Personal Data which are specified in an agreement between the Data Controller and the recipient of the transferred Personal Data, provided that such an agreement: (i) ensures application of the special safeguards; or (ii) includes the standardized contractual clauses published in the Office’s Gazette. In addition to the EEA countries, the Office considers, inter alia, Switzerland, Norway, Argentina, Faroe Islands, Guernsey, Jersey, Iceland, the Isle of Man, Canada, Andorra, Liechtenstein and Israel as providing sufficient special safeguards for cross-border data transfer. Although the Office does not consider the US to be a “safe” country in this respect, Data Controllers can benefit from the Safe Harbor Agreement when transferring Personal Data to recipients located in the US;
- the transfer is made from a public register or a register accessible to everyone who proves a legal interest;
- the transfer is necessary for the establishment or exercise of an important public interest arising under a special Act or an international treaty binding on the Czech Republic;
- the transfer is necessary for the performance of a contract to which the Data Subject is party, or if the processing is essential for the Data Subject to enter into negotiations for the formation of a contractual relationship or for the amendment of an existing contract;
the transfer is necessary for the conclusion or performance of a contract entered into between the Data Controller and third parties in the interests of, or at the request of, the Data Subject; or

the transfer is necessary for the protection of the rights or vital interests of the Data Subject, especially for the protection of the Data Subject’s life or provision of health care.

Subject to the exemptions provided by: (i) international treaties binding on the Czech Republic (e.g., the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (“Convention 108”), to which the Czech Republic is a signatory); or (ii) decisions of the competent bodies of the European Union (e.g., decision No. 2000/520/EC of the European Commission on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce), the Data Controller must apply for Office approval in relation to every transfer of Personal Data to a third country (i.e., non-EEA country).

Since the Czech Republic is a signatory country to Convention 108, the provisions of Convention 108 supersede the provisions in the CDP regarding the transfer of Personal Data to other countries.

According to Article 12 of Convention 108, a contracting state must not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization any cross-border flows of Personal Data going to the territory of another contracting state.

Article 12 applies to transfers across national borders, by whatever medium, of Personal Data undergoing automatic processing or collected with a view to being automatically processed.

At the time of writing, the following countries are contracting states to Convention 108: all EU countries, Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Liechtenstein, Mauritius, Moldova, Monaco, Montenegro, Norway, Russia, San Marino, Senegal, Serbia, Switzerland, the former Yugoslav Republic of Macedonia, Uruguay, Tunisia, Turkey, and Ukraine.

Under GDPR, the rules for transfer of Personal Data are set out similarly. Additionally, GDPR expressly lists Binding Corporate Rules as an appropriate safeguard for transfer of Personal Data to third countries and rules therefor.

12. Security Requirements

Organizations are required to take steps to: (i) ensure that Personal Data in its possession and control are protected from unauthorized access and use; (ii) implement appropriate physical, technical and organization security
safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

Similar requirements apply under the GDPR, whereby the GDPR expressly obligates both, the Controller and the Processor, to implement appropriate technical and organisational measures.

13. Special Rules for Outsourcing of Data Processing to Third Parties

There are no specific rules for outsourcing in the Czech Republic. As long as the outsourcing entity complies with its duties as Data Processor and the Data Controller complies with its duties, the outsourcing may be considered valid. Special rules may, however, apply in certain sectors (such as the banking sector). The same applies under GDPR.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

Under the GDPR fines may amount up to EUR 20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year for serious infringements.

15. Data Security Breach

Generally, if there is a data security breach, the breach does not have to be reported under the CDP. However, given that a duty to prevent damage generally applies, any security breach that may cause damage to Data Subjects must be duly reported to them in order to allow them to adopt the appropriate course of action (e.g., change of password, etc.). Such notice should be delivered to the Data Subjects as soon as possible in order to ensure that they will be able to prevent potential damage.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, and civil actions and/or class actions.

Under GDPR, data breach notification will be mandatory.

More precisely, the Data Controller has to report such breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it. When it is not made within 72 hours, the report must also state the reasons for the delay. The notification sent to the supervisory authority must possess at least basic information as to what is the nature of the breach, contact details...
of the Office, describe the likely consequences of the breach, describe the measures taken or proposed to be taken by the controller to address this breach.

16. Accountability

Subject to regulatory guidance, organizations may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data, furnish the results of the privacy impact assessments to privacy regulators upon request, and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

Under the GDPR, performance of data processing impact assessment will be mandatory in case where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

In addition, the accountability principle more generally is strengthened under the GDPR. The GDPR explicitly states that the Controller shall be responsible for, and be able to demonstrate compliance with the other principles relating to the processing of Personal Data (e.g., lawfulness, fairness and transparency), thereby introducing extensive new documentation obligations.

17. Whistle-Blower hotline

Whistle-blowing is not specifically regulated in the CDP. Therefore, any processing of Personal Data carried out in connection with the operation of a whistle-blowing hotline in the Czech Republic will be subject to general rules and obligations regarding the processing of Personal Data.

The CDP requires all persons intending to process Personal Data in relation to Data Subjects in the Czech Republic to register with the Office. Registration is not required, inter alia, if the processing is carried out on the basis of a special law or is necessary to fulfill the legal obligations and rights of the Data Controller arising under a special law (e.g., labor law, criminal law, etc.).

Given the foregoing, in case of the processing of Personal Data due to a whistle-blowing hotline, an argument can be made that such processing is excluded from the general registration obligation according to the CDP on the grounds that the Data Controller fulfills the legal obligations and rights arising under law (e.g., prevention of occurrence of damage or breach of applicable laws).

However, given the fact that processing of Personal Data in connection with the whistle-blowing hotline is often carried out on the basis of requirements of a foreign law or statute (e.g., the US Sarbanes Oxley Act) rather than to fulfill the legal obligations arising under Czech law and such processing often
exceeds the Personal Data processing that falls within the exception as stipulated above, it is generally recommended to register the respective Personal Data processing connected with the operation of the whistle-blowing hotline with the Office.

Whistle-blowing is not specifically regulated in the GDPR, thus the general rules on data processing apply.

18. E-Discovery
Czech law does not specifically regulate e-discovery systems. Thus, when implementing an e-discovery system, the general data protection rules apply.

As e-discovery is not specifically regulated under the GDPR as well, the general rules will also apply (e.g., principle of legality, principle of data minimization, notification obligation with respect to Data Subjects, etc.). Nevertheless, there is no legal obligation regarding implementation of e-discovery system for companies in the position of a Data Controller under the Czech law that would justify data processing based on the legal title of “compliance with a legal obligation” under Art. 6 (1) c) of the GDPR.

19. Anti-Spam Filtering
Whether there are any regulatory concerns pertaining to the deployment of spam-filtering technology is determined by considering the nature of the software that is implemented (i.e., whether the spam-filtering solution is automatic and applicable in the same manner for all of the employees or whether it allows certain IT officers of the company to monitor the content of the spam).

20. Cookies
There has been a transition in the regulatory regime from opt-out to opt-in requirements when it comes to deployment of cookies. The recent EU Directive 2009/136/EC calls for express prior consent, i.e., opt-in; nevertheless, the methods for giving such consent remain rather broad. Particularly, within the Czech jurisdiction, according to the opinion of the Office, it is acceptable not only to provide express consent for the use of cookies by accepting the terms when opening a website, but also through setting the web browser to accept cookies by default.

The GDPR also not specifically addresses the use of cookies. However, the same is, inter alia, the subject matter of the draft ePrivacy Regulation that was proposed by the European Commission in January 2017. According to the draft, the use of cookies will require the user’s consent, unless the cookie is required to provide the service to the customer.
21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.

Under the GDPR, an organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond or opt out. An organization may be required to obtain consent for a specific activity.

The draft ePrivacy Regulation also generally requires prior opt-in consent for sending direct electronic marketing communications.
Denmark

Daiga Grunte-Sonne
Copenhagen
Tel: +45 38 77 41 18
DSO@kromannreumert.com

Tina Brøgger Sørensen
Copenhagen
Tel: +45 38 77 44 08
tib@kromannreumert.com
1. Recent Privacy Developments

The key legislation regulating data privacy in Denmark is the Danish Act on Processing of Personal Data, Act No. 429 of 31 May 2000, with subsequent amendments (the “Data Protection Act”), which is based on EC Directive No. 95/46/EC of 24 October 1995 (the “Data Protection Directive”).

**The EU General Data Protection Regulation**

Denmark is currently preparing for the EU General Data Protection Regulation (the “GDPR”), which will start to apply from 25 May 2018 and will replace the Data Protection Directive, and thus the Data Protection Act.

Besides a greater harmonization in the area of data protection, the GDPR aims to take globalization and technological developments into account. The GDPR introduces a number of requirements new in Danish data protection law, e.g., an obligation to designate a Data Protection Officer, mandatory impact assessments and a duty to notify the authorities in case of a security breach, etc. Thus, the GDPR will change the current legal position in Denmark.

Further, the GDPR will implement larger fines for non-compliance with the data protection rules (up to EUR 20 million or as much as 4% of a worldwide annual turnover of an undertaking). Such fines are substantially higher than any fine issued in Denmark (the highest fine ever was issued in 2001 and amounted to DKK 25,000, which corresponds to approximately EUR 3,360), which undoubtedly increases awareness among companies in relation to data protection issues, certainly taking into account that both Data Controllers and Data Processors are subject to the rules.

The GDPR allows EU member states to enforce national rules to apply alongside the GDPR. The Danish Ministry of Justice has published a report that is forming the basis for the interpretation of the GDPR, and a subsequent bill proposing specific national rules on data protection was presented on 7 July 2017. The bill is expected to be adopted in the late fall of 2017. Thus, the upcoming Act on Processing of Personal Data will apply alongside the GDPR.

2. Emerging Privacy Issues and Trends

The Danish Data Protection Agency (the “DPA”) has overall reviewed and assessed a decreasing number of cases during 2016. However, the number of reviewed and assessed cases related to public authorities have increased during 2016. Many of the cases related to public authorities concern data security breaches.

Generally, a number of major cases regarding security breaches have reached the public during 2016 and have been reviewed and assessed by the DPA.
One of these cases concerned the Danish Serum Institute. The Danish Serum Institute accidentally sent a letter containing unencrypted CPR-numbers to the Chinese Embassy. In this case, the DPA found that there had been no intentional security breach. Further, the DPA found that there had been no actual risk of the individuals, whose information had been disclosed. Therefore, the DPA found that it was not necessary to inform the Data Subjects about the security breach.

Another of the cases concerned Novo Nordisk’s Jobbank. Due to a human error by an external IT-developer a test-site containing personal information of 95,000 persons, who had subscribed for news concerning job openings at Novo Nordisk, was made public on the Novo Nordisk website. Novo Nordisk immediately contacted the IT-developer and made sure the site was removed. Furthermore, Novo Nordisk ensured that Google removed all saved versions of the site. The DPA found that the security breach entailed that Novo Nordisk had not lived up to the security requirements when processing Personal Data.

In 2017, the DPA is expected to use the main part of their resources on focusing on the implementation of the GDPR.

3. Law Applicable

As mentioned above, the primary legal source regarding data privacy and protection is the Data Protection Act, which entered into force in 2000. There have been many amendments to the Data Protection Act through the years, most recently in 2013. Additionally, as Denmark is part of the European Union and thus the Data Protection Act implements the Data Protection Directive, the decisions from the courts of Denmark as well as the European Court of Justice have relevance when interpreting the Data Protection Act. The Data Protection Act will apply until 24 May 2018, after which date, the rules in the GDPR will apply alongside the new Act on Processing of Personal Data, which is presumed to be adopted in the fall of 2017.

Interpretation of the Data Protection Act and the current practice is also partly based on the earlier practice in accordance with the Act No. 293 of 8 June 1978 on Private Registers, which was effective prior to the adoption of the Data Protection Directive.


Collection and processing of data is, to some extent, also regulated by other legislation, for example, there are specific rules in the Financial Business Act and the Payment Services and Electronic Money Act as regards the financial sector. These separate set of rules are stricter than the Data Protection Act, thus, the Data Protection Act provides the minimum regulation and applies where other legislation does not provide a higher level of protection for the Data Subject.

The responses below relate specifically to the Data Protection Act but references to other legislation will be provided where relevant.

4. Key Privacy Concepts

a. Personal Data

Personal Data is defined in the Data Protection Act as “any information relating to an identified or identifiable natural person ("Data Subject")”.

Hence, Personal Data must be considered as a broad concept, e.g., any information that in any way can be connected to a specific physical person, with the help of reasonable means, will constitute “Personal Data”, regardless of whether the data will be perceived as objective (facts) or subjective (opinions). This also includes encrypted information as long as the encryption key exists.

Information related to legal entities is not regarded as Personal Data. However, this does not apply to data related to one-man businesses.

Further, anonymous data is not regarded as Personal Data, which is based on the assumption that the anonymization process is carried through effectively. The assessment in this respect is rather strict, for example, encrypted data will not be regarded as anonymous as long as the Data Controller or another party can make the data "readable" again and connect the data to a particular individual. Theoretically, only "one-way" encryption, e.g., when the encryption key is destroyed, will meet these requirements. However, the means of the anonymization must be subject to a concrete assessment, as in practice it is impossible to prevent every attempt of decryption.

b. Data Processing

The Data Protection Act defines data processing as “any operation or set of operations which is performed upon Personal Data, whether or not by automatic means”.

Thus, all actions, including but not limited to collection, registration, selection, transfer, searching, blocking, rectification, systemization and deletion are considered as data processing.
c. Processing by Data Controllers
The Data Protection Act applies to entities that are Data Controllers, e.g., any “natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data”.

The entity processing data on behalf of the Data Controller is regarded as a Data Processor. The Data Processor may only process data in accordance with the Data Controller’s instructions and such data processing must be governed by a written contract between the parties. The contract must stipulate that the Data Processor may only act on instructions from the Data Controller and that there must be implemented appropriate technical and organizational measures to protect data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Data Protection Act.

d. Jurisdiction/Territoriality
The Data Protection Act applies to any Data Controller established in Denmark, when the activities relating to the processing of data take place within the EU/EEA.

Further, the Data Protection Act applies to any data processing carried out on behalf of Danish diplomatic representations.

The Data Protection Act will also apply if the Data Controller is situated outside the EU/EEA and the processing of data is carried out with the use of equipment situated in Denmark, unless such equipment is used only for the purpose of transmitting data through the territory of the EU/EEA. The Data Protection Act will moreover apply to the collection of data in Denmark for the purpose of processing outside the EU/EEA.

e. Sensitive Personal Data
Pursuant to the Data Protection Act, Sensitive Personal Data is regarded as information revealing/concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

As a starting point, such data may only be processed with the Data Subject’s explicit consent.

Further, Sensitive Personal Data may be processed if:

- the processing is necessary to protect the vital interests of the Data Subject or of another person where the person in question is incapable of giving his/her consent;
- the processing relates to data which has been made public by the Data Subject; or
• the processing is necessary for the establishment, exercise or defense of legal claims.

There are also a number of exceptions specifically related to the different categories of Sensitive Personal Data, for example, information on trade union membership may take place when necessary for compliance with the labor law obligations, or different areas of practice, such as the area of criminal law or health care services.

Moreover, processing of data related to criminal offenses, serious social problems or other purely private matters (such as grounds for dismissal, divorce or death in the family) must be very limited, as these types of data are regarded as semi-sensitive under Danish law.

Processing of such data on behalf of a public administration may only take place, if it is necessary for the performance of the tasks of the administration and disclosure of the data to third parties must be very limited and may mainly be based on the Data Subject’s explicit consent.

Private persons and entities may only process such data with the Data Subject’s explicit consent or if the processing is necessary for pursuing legitimate interests which clearly override the interests of the Data Subject. The same applies for disclosure of the data to third parties.

Moreover, the processing may also take place if the conditions above regarding processing of Sensitive Personal Data are satisfied, for example, processing is necessary for the establishment, exercise or defense of legal claims. This applies to both public administration and private entities and covers furthermore disclosure to third parties.

f. Employee Personal Data

Collection and processing of Employee Personal Data is mainly regulated by the Data Protection Act but specific regulations apply as well, for example, the Act on Use of Health Information on the Labor Market, which determines that only health data that has significant relevance for the job position may be collected and processed. However, the basic principles of data processing will always apply (please see Section 7) and the employer must also comply with principles of processing of Sensitive Personal Data (please see Section 4(e), above), when relevant.

The DPA must be notified of the employer’s processing of Sensitive Employee Data prior to such processing actually taking place. The application for such processing can be submitted electronically and must be approved by the DPA. The approval triggers an administrative fee of DKK 2,000 (approximately EUR 270).
Further, the DPA has issued guidelines regarding control of the employees’ use of the Internet and email. Such monitoring may only take place if:

- the employer has a legitimate interest in retaining copies of emails and logs of Internet use;
- the employee has been made aware of the fact that the employer keeps copies of emails and logs of Internet use;
- the employee is informed that the employer may review such copies and log-files, when suspicion of misuse arises; and finally
- the emails that are marked “private” or otherwise have clearly private content must be excluded from the review.

5. Consent

a. General

Pursuant to the Data Protection Act, the Data Subject’s consent must be freely given, specific and informed.

The Data Subject must have been provided with adequate information regarding the processing of the data in order for the consent to be “informed”. Further, the consent must constitute a positive action by the Data Subject, meaning that consent based on the silence or passivity of the Data Subject will not be regarded as sufficient.

Processing of data may always be based on the Data Subject’s consent. However, the Data Subject has a right to withdraw his/her consent at any given time, hence, the practical reality is that the data mostly is processed in accordance with the general processing rules where processing under certain circumstances is permitted without the Data Subject’s consent (please see Section 7 for further information).

b. Sensitive Data

The requirements for a legally valid consent regarding Sensitive Personal Data are the same as mentioned above under Section 5(a).

c. Minors

Minors, who under Danish law are individuals under 18 years of age, are not able to give a binding expression of will and are therefore not able to give a valid consent. In order to obtain a valid consent from a minor, the consent must be obtained from a parent or a legal guardian.

In relation to the processing of data on behalf of a public administration, a minor’s expression of will shall be legally binding and effective in relation to particular actions or rights granted by the substantial law, for example,
submission of certain applications or making certain decisions on his/her own behalf.

d. **Employee Consent**
The requirements for a legally valid employee consent are the same as mentioned above under Section 5(a).

e. **Online/Electronic Consent**
Online/electronic consent is permissible and will be equally binding as consent given in written or oral form, as long as the requirements mentioned under Section 5(a) are fulfilled. The burden of proof in this respect lies with the Data Controller.

6. **Information/Notice Requirements**
Where the Personal Data have been collected from the Data Subject, the Data Controller must provide the Data Subject with the following information:

1. the identity of the Data Controller and of his/her representative;
2. the purposes of the processing of the data; and
3. any further information which is necessary, taking into account the specific circumstances of the collection of the data in order to enable the Data Subject to safeguard his/her interests. Such information may include:
   a. the categories of recipients (but not the particular recipients);
   b. whether the response to the questions is voluntary, including possible consequences of failure to reply; and
   c. the rules on the right of access to and the right to rectify the data.

Where the data has *not* been obtained *directly* from the Data Subject, the Data Controller must provide the Data Subject with the following information:

1. the identity of the Data Controller and of his/her representative;
2. the purposes of the processing of the data; and
3. any further necessary information, such as:
   a. the categories of data;
   b. the categories of recipients; and
   c. the rules on the right of access to and the right to rectify the data.

This information must be provided no later than the time when the data is disclosed, which in practice means within 10 days.
7. Processing Rules

There are a number of basic principles in relation to processing of data. Generally, the Data Controller must always comply with good practice for the processing of data, which means, inter alia, that the processing must be fair and reasonable. Further, the following principles apply:

1. The data must be collected solely for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes.

2. The processed data must be adequate, relevant and not excessive in relation to these purposes.

3. The data must be updated when relevant and the necessary checks must be carried out to ensure that no inaccurate or misleading data is processed or retained. Data which turns out to be inaccurate or misleading must be erased or rectified without delay.

4. The collected data may not be retained for a longer period than it is necessary for the purposes for which the data is processed.

As a general rule, Personal Data may only be processed if explicit consent is obtained from the Data Subject. The data may, however, also be processed without the Data Subject’s consent, provided that processing is necessary:

a. for the performance of a contract where the Data Subject is party or in order to take steps at the request of the Data Subject, prior to entering into a contract;

b. for the Data Controller’s compliance with a legal obligation;

c. in order to protect the vital interests of the Data Subject;

d. for the performance of a task carried out in the public interest;

e. for the performance of a task carried out in the exercise of official authority vested in the Data Controller; or

f. for the purposes of the legitimate interests pursued by the Data Controller where these interests are not overridden by the interests of the Data Subject (the rule of balancing of interests).

Sections (e) and (f) apply equally to the disclosure of data to third parties.

8. Rights of Individuals

The Data Subject has a right to access the data related to him/her. If the Data Subject submits a request to that effect, the Data Controller must inform the Data Subject whether or not data relating to him/her is being processed. If the
Data Controller processes such data, the following information must be communicated to the Data Subject:

1. the data that is being processed;
2. the purposes of the processing;
3. the categories of recipients of the data; and
4. any available information about the source of such data.

Such requests must be replied to without delay, e.g., as soon as possible. If it is not possible to provide a reply within four weeks, the Data Controller must inform the Data Subject of the grounds for this and when the reply can be expected.

The Data Subject has a right to receive the information mentioned above twice a year. Thus, the Data Subject is not entitled to a new communication in this regard until six months after the last communication, unless he or she can establish that he/she has a specific interest to that effect.

The Data Subject may, at any time, object to the processing of data relating to him/her. Where this objection is justified, the processing may no longer involve the particular data. An objection will be considered justified if the processing is illegal, or the particular circumstances of the case justify the objection. This can be the case, for example, where an employee wishes to have his/her contact information removed from the employer’s website due to harassment from a former spouse.

In addition, the Data Controller must at the request of the Data Subject rectify, erase or block data, which turn out to be inaccurate or misleading or in any other way processed in violation of law or regulations. The Data Controller must also notify the third party to whom the data has been disclosed of any such rectification, erasure or blocking. However, this will not apply if such notification proves impossible or involves a disproportionate effort.

9. Registration/Notification Requirements

In respect of processing operations carried out on behalf of a private Data Controller and the notification obligation of such processing, the theoretical main rule under the Data Protection Act is that the processing must be notified with the DPA before its commencement. However, the practical reality is that notification is only necessary when processing involves Sensitive Personal Data, as many processing operations of data are, in fact, exempt from the notification obligation. The notification obligation is particularly relevant in relation to the processing of employee data – please see Section 4(f).

The exemption to the notification obligation can be found in both the Data Protection Act and in the Executive Orders No. 534 of 15 June 2000 and No.
410 of 9 May 2012 regarding exemptions to the notification obligation of certain processing operations carried out on behalf of a private controller.

If a Data Controller is obliged to notify a processing of data, the Data Controller must notify the DPA prior to the commencement of the processing and such notification must include the following information:

- the name and address of the Data Controllers and of their representatives, if any, and of the Data Processors, if any;
- the category of processing and its purpose;
- a general description of the processing;
- a description of the categories of Data Subjects and of the categories of data relating to them;
- the recipients or categories of recipients to whom the data may be disclosed;
- intended transfers of data to third countries and statutory authority for such transfers (e.g., EU standard model clauses, adherence to EU-US Privacy Shield, binding corporate rules etc.);
- a general description of the measures taken to ensure security of processing;
- the date of the commencement of the processing; and
- the date of erasure of the data.

Notification must be made for every separate processing, or alternatively for multiple processing for which one overall purpose applies. This could be the case with different data processing connected to one specific assignment.

The standard notification form can be downloaded from the website of the DPA (www.datatilsynet.dk) and can be filed electronically, by email or by ordinary mail. The notification must be filed in Danish.

With respect to processing carried out on behalf of a public administration body, the theoretical main rule under the Data Protection Act is that the processing needs to be notified prior to its commencement. However, the practical reality is that notification is only necessary in certain situations, when processing so-called data of a confidential nature. Under Danish law, data can be “of a confidential nature” either when defined confidential by law or when its secrecy is necessary to safeguard essential public or private interests. Consequently, “data of confidential nature” covers a wider scope of data than Sensitive Personal Data.
The exemptions to the notification obligation can be found both in the Data Protection Act and in Executive Order No. 529 of 15 June 2000 on exceptions from the obligation to notify certain processing carried out on behalf of the public administration.

10. Data Protection Officers

In Denmark, it is not a requirement to appoint or designate a Data Protection Officer ("DPO") or other individual who will be accountable for the data protection practices of a legal entity or a public authority. The current legal position in this respect will, however, change when the GDPR applies from 25 May 2018. Under the GDPR, all public authorities shall designate a DPO. Data Controllers and Data Processors shall also designate a DPO if their core activities consist of either (i) processing operations which, by virtue of their nature, scope or purpose, require regular and systematic monitoring of Data Subjects on a large scale, or (ii) large-scale processing of Sensitive Personal Data.

11. International Data Transfers

Any transfer of Personal Data to a third country, e.g., outside the EU/EEA, may only take place if the third country in question ensures an adequate level of protection.

The adequacy of the level of protection afforded by a third country must be assessed in light of all the circumstances in relation to the data transfer operation, in particular (i) the nature of the data, (ii) the purpose and duration of the processing operation, (iii) the country of origin and the country of final destination, (iv) the rules of law in force in the third country in question and (v) the professional rules and security measures which are complied with in that country.

In addition, transfer of data to a third country may take place if:

1. the Data Subject has given his/her explicit consent;

2. the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject’s request;

3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a third party;

4. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;

5. the transfer is necessary in order to protect the vital interests of the Data Subject;
6. the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case;

7. the transfer is necessary for the prevention, investigation and prosecution of criminal offenses and the execution of sentences or the protection of persons charged, witnesses or other persons in criminal proceedings; or

8. the transfer is necessary to safeguard public security, the defense of the realm, or national security.

Outside the scope of the transfers referred to in items 1 to 8, the DPA may authorize a transfer of Personal Data to a third country which does not have an adequate level of protection, where the Data Controller adduces adequate safeguards with respect to the protection of the rights of the Data Subject. Specific conditions may be laid down for the transfer. The DPA must inform the European Commission and the other Member States of the authorizations granted pursuant to this provision.

The transfer of Personal Data to third countries may be carried out without authorization from the DPA on the basis of contracts in accordance with the standard contractual clauses approved by the European Commission (EU standard model contracts), provided that the wording of these contractual clauses is not amended.

Further, transfer of data to the entities established in the US may take place without authorization if the entity in question is EU-US Privacy Shield-certified. However, this does not apply for transfers of Sensitive Personal Data where such authorization still is necessary.

Groups of companies where the entities are established in many different jurisdictions may, with advantage, choose to prepare a set of binding corporate rules (“BCR”) for data transfers within the group. The binding corporate rules must be approved by a supervisory authority in one of the EU Member States. Usually, the BCR are submitted to the supervisory authority in the Member State where the group has its headquarters or main office (the so-called leading supervisory authority). The leading supervisory authority will coordinate the approval process with the other involved local data protection supervisory authorities within the EU and often choose one or more co-reviewers. When the approval is granted, no separate local approval of the BCR in Denmark is necessary. However, as Denmark is not part of the mutual recognition scheme, a separate approval for the transfer based on the BCR must be obtained from the DPA. In addition, it is important to note the BCR will solely be basis for legal transfer of data, so disclosure of data will be subject to all the applicable data protection laws.
12. Security Requirements

The Data Controller must implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Data Protection Act. The same applies to Data Processors.

In practice, this means that the entities must ensure limited and only authorized access to the data, effective procedures in this respect, use of passwords, firewall or other antivirus programs, encryption, etc. Where Personal Data is transferred through the internet, it must be done through a secure connection and encryption is, under certain circumstances, a requirement.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

The Data Controller may outsource the processing of data to a third party, under the assumption that the Data Processor acts in accordance with the instruction from the Data Controller, and that any action taken by the Data Processor will be considered as made by the Data Controller. The Data Controller must ensure the Data Processor's compliance with the Data Protection Act.

14. Enforcement and Sanctions

If the Data Controller breaches his/her obligations under the Data Protection Act, or does not act in accordance with a decision made by the DPA, the Data Controller may be liable for a fine or punished with imprisonment of up to four months (individuals only). However, imprisonment as a sanction is very unlikely.

In Denmark, the level of fines is rather low – between DKK 3,000 and DKK 10,000 (EUR 403 to EUR 1,343). As mentioned in Section 1, the highest fine until now amounted to DKK 25,000 (EUR 3,360).

Selling access to a non-public protected information system, which contains Personal or Sensitive Personal Data, can be punished with imprisonment of up to six years in severe cases. This applies to individuals only.

In addition, any breach of the obligations under the Data Protection Act may constitute grounds for liability to the extent the Data Subject suffers damages, should these be monetary or integrity related.

15. Data Security Breach

Currently, there is no requirement to notify the Data Subjects or the DPA when a data security breach occurs.
However, the DPA requires that in situations where Personal Data have been leaked to the public against the rules of the Data Protection Act, the Data Controller must, depending on the situation and the particular circumstances, as soon as possible attempt to:

- delete the data from the Internet, search engines, etc.;
- have the data returned from the wrong receivers;
- notify the relevant Data Subjects; and
- implement long-term measures to ensure that such incidents will not take place in the future.

16. Accountability

The Data Controller does not have any legal obligation to prepare documents like privacy policies, IT policies, internal guidelines or description of internal procedures, etc., or to generally document any data protection impact assessments. However, the reality is that such documents often provide the necessary or appropriate solutions for fulfilling the obligations under the Data Protection Act, such as providing the necessary information to the Data Subjects or ensuring the Data Processor’s compliance with the provisions of the Data Protection Act.

17. Whistle-Blower Hotline

Whistle-blower hotlines are permissible in Denmark subject to prior approval from the DPA. The DPA generally takes the view that such hotlines should be a voluntary alternative to the entity’s usual lines of communication. Thus, it should not be mandatory for the employees to raise their concerns through the whistle-blower hotline.

Only reporting of serious offenses are permissible via the hotline, e.g., offenses that amount to serious misconduct or suspected serious misconduct which may affect the entity as a whole or which may have a decisive impact on the life and health of individuals. Such matters are undoubtedly serious economic crime, including bribery, fraud, forgery and similar offenses as well as irregularities in the areas of accounting and auditing, internal controls or financial reporting, anti-competition and insider trading. Other examples of incidents that may be reported include cases of environmental pollution, serious violations of occupational safety rules and serious offenses against an employee, for instance violence or sexual offenses.

Further, the DPA has accepted that incidents falling within the US Sarbanes-Oxley Act may be reported, e.g., accounting, internal control and audit irregularities, and suspected corruption and banking crimes.
However, less serious misconduct should not be capable of being reported, including for example cases of mental bullying, collegial difficulties, incompetence, absence, and breach of dress codes, smoking and alcohol policies and workplace rules on the use of emails/Internet, etc. In cases like this, the usual lines of communication should be used instead.

Finally, the Data Protection Act requires the whistle-blower hotline to be designed only with a view to reporting persons who are related to the entity such as employees, members of the board of directors, auditors, lawyers, suppliers etc.

The entity has the obligation to inform its employees of the existence and the functions of the whistle-blower hotline and must also have specific procedural rules on how to handle the given information, both concerning the person reporting the incident and the Data Subject.

Anonymous reporting is permissible, if necessary; however, employees and board members should not be encouraged to report anonymously.

Prior to implementation of the whistle-blower hotline, the entity must submit an application to the DPA, which will trigger an administrative fee of DKK 2,000 (approximately EUR 270) upon approval. The entity must also submit an application for processing of Personal Data in the HR department, unless such approval has already been granted by the DPA (the fee of DKK 2,000 (approximately EUR 270) applies here as well).

The Danish Financial Business Act contains a specific set of whistle-blower rules that are applicable to the financial sector, which came into force on 1 September 2014. These rules require all financial institutions to implement a mandatory whistle-blower scheme that must offer:

- a special, autonomous and independent report channel (meaning independent of the daily management of the entity);
- the ability to report any violation of the applicable financial rules, regardless of the significance of the suspected violation;
- the ability to file a report anonymously;
- the ability to file a report for all Danish employees (no requirement about access to file reports for employees of other group entities or third parties); and
- the ability for the employees to file a report on the entity as such, on other employees and/or on board members.

In this respect, the interpretation of “financial institutions” is fairly broad and includes mortgage-credit institutions, investment trusts, financial services
advisers, company pension funds, banks, financial services companies and securities services.

As for the voluntary whistle-blower schemes, the financial institution in question must submit an application to the DPA and await its approval, prior to the implementation of such scheme. In addition, the institution must submit an application for processing of Personal Data in the HR department, unless such approval has already been granted by the DPA. The fee for approval of each application is DKK 2,000 (approximately EUR 270).

The scheme may be outsourced to a third party, either a supplier of whistle-blower hotline solutions or, for example, an intra-group entity, but the responsibility for ensuring compliance with the requirements under Danish law remains with the financial institution in question.

18. E-Discovery

In Denmark, e-discovery is not used in civil litigation and will only be relevant in criminal cases.

19. Anti-Spam Filtering

As anti-spam filter solutions involve monitoring, the employees must be informed of the implementation of such a measure. Please see Section 4(f).

20. Cookies

The use of cookies is regulated by Executive Order No. 1148 of 9 December 2011 on Information and Consent Required in Case of Storing and Accessing Information in End-User Terminal Equipment (the "Cookie Order"), which is based on EC Directive No. 2002/58/EF of 12 July 2002. The Cookie Order requires collection of explicit and informed consent from the user prior to placing cookies on the user’s computer or other electronic device.

The user must be provided with comprehensive information about the storing of, or access to, the information collected via cookies. The information will be regarded as sufficiently comprehensive if:

a. it appears in a clear, precise and easily understood language or similar picture writing;

b. it contains details of the purpose of the storing of or access to information in the end-user’s terminal equipment;

c. it contains details that identify any natural or legal person arranging the storing of, or access to, the information (e.g., also third parties);

d. it contains accessible means by which the end-user can refuse consent or withdraw an already given consent;
e. it contains clear, precise and easily understood guidance on how the end-user should make use thereof; and

f. it is made immediately available to the end-user by being communicated fully and clearly to the end-user.

The Danish Business Authority, which is the supervisory authority overseeing the use of cookies, has issued guidelines on the Cookie Order. See the English version of the guidelines here: https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf

21. Direct Marketing

Use of Personal Data for the purposes of the Data Controller’s own direct marketing must comply with the general processing rules (please see Section 7).

In addition, the Data Protection Act contains specific rules on disclosure of consumer-related Personal Data to third parties or use of such data on behalf of third parties for the purpose of marketing. The disclosure or use of such data for that purpose is subject to the consumer’s prior explicit consent. However, the disclosure or use of such data may take place without consent, if the disclosure/use relates to general customer data which form the basis for classification into customer categories, provided that (i) the rule of balancing of interests justifies such disclosure/use (please see Section 7(f)) and (ii) the Data Controller observes the objection procedure.

Thus, the entity must – prior to any disclosure or use of data – check the Central National CPR Register for markings, e.g., whether the consumer in question has filed a statement to the effect that he/she does not wish to be contacted for the purpose of marketing activities. If the consumer has not given such information to the CPR Register, the entity must inform the consumer about the right to object to the intended disclosure/use in a clear and intelligible manner. The consumer must also be granted an opportunity to object to the disclosure/use in a simple manner within a period of 14 days. The data may not be disclosed/used until the time limit for objecting has expired.

The entity may not demand any payment of fees in connection with objections.

In Denmark, direct marketing is also regulated by other legislation. Pursuant to the Danish Marketing Practices Act, an entity may not contact anyone (e.g., consumers, other companies, public bodies, etc.) by electronic means (e.g., email, text messages, MMS, etc.) for the purposes of direct marketing without their prior, explicit consent. A very narrow exemption from this rule relates to situations where the person in question, through earlier contact to the entity,
has given his/her contact information when purchasing good or services. Under these circumstances, the entity may communicate marketing messages, but only with regard to the same types/categories of products or services as those purchased by the person in question on earlier occasions. At the same time, the person in question must have a possibility to unsubscribe to such marketing messages, and such un-subscription actions must be without cost and must generally be carried through in an easy manner.

Direct marketing via ordinary mail is allowed subject to prior check of markings in the CPR Register, cf. above.

Moreover, direct marketing to consumers via phone is subject to the consumer’s prior consent, cf. the Danish Consumer Contracts Act. Particular areas are exempted from this requirement, for example, insurance contracts and subscriptions for newspapers and magazines.
Finland

Samuli Simojoki
Helsinki
Tel: +358 40 571 3303
samuli.simojoki@borenius.com

Louna Taskinen
Helsinki
Tel: +358 40 935 5326
louna.taskinen@borenius.com
1. Recent Privacy Developments

In Finland, the Ministry of Justice (“MoJ”) appointed in 2016 a working group, consisting of representatives of all government departments and some representatives of private sector organizations, with the lead responsibility for the implementation of the General Data Protection Regulation (the “GDPR”) in Finland. One of the main tasks of the working group was to review the current Finnish Personal Data Act (523/1999) (“PDA”), implementing Directive 95/46/EC, in the light of the GDPR and to determine whether such general Act on data protection is still needed as well as whether and how the GDPR opening clauses should be implemented in the national legislation.

The MoJ working group finished its work in the end of May 2017. On 21 June 2017, the Ministry of Justice published a committee report based on the work of the working group proposing that the PDA currently in force shall be repealed and a new Finnish Data Protection Act implementing national legislation making use of the GDPR’s opening clauses shall be adopted. The committee report included a proposal for a government bill on the Finnish Data Protection Act.

To the extent possible and appropriate, the MoJ working group retained the provisions of the current PDA as the starting point for the proposed Data Protection Act and some of the provisions currently in force have been retained as is, such as the provision on the processing of personal identification number.

Essential propositions of the MoJ working group are the following:

- The provisions of the proposed Act, as well as mutatis mutandis the GDPR, shall apply to the processing of Personal Data in Finland also in course of activity which falls outside the scope of Union law and also to the processing of Personal Data carried out by Finnish authorities when implementing the activities covered by Chapter 2 of Title V of the TEU. However, should there be any legislation providing otherwise, the proposed Act and the GDPR (mutatis mutandis) shall not be applied. For example, the processing of Personal Data by the Finnish Defence Forces and certain entities within the Ministry of Interior are subject to special legislation and would thus be largely excluded from the scope of the proposal.

- Due to the fact that the current PDA provides for a more detailed legal basis for the processing of Personal Data than the GDPR, the working group proposed that the legal basis for the processing of Personal Data in certain situations shall be supplemented by the provisions of the proposed Act. An example of such proposition is an insurance company’s right to process Personal Data as well as special categories of data collected in the course of its insurance activity and relating to the state of
health, illness or handicap of the policyholder/claimant or the treatment or other measures directed at the policyholder/claimant, where the processing of such data is necessary for the determination of the liability of the insurance company.

- In regard of Article 8 of the GDPR, the working group did not reach consensus of the age limit for when a child can give a lawful consent. However, the working group stated in its report that both the age limits 13 and 15 are possible. This issue will be resolved later on or in sectoral laws that include provisions on the processing of Personal Data.

- The current central government data protection authorities, the Data Protection Ombudsman and the Data Protection Board, shall be replaced by a single authority, a Data Protection Agency. The Data Protection Agency would continue the operations of the Data Protection Ombudsman with certain internal organizational changes.

- Certain exceptions to the provisions of the GDPR were proposed in order to integrate the protection of Personal Data and the freedom of speech and expression. In addition, some derogations from certain provisions of the GDPR were proposed to the processing of Personal Data for the purposes of scientific and historical research as well as statistical purposes.

After its publication in June, the committee report was on circulation for comments. The deadline for comments was 8 September 2017, after which a final proposal (i.e., a government bill) is to be drawn up and submitted to the Parliament. After the parliamentary proceedings, the proposed Act is to come to force on 25 May 2018. At the time of writing, the government bill for the Finnish Data Protection Act was not published and no further specifics on the schedule of the parliamentary proceedings are available.

On 27 January 2017, the MoJ published a report concerning the European Union data protection reform. The report was prepared in cooperation with the Finnish Data Protection Ombudsman and it issues general guidance for organizations on how to prepare for the upcoming GDPR.

On 19 April 2017, the working groups of the Ministry of the Interior ("MoI"), the Ministry of Defense ("MoD") and the Ministry of Justice published and submitted to the relevant ministries their reports on the future intelligence legislation in Finland. Up until now, there has been no uniform intelligence regulation in Finland, and especially in the field of military intelligence, the current legislation is scarce. In their report, the working groups of MoI and MoD proposed that two comprehensive intelligence acts shall be adopted; one on the field of civilian intelligence and another on the field of military intelligence.
Further, the working group of the MoJ proposed that the wording of Section 10 of the Finnish Constitution (right to private life) shall be amended. The current wording of Section 10 of the Finnish Constitution strongly limits the grounds on which the confidential communications can be intervened, and thus the civilian intelligence legislation can not effectively be implemented in a way that the needs for ensuring the protection of national security would be met within the wording of the present Section 10.

After their publication, the reports of the working groups of MoI and the MoD were on circulation for comments, after which the final government bills are to be drawn up and submitted to Parliament during the autumn season of 2017 or in the beginning of year 2018 at the latest. The period for giving comments ended in the last half of June, but at the moment of writing this, the government bills for neither the civilian intelligence legislation nor the military intelligence legislation has been published.

2. Emerging Privacy Issues and Trends

The role of civilian intelligence legislation: fighting against serious threats to national security or dispossessing the citizen’s right to privacy

The juxtaposition of the need for civilian intelligence legislation and the thereto-related privacy concerns is a matter that regularly emerges as a topic for public discussion. The issue was topical again after the first terrorist attack since the end of Second World War took place in Finland in August 2017.

The public debate is directed at the proportionality of the intelligence operations as well as the targeting of the operations (and preventing “mass surveillance”), but the question relating to bringing into force the legislation is also somewhat political. Due to the current situation where there is no comprehensive surveillance legislation in place in Finland, the government parties wish to bring the civilian and the military surveillance legislations into force through accelerated procedure, which would require that 5/6 majority of the members of the parliament would vote in favor of the proposed legislation.

Both the MoD and the MoI working groups underline in their reports – and have later on been supported in the public by the representatives of the said ministries – that basic and human rights have been taken into detailed consideration in drafting the draft proposals, and that the importance of ensuring that the intelligence operations are subjected to internal and external oversight, has been recognized. Whether or not due to the public debate regularly arising, it seems that the submission of the government bills to the Parliament has been re-scheduled from the autumn season of 2017 to the beginning of year 2018.
3. Applicable Law

The general data protection law currently in force in Finland is the Personal Data Act (523/1999) ("PDA"), by which the EU Data Protection Directive (95/46/EC) was implemented in Finland. On 25 May 2018, the PDA shall be repealed and replaced by a new Finnish Data Protection Act implementing national legislation making use of the GDPR’s opening clauses.

http://www.finlex.fi/fi/laki/ajantasa/1999/19990523


The Act on the Protection of Privacy in Working Life (759/2004) ("APPWL") governs data protection in working life, by laying down provisions on such matters as the processing of employees’ Personal Data, the processing of information on drug use, camera surveillance in the workplace and retrieving email messages that belong to the employer. It is not yet known, whether the material provisions of the APPWL will be affected by the GDPR, but among the privacy professionals, it is widely expected that no dramatic changes will be seen.


Under the Information Society Code (917/2014) ("ISC") relevant provisions on electronic communications and providing information society services are drawn together in one act, repealing many of the previously effective acts on different fields of electronic communications. In practice, provisions in relation to several important areas, such as telecommunications, protection of privacy and confidentiality of messages, domain names, electronic marketing and cookies are under this act. The ISC will be subject to need of amendments due to the EU’s ePrivacy Regulation, but before the final contents of the ePrivacy Regulation are clear, it is too early to evaluate the extent of the needed amendments.

http://www.finlex.fi/fi/laki/ajantasa/2014/20140917


There are numerous sector-specific regulations, which include data protection-related provisions. In particular, the processing of Personal Data in health care and social welfare is closely regulated. The status and rights of medical patients and clients of social services are protected by the Act on the Status and Rights of Patients 785/1992 and the Act on the Status and Rights of Social Welfare Clients (812/2000).
4. **Key Privacy Concepts**

The following Key Privacy Concepts that are based on the provisions of the PDA will be applied until the repeal of the PDA on 25 May 2018, after which the definitions and concepts of the GDPR will be applied instead.

**a. Personal Data**

The PDA defines “Personal Data” as any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. Under the Finnish Data Protection Board’s praxis, the PDA also applies to deceased individuals.

**b. Data Processing**

The PDA includes an extensive definition stipulating that the processing of Personal Data shall pertain to the collection, recording, organization, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of Personal Data, as well as other measures directed at Personal Data. In practice, all measures directed at Personal Data are deemed as processing of Personal Data under the PDA.

The PDA does not apply to the processing of Personal Data by a private individual for purely personal purposes or for comparable ordinary and private purposes.

**c. Processing by Data Controllers**

Within the meaning of the PDA, a “Data Controller” conceptually refers to one or several persons, corporations, institutions or foundations, for the use of whom a Personal Data file is set up and who are entitled to determine the use of the file, or who have been designated as Data Controllers by law.

**d. Jurisdiction/Territoriality**

The PDA applies to the processing of Personal Data carried out by Data Controllers who are established in Finland or are otherwise subject to Finnish law. Furthermore, the PDA is applied if a Data Controller is not established within the EU but uses equipment located in Finland in the processing of Personal Data. In such case, the Data Controller shall designate a representative established in Finland.

An exemption has been provided should the equipment be used solely for the transfer of data through the territory of Finland. Based on the preparatory works for the PDA, the mere transfer of data through servers placed in Finland constitutes the use of equipment solely for the transfer of data.
e. **Sensitive Personal Data**

As a primary rule, the processing of sensitive data is prohibited unless a specific derogation is at hand. Within the meaning of the PDA, sensitive data refers to Personal Data relating or intended to relate to:

- race or ethnic origin;
- social, political or religious affiliation or trade-union membership of a person;
- a criminal act, punishment or other criminal sanction;
- the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person;
- sexual preferences or sex life of a person; or
- social welfare needs of a person or the benefits, support or other social welfare assistance received by the person.

The PDA includes a detailed list of exemptions from the prohibition to process sensitive data. The prohibition does not apply:

- if the Data Subject has given an express consent;
- to the processing of data on the social, political or religious affiliation or trade-union membership of a person, where the person has, by his/her own initiative, brought the data into the public domain;
- if the processing is necessary for safeguarding a vital interest of the Data Subject or someone else, should the Data Subject be incapable of giving consent;
- to the processing of Personal Data necessary for drafting or filing a lawsuit or for responding to or deciding of such lawsuit;
- to the processing of data, which is based on the provisions of an act; or
- to the processing of data required for purposes of historical, scientific or statistical research.

In addition, the PDA includes specific conditions for the processing of data collected for example in the course of operations of a health care unit, an insurance company or a social welfare authority.

Data processing is limited also with respect to personal identity numbers. In principle, save for limited conditions and exceptions, ID numbers may be processed only on the Data Subject’s unambiguous consent or by virtue of an act. Also, personal identity numbers should not be unnecessarily included in hard copies printed or drawn up from a Personal Data file.
f. Employee Personal Data

In Finland, the processing of Employee Personal Data is regulated by the APPWL, a special statute applied to processing of Personal Data in the context of working life and supplementing the provisions of the PDA in this context. The APPWL covers the processing of Personal Data of both employees and (mutatis mutandis) the applicants.

Under the APPWL, employers may process Employee Personal Data only in accordance with specific conditions. The processing is permitted only insofar as the data is directly necessary for the employee’s employment relationship (necessity requirement).

It is specifically stipulated in the APPWL that no exceptions can be made to the aforementioned requirement of necessity, not even with the employee’s consent.

When collecting Employee Personal Data, the employer shall, as a primary rule, collect the data from the employees themselves. If data is collected from elsewhere, the consent of the employees concerned is required. Exceptions to obtaining this consent are limited only to situations where an authority discloses information to the employer to enable it to fulfill a statutory duty or when the employer acquires personal credit data or information from the criminal record in order to establish the employee’s reliability.

When data is to be or has been collected from a source other than the employee him/herself, such as when establishing employee reliability, the employer is obliged to notify the employee about the processing and use of the data. The employer must notify the employee of this information before it is used in making decisions concerning the employee.

In addition, the APPWL contains provisions on the processing of employees’ health information. In principle, information concerning an employee’s state of health may be processed only if the information has been collected from the employees themselves or from elsewhere with a written consent from the employees, and if the information needs to be processed in order to pay sick pay or health-related benefits, establish justifiable reasons for absence, assess an employee’s working capacity upon his/her express wish, or if provided elsewhere in the law. Health information may be processed only by those persons who prepare, make or implement decisions concerning employment relationships on the basis of such information.

The collection of Personal Data during recruitment and during an employment relationship is governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings (334/2007), under which employees or employee representatives need to be consulted prior to initiating data processing activities. The Act on Cooperation within Undertakings is applicable if the company concerned regularly employs at least 20 employees.
5. Consent

a. General
Consent is defined in the PDA as any voluntary, detailed and conscious expression of will, whereby the Data Subject approves the processing of his/her Personal Data. The requirement of "unambiguity" underlines the importance of the clarity of the Data Subject's expression of will.

Consent does not necessarily have to be in writing and can be given orally provided that the above-mentioned requirements are fulfilled. According to the preparatory works for the PDA, even an implied consent could, in certain cases, be sufficient to satisfy the set requirements. The Data Subject has the right to withdraw his/her consent at any time.

The requirements that a given consent must satisfy shall, in the last resort, be determinable on a case-by-case basis. In case of dispute, the Data Controller is required to prove that consent exists.

Consent does not supersede the requirement of necessity (see Section 7 below), meaning that the processing of such data which cannot generally and objectively be considered necessary for the purpose of processing is not justified even if the Data Subject has given his/her consent.

As the foregoing regarding consent is based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the definitions and concepts of the GDPR will be applied instead.

b. Sensitive Data
A Data Subject’s express consent constitutes one of the exceptions to the general prohibition to process sensitive data, as stipulated in the PDA. The requirement of “express” consent highlights that the Data Subject’s consent must be expressed in a precise and active manner. An express consent usually has to be given in writing and must indicate the purpose of the processing of Personal Data for which the permission has been granted.

As the foregoing regarding consent is based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the definitions and concepts of the GDPR will be applied instead.

c. Minors
The PDA does not include any specific provisions concerning the consent of minors.

In regard Article 8 of the GDPR (conditions applicable to child’s consent in relation to information society services), the Ministry of Justice’s working party with the lead responsibility in the implementation of the GDPR in Finland (see Section 1) did not reach consensus regarding the age limit for when a child can give a lawful consent. However, the working group stated in its report
(published in 21 June 2017) that both the age limits 13 and 15 are possible. The matter related to acceptable age limit will be resolved later on or in the sectoral laws that include provisions on the processing of Personal Data.

d. Employee Consent

The general requirements concerning consent are applicable to employee consent as well. Under the APPWL, employee consent shall not provide an exception to the requirement of necessity, meaning that the employer is only allowed to process Personal Data directly necessary for the employee’s employment relationship.

Furthermore, the collection of Personal Data during an employment relationship is subject to cooperative procedures under the Act on Cooperation within Undertakings (334/2007). Thus consent given by employees separately from these procedures can be insufficient.

e. Online/Electronic Consent

A Data Subject can give his/her lawful consent in the electronic environment. If Personal Data is collected and processed online, information on the collection and processing must be made available in connection with the online service (e.g., inclusion of a hyperlink to a description of file/privacy notice). If the Data Subject’s consent constitutes the basis for Personal Data processing, all necessary information must be made available to the Data Subject upon giving the consent. The Data Controller must be able to prove that consent has been given.

6. Information/Notice Requirements

When collecting Personal Data, the Data Controller shall see to it that the Data Subject can access information on: (i) the Data Controller and, where necessary, the representative of the Data Controller; (ii) the purpose of the processing of Personal Data; (iii) the regular destinations of disclosed data; and (iv) how to proceed in order to make use of the rights of the Data Subject in respect of the processing operation in question. The aforementioned information shall be provided at the time of the collection and recording of data or, if the data is obtained from a source other than the Data Subject and intended for disclosure, at the time of the first disclosure of data at the latest.

The above-mentioned required information can, in practice, be provided to the Data Subject in a description of file, constituting another necessary requirement for the Data Controller. Under the general rules provided in the PDA, the Data Controller shall draw up a description of the created Personal Data file. The file must indicate the following information:

1. the name and address of the Data Controller and, where necessary, those of the representative of the Data Controller;
2. the purpose of the processing of Personal Data;
3. a description of the group or groups of Data Subjects and data or data groups relating to them;

4. the regular destinations of disclosed data and whether data is transferred to countries outside the EU or the EEA; and

5. a description of the principles in accordance to which the data has been secured.

The Data Controller shall keep the description of the file available to anyone. This obligation may be derogated from if necessary for the protection of national security, defense or public order and security, for the prevention or investigation of crime, or for a supervision task relating to taxation or public finances.

As the foregoing regarding informing Data Subjects is based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the relevant requirements of the GDPR will be applied instead.

7. Processing Rules

The PDA provides a list of general rules, i.e., principles applying to the processing of Personal Data. The rules are and concern the following: duty of care, defined purpose of processing, exclusivity of purpose, general prerequisites for processing, data quality, and the drawing of a description of file (discussed in Section 6 above).

Duty of care

Controllers shall process Personal Data lawfully and carefully, in compliance with good processing practice, and also otherwise so that the protection of the Data Subject’s private life and the other basic rights which safeguard his/her right to privacy are not restricted without a basis provided by an act. Anyone operating on behalf of a Data Controller, in the form of an independent trader or business, is subject to the same duty of care.

Defined purpose of processing

The processing of Personal Data by the Data Controller must be appropriate and justified. The purpose of the processing of Personal Data, the regular sources of Personal Data and the regular recipients of recorded Personal Data shall be defined before the collection of Personal Data. The purpose of the processing shall be defined so that the operations of the Data Controller in which Personal Data is processed are made clear.

Exclusivity of purpose

Personal Data must not be used or otherwise processed in a manner incompatible with the defined purpose of processing. Later processing for the
purposes of historical, scientific or statistical research is not deemed incompatible with the original purposes.

General prerequisites for processing

The consent of a Data Subject constitutes the primary justification to process Personal Data. Should no consent be given, the PDA also enables Personal Data to be processed, if:

- the Data Subject has given as assignment for the same, or the processing is necessary in order to perform a contract to which the Data Subject is a party;
- it is necessary, in an individual case, in order to protect the vital interests of the Data Subject;
- the processing is based on law;
- there is a relevant connection between the Data Subject and the operations of the Data Controller, which is based on the Data Subject being a client or member of, or in the service of the Data Controller or on a comparable relationship between the two (connection requirement);
- the data relates to the clients or employees of a group of companies and it is processed within the said group;
- the processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the Data Controller;
- the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business; or
- the Data Protection Board has issued a permission.

Personal Data may be disclosed on the basis of the above-mentioned connection requirement only if such disclosure is a regular feature of the operations concerned and if the purpose for which the data is disclosed is not incompatible with the purposes of the processing and if it can be assumed that the Data Subject is aware of such disclosure.

Principles relating to data quality

Personal Data processed must be necessary for the defined purpose of processing (necessity requirement). The Data Controller shall additionally see that no erroneous, incomplete or obsolete data is processed (accuracy requirement). This duty of the Data Controller shall be assessed in the light of the purpose of the Personal Data and the effect of the processing on the protection of the Data Subject’s privacy.
As the foregoing processing rules are based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the relevant processing rules of the GDPR will be applied instead.

8. Rights of Individuals

The PDA provides Data Subjects with three fundamental rights, namely the rights of access, data rectification, and the prohibition of processing. Under the PDA, everyone shall have the right to access data on him/her in a Personal Data file or to a notion that a file contains no such data, unless this right has been specifically restricted, e.g., on the basis of a compromise to national security, public order or danger caused to the health of someone.

By the request of the Data Subject, or on its own initiative, a Data Controller shall rectify, erase or supplement erroneous, unnecessary, incomplete or obsolete data from its Personal Data file. The Data Controller shall furthermore prevent the dissemination of such data. If the Data Controller refuses this request, he must, to this effect, provide a written certificate with which the Data Subject may bring the matter to the attention of the DPO.

A Data Subject has the right to prohibit a Data Controller from processing Personal Data for the purposes of direct advertising, distance selling, other direct marketing, market research, opinion polls, public registers or genealogical research.

As the foregoing rights of individuals are based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the relevant provisions of the GDPR will be applied instead.

9. Registration/Notification Requirements

The PDA includes three types of notification requirements. First, the DPO shall be notified of all automatic data processing. There are several exceptions to this rule and, in practice, most data processing does not require notification. General notification applies to, for example, data processing for direct marketing purposes and when outsourcing the processing of Personal Data.

Second, Data Controllers shall notify the DPO regarding Personal Data transfers outside the EU/EEA. There are several exceptions to this rule and, in practice, most international data transfers do not require notification, as there is no obligation to notify the DPO, e.g., when using the European Commission’s standard contractual clauses.

Third, the PDA stipulates that anyone engaged in credit data activity or carrying out debt collection or market or opinion research as a business, or operating in recruitment, personnel assessment or computing on behalf of another, or using or processing files or Personal Data in this activity, shall notify the same to the DPO.
The notification process is not an authorization process. Therefore the Data Controller is always responsible for the lawfulness of its data processing regardless of the notification.

As the foregoing regarding notification rules is based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the relevant requirements of the GDPR will be applied instead.

10. Data Protection Officer

Finnish data protection laws do not include a general obligation as regards the appointment of Data Protection Officers. There are, however, certain specific requirements in the health care sector. The Act on the Electronic Processing of Information of Social Welfare and Health Care Clients (159/2007) and the Act on Electronic Prescription (61/2007) require that, inter alia, providers of social welfare or health care services must appoint a Data Protection Officer for monitoring and supervision duties.

After 25 May 2018, the provisions of the GDPR shall be applied, including the obligation to designate a Data Protection Officer in cases where the preconditions of Article 37 are met, and thus a significantly larger amount of entities in Finland will be subject the obligation of designating a Data Protection Officer.

11. International Data Transfers

The PDA does not include any special restrictions with respect to the transfer of data within the EU/EEA. Personal Data may be transferred outside the EU/EEA only if the country in question guarantees an adequate level of data protection, determined on the basis of the PDA or the findings of the European Commission.

The PDA provides a list of eight derogations enabling the transfer of data outside the EU/EEA. The above-mentioned requirements shall not prevent such data transfer if:

1. the Data Subject has unambiguously consented to the transfer;
2. the Data Subject has given an assignment for the transfer, or this is necessary in order to perform a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject before entering into a contract;
3. the transfer is necessary in order to make or perform an agreement between the Data Controller and a third party and in the interest of the Data Subject;
4. the transfer is necessary in order to protect the vital interests of the Data Subject;
5. the transfer is necessary or called for by law for securing an important public interest or for the purposes of drafting or filing a lawsuit or for responding to or deciding such a lawsuit;

6. the transfer is made from a file from which the disclosure of data, either generally or for special reasons, has been specifically provided in an act;

7. the Data Controller gives adequate guarantees of the protection of the privacy and the rights of individuals by means of contractual terms or otherwise, and the Commission has not found, pursuant to relevant articles of the Data Protection Directive, that the guarantees are inadequate; or

8. the transfer is made by using standard contractual clauses as adopted by the Commission in accordance with the Data Protection Directive.

As the foregoing regarding international data transfers is based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the relevant provisions of the GDPR will be applied instead.

12. Security Requirements

The PDA requires the Data Controller to carry out the technical and organizational measures necessary for securing Personal Data against unauthorized access, accidental or unlawful destruction, manipulation, disclosure, transfer, and other unlawful processing. The available techniques, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out these measures.

In addition, the PDA includes a secrecy obligation. Anyone who has gained knowledge of characteristics, personal circumstances or economic situation of another person while carrying out measures relating to data processing shall not disclose such data to a third person against the provisions of the PDA.

As the foregoing on security requirements is based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the relevant requirements of the GDPR will be applied instead.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

The duty of care, i.e., the general processing rule applying to the Data Controller, applies also to any third party who, in the form of an independent trader or business, operates on behalf of the Data Controller. Thus, the third party shall process Personal Data in accordance with the same principles as the Data Controller (see Section 7). Before starting the processing of data, the third party shall provide the Data Controller with appropriate commitments and other adequate guarantees of the security of data. In practice, compliance
with these requirements is ensured contractually between the Data Controller and the third party to whom data processing activities are outsourced.

Furthermore, the outsourcing of data processing requires a notification to the DPO, should the third party process Personal Data on behalf of the Data Controller.

As the foregoing regarding special rules for the outsourcing of data processing to third parties is based on the provisions of the PDA, it will hold true until the repeal of the PDA on 25 May 2018, after which the relevant requirements of the GDPR will be applied instead.

14. Enforcement and Sanctions

The Finnish Penal Code (39/1889) provides criminal sanctions for Personal Data offense and breaking into a Personal Data file. A natural person can also commit such actions, and thus, e.g., a single employee of an entity may be subject to criminal liability for committing unlawful processing of Personal Data. The foregoing shall be applicable even after the GDPR becomes applicable on 25 May 2018.

A person who intentionally or with gross negligence fails to comply with the provisions of the PDA shall be sentenced to a fine for a Personal Data violation, provided that a more severe penalty is not provided in another act.

A Data Controller is liable to compensate for the economic and other loss suffered by the Data Subject or another person as a result of the processing of Personal Data in violation of the PDA.

The DPO may order the Data Controller to enforce the Data Subject’s right of access or to rectify an error.

The Data Protection Board may, at the request of the Ombudsman, give an order prohibiting the processing of Personal Data in violation of the PDA, compelling a person to remedy an instance of unlawful conduct or neglect, ordering the operations pertaining to a file to be ceased or revoking its permission for processing granted earlier.

The field of enforcement and sanctions is subject to changes due to the GDPR. Thus, without regard the first chapter, the foregoing will hold true only until the repeal of the PDA on 25 May 2018, after which the relevant provisions of the GDPR will be applied instead.

15. Data Security Breach

At the moment Finnish data protection laws do not impose a general obligation to report data security breaches to a governmental body. However, in relation to specific industries and entities, special regulation exists as follows.
The ISC provides notification requirements for Telecommunications Operators, Added Value Service Providers and Domain Name Registrars. According to the ISC, these entities are required to notify the Finnish Communications Regulatory Authority (“FICORA”) of violations of information security and information security threats.

The Act on Strong Electronic Identification and Electronic Signatures (617/2009) provides notification requirements for Identification Service Providers, according to which the Identification Service Providers are required to report severe risks and threats to their data security to FICORA and to the DPO, when the risk or threat concerns Personal Data.

Financial service institutions, e.g., credit institutions and fund management companies, are required to notify the Finnish Financial Supervisory Authority (“FSA”) under the FSA’s standards.

Under the Securities Markets Act (746/2012), listed companies have a general disclosure obligation, based on Article 17 of Regulation (EU) No 596/2014 on market abuse (market abuse regulation), to disclose information materially affecting the value of a security. We note that a material data breach may give rise to such disclosure obligation.

The Act on the Electronic Processing of Client Data in Social and Health Care Services (159/2007) provides certain notification requirements for Healthcare and Social Welfare Service Providers in cases where the service provider finds significant deviations from the fulfillment of essential requirements of a data system in which patient data or client data is processed.

The Finnish Act on Common Administrative e-Service Support Services (571/2016) provides notification requirements for Administrative e-Service Providers and User Organizations.

After 25 May 2018, the provisions of the GDPR relating to notification of a Personal Data breach will become applicable in Finland.

16. Accountability

There is currently no law/regulation/guidance in Finland that mandates Data Controllers to conduct privacy impact assessments or furnish evidence relating to the effectiveness of their data protection management. Pursuant to the PDA, Data Controllers are merely obligated to plan their Personal Data processing activities prior to the collection of the Personal Data.

However, after 25 May 2018, the relevant provisions of the GDPR will become applicable in Finland.
17. Whistle-Blower Hotline

The DPO has published a guide on the implementation of whistle-blower hotlines in Finland-based companies that must comply with the Sarbanes-Oxley Act of the United States (“SOX”). No other official guidance has been given addressing anything other than SOX-based whistle-blowing schemes. The DPO’s guideline can, however, be used as an interpretative tool when assessing other similar whistle-blowing schemes.

In general, whistle-blower hotlines at workplaces are not in conflict with Finnish data protection laws, provided that these systems are designed to comply with the data processing requirements imposed by law, fundamentally the general data protection related legislation and the APPWL (see Section 4 (f)). Upon establishing whistle-blower hotlines, companies should, inter alia, define clearly what types of information may be processed and disclosed therein and limit the data to cover accounting, internal auditing, white-collar crime, and prevention of corruption. The data must be correct and directly related to the employment relationship, and comply, e.g., with the requirements for data security, description of file, informing of Data Subjects, right of access, right of rectification, and so forth.

18. E-Discovery

The ISC allows the employer to access the traffic data of messages (such as the size, aggregate size, type, number, connection mode or target addresses of the messages) if the employer complies with certain detailed requirements. Under the ISC, collection of traffic data is allowed for the purposes of preventing and investigating potential misuses of the employer’s IT systems or unauthorized disclosure of the employer’s business secrets. As a general rule, data may only be processed with the help of an automatic search function that may be based on the size, aggregate size, type, number, connection mode or target addresses of the messages.

The employer must inform employees beforehand about such monitoring through a cooperative procedure. A prior notification must also be submitted to the DPO. Finally, the employer must draw up a report of the manual processing of traffic data including detailed information on the processing. Companies must also annually notify the DPO of any manual processing of traffic data.

19. Anti-Spam Filtering

Messages and identification data may be processed to the extent necessary for the purpose of ensuring information security as provided by the ISC. Such allowed measures include automatic analysis of message content, automatic prevention or limitation of message conveyance or reception and automatic removal of malicious software posing a threat to information security from messages.
20. Cookies

Under the ISC, a service provider may save cookies or other data concerning the use of a service in the user’s terminal device, and use such data if the user has given his/her consent thereto and the service provider gives the user comprehensible and complete information on the purposes of saving or using such data. Implied consent through the use of browser settings is compliant under the ISC and under the guidance issued by FICORA.

The provision above does not apply to any storage or use of data intended solely for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

The aforementioned storage and use of data is allowed only to the extent required for the service, and it may not limit the protection of privacy any more than is necessary.

21. Direct Marketing

Pursuant to the PDA, a Data Subject has the right to prohibit the Data Controller from processing Personal Data for the purposes of direct marketing. A natural person must be able to prohibit such forms of direct marketing easily and free of charge. After 25 May 2018, the Data Subject’s right to object the processing of his Personal Data for purposes of direct marketing will be subject to the relevant provision of the GDPR.

Under the ISC, direct marketing by means of automated calling systems, fax, or email, or text, voice, sound or image messages may only be directed at natural persons who have given their prior consent. A service provider or a product seller may use a natural person’s customer contact information that it has obtained in the context of an earlier sale in direct marketing of its own products of the same product group and of other similar products. The customer shall be clearly and extensively notified of the possibility to prohibit such use of contact information at the time when it is collected and in connection with any marketing message.

Direct marketing to legal persons is allowed if the recipient has not specifically prohibited it. Any legal person shall be allowed the opportunity to prohibit the use of its contact information in direct marketing easily and with no separate charge and be given clear notification of this possibility.
Magalie Dansac Le Clerc
Paris
Tel: +33 1 44 17 59 82
magalie.dansacleclerc@bakermckenzie.com

Yann Padova
Paris
Tel: +33 1 44 17 59 23
yann.padova@bakermckenzie.com
1. Recent Privacy Developments

a. New regulations

Release of the draft legislation on Personal Data protection implementing the “European Data Protection Package” in French law

On 13 December 2017, the Government introduced a draft legislation on Personal Data protection (the “Bill”) and initiated the accelerated procedure.

The discussion of the Bill before the French National Assembly is scheduled for the public sessions of 6, 7 and 8 February 2018.

The purpose of the Bill is to bring national law into line with the “European Data Protection Package” adopted by the European Parliament and the Council on 27 April 2016, which consists of the following texts:

- Regulation (EU) 2016/679 on the protection of individuals with regard to Personal Data, which constitutes the general framework for data protection and is directly applicable from 25 May 2018 (the “GDPR”);

- Directive (EU) 2016/680 on the processing operations carried out for the purpose of preventing, detecting, investigating and prosecuting criminal offenses or carrying out criminal sanctions, to be transposed by 6 May 2018 at the latest, which transposition by the Bill will not be analyzed in this publication.

In order to bring national law into line with the GDPR, the government has made the “symbolic” choice not to repeal the founding law on this matter, the French Data Protection Act No. 78-17 of 6 January 1978 (the “FDPA”).

The Bill minimally adapts the FDPA (1). In addition, while the GDPR is directly applicable, it contains some 50+ opening clauses partly addressed in the Bill (2). Finally, the Bill itself provides that the FDPA may still be subject to major changes at a later stage (3).

(1) The minimal adaptation of the FDPA

The Bill removes from the FDPA provisions contrary to the GDPR and completes it with the necessary provisions, including the following:

- French data protection authority’s (the “CNIL”) missions (Article 1):
  The CNIL will be able to implement tools (guidelines, recommendations, reference documents, codes of conduct, standard security regulations) fulfilling the dual objective of facilitating the compliance of processing operations with the data protection requirements and risk assessment by controllers and their processors. In addition, the CNIL will now be able to approve certifying bodies and certify persons, products and procedures as being compliant with the GDPR and national law.
• **Control methods of the CNIL agents (Article 4):** The CNIL agents will be able to carry out online checks under assumed identities, which conditions will be specified by a decree taken by the Council of State issued after consultation with the CNIL.

• **Cooperation of the CNIL with the authorities of other Member States (Article 5):** When a joint control operation takes place on the French territory, CNIL agents will be present alongside the agents of the other authorities. The CNIL shall communicate to the other authorities the relevant information and may empower their agents to exercise powers of verification and investigation under its control.

• **Measures and sanctions taken by the CNIL (Article 6):** The president of the CNIL will be able to warn controllers and processors of the illegality of the envisaged processing operations or to give them a formal notice, and if they do not comply with the obligations imposed by the GDPR or national law, to refer to the sanction committee. The sanction committee may issue a reminder, an injunction for compliance under a penalty up to EUR 100,000 per day, a temporary or definitive limitation of the processing, the withdrawal of a certification, the suspension of data flows to a third country, the withdrawal of a decision approving a binding business rule or a fine up to EUR 10 or 20 million, or 2% to 4% of worldwide turnover, depending on the obligation not complied with.

• **Sensitive data (Article 7):** The Bill repeats the GDPR ban principle on the processing of sensitive data and expands the current scope of this data. The biometric, genetic and sexual orientation data will now be regarded as sensitive data.

• **Suppression of prior formalities (Article 9):** Most prior formalities, and the entire current prior authorization regime, are abolished and will be replaced by the obligation to carry out a privacy impact assessment when the processing operation is likely to pose a high risk to the rights and freedoms of individuals.

(2) **The approach to opening clauses**

The Bill does not take full advantage of the scope of action left to the Member States by the GDPR but only implements part of it, “judiciously” says the CNIL in its opinion of 30 November 2017, including the following measures:

• **Scope of application of national law (Article 8):** In case of divergent legislation between Member States due to the scope of action left by the GDPR, national law will apply where the person resides in France, even if the controller is not established in France. However, as regards the freedom of expression and information, the law of the Member State in which the controller is established will apply.
• **Prohibition of processing of the social security number (Article 9):**
The Bill provides for a general principle prohibiting the processing of the social security number (the “NIR”). A decree issued by the Council of State, after a reasoned and published opinion of the CNIL, will authorize its use by specific bodies and for limited purposes.

• **Data relating to offenses (Article 11):** The processing of this data may be carried out by legal persons under private law collaborating with the public service of justice. It may also be used by any person who has been the victim of an offense or accused of it in order to prepare and follow the proceedings relating to the offence. Finally, re-users of court decisions will be able to process data relating to offenses for the purpose of making all decisions of the administrative and judicial courts available to the public in open data, subject to respect of the Data Subject’s privacy and after analyzing the risk of re-identification.

• **New remedy for the CNIL on international data transfers (Article 17):**
the draft law implements the decision of the CJEU of 6 October 2015 by allowing the CNIL, in cases in which a data transfer made under an adequacy decision is contested, to lodge a request for the temporary suspension of the data transfer before the Council of State. The Council of State must then refer the question of the validity of the adequacy decision to the CJEU for a preliminary ruling.

(3) **A later significant change to the FDPA?**

In addition to the discussions that will take place in the National Assembly, the Senate and the Joint Committee on the Bill, the FDPA may still be subject to major changes.

Indeed, Article 20 of the Bill empowers the government to **proceed by ordinance to a general rewriting of the FDPA** in order to improve the intelligibility and consistency with all legislation relating to the protection of Personal Data.

Thus, the process of bringing French law into line with the GDPR was only initiated with the presentation of the Bill.

**The Digital Republic Act n°2016-1321 of 7 October 2016**

In October 2014, the French government, through the French Digital Council (Conseil National du Numérique), launched a national consultation on digital technology. This consultation was aimed at helping draft a bill around digital technology issues (the “Bill”). More than 4,000 contributions were received from businesses, government departments and individuals, which were summarized and examined by the Conseil National du Numérique. The findings and proposals were presented to the government on 18 June 2015. The Bill contained several provisions on three main topics: (i) championing
data and knowledge dissemination through the open government data initiative in France; (ii) helping to protect individuals in the digital realm (further summarized below); and (iii) providing universal access to digital technology.

After the consultation, the Bill was reviewed successively by the National Assembly and the Senate. After some debates, the Bill was sent to the Joint Committee. A new draft was published on 29 June 2016. The National Assembly adopted the provisions proposed on 20 July 2016. The Senate discussed the text on 27 September 2016 and the compromised version of the text was finally adopted on 28 September 2016. The enacted version of the law is Law n°2016-1321 of 7 October 2016 (the Act).

The privacy-related provisions are mainly the following:

- The Acts introduces a general right allowing the Data Subjects to decide and control the uses that are made of their Personal Data.

- Consumers have the right to portability and recovery of data. The exercise of this right must be free of charge and applies to all files that are posted online by the consumer and all data arising from the use of the consumer’s user accounts which are available online, except those that have been subject to a significant enrichment by the supplier, and all data related to the consumer’s user accounts where it facilitates the changing of supplier and takes into account the economic importance of the relevant services, the intensity of the competition among providers, the utility for the consumer, the frequency and the financial issues of the use of these services.

- The powers of the French Data Protection Authority, the Commission Nationale de l’Informatique et des Libertés (the “CNIL”), are extended, as it would have to be consulted for every bill or decree related to data protection and processing. Opinions will automatically be published. In addition, the CNIL is now entitled to impose fines of up to EUR 3 million (instead of the former administrative fines of up to EUR 300,000). In emergency circumstances, formal notice from the CNIL for breach of Personal Data protection rules may be reduced to 24 hours.

- The CNIL has now the power to certify, approve and publish standards or general methodologies to certify the compliance of Personal Data anonymization processes with the GDPR, notably for the reuse of public information available online.

- The CNIL may, at the request of an authority having the similar competences in a non-EU Member State, provided that said authority is located in a non-EU Member State offering an adequate protection, proceed to conduct investigations, except for certain categories of data processing. It may even disclose to such authorities information that it
collects or possesses, upon request. In such case, the CNIL will have to enter into a convention governing its relationships with said authority. Such convention will be published in the official journal.

- The Act establishes that the parents or legal guardian of natural persons under the age of 18 receive the information regarding the data processing and exercise the Data Subjects’ rights. However, for certain types of medical research mentioned in the Public Health Code, natural persons above the age of 15 may object to their parents or legal guardian accessing the Personal Data about them that has been collected and processed in the context of medical research, and may exercise alone the right to access and rectify data and the right to object to the processing.

- The Act sets forth a fast track procedure to ensure the right to be forgotten for minors (e.g., natural persons under the age of 18). Such provision will have to be made consistent with the GDPR.

- The Act provides for a strengthening of the information obligation. The Data Controller must provide Data Subjects information related to the retention period of their Personal Data, or if that is not possible, the criteria used to determine said period.

- The Act provides provisions on digital data management after death: Internet users are able, during their life time, to give instructions regarding their data after their death and to appoint a person responsible for carrying out their instructions. ISPs have to inform the about what will happen to their data after their death and let them choose whether they wish to transfer them to a third party or not. This provision will have to be made consistent with the GDPR.

b. News from Authorities

CNIL’s “connected vehicles and personal data” compliance package

On 17 October 2017, in an effort to extend “compliance packages” to include smart meters, public housing, and insurance, the CNIL published its compliance package on “connected vehicles and personal data”. This package is the result of more than two and a half years’ work in collaboration with players in the automotive industry, and companies from several other business sectors including insurance, telecoms and public authorities.

This tool is designed to enable professionals to comply with the GDPR. This involves incorporating Personal Data protection, beginning in the vehicle’s design phase (privacy by design and by default), and ensuring that users have control over their data.
A particularly broad application

The field of application of the compliance pack is based on a broad definition of Personal Data. Thus, the CNIL considers a vehicle’s usage data to be personal (for example, the data relating to the driving behavior or the number of kilometers traveled) as well as the technical data (such as data relating to wear on the vehicle’s parts) which, by cross-checking with other files, can be associated with a given individual.

Initial application of the right to informational self-determination

The pack includes a series of founding principles and obligations from recent laws, some of which are being implemented for the first time. This is notably the case of the right to “informational self-determination”. By virtue of this right “everyone has the right to decide and control how [his/her] data are used (...)." Applied to connected vehicles, this right specifically translates into default settings that protect privacy, by for example establishing configurable dashboards enabling the user to easily access his/her data.

In addition, the CNIL provides useful clarifications on the notion of “data relating to criminal offences”, the processing of which is prohibited except in exceptional cases. Thus, the CNIL states that instantaneous vehicle speed, which is likely to reveal the commission of a criminal offense, “is not data relating to a criminal offence by nature because it is not sufficient to establish such an offence in itself and alone”. On the other hand, instantaneous speed is a data relating to criminal offences “by destination”, i.e. according to the purpose pursued. This is therefore a case-by-case assessment, depending on the purpose of the data collection, to be carried out by the controller in order to determine the legal qualification of the processing of instantaneous speed data.

Scenarios based on the data communication circuit

The CNIL is considering three scenarios based on the “data circuit” already used in previous Packs.

- **Scenario no. 1 “IN ⇒ IN”:** data collected in the vehicle stays in the vehicle
- **Scenario no. 2 “IN ⇒ OUT”:** data collected in the vehicle is transmitted externally to provide a service for the Data Subject.
- **Scenario no. 3 “IN⇒OUT”:** data collected in the vehicle is transmitted externally to trigger an automatic action within the vehicle.

Once the most appropriate scenario has been identified for each service, the Data Controller will be able to rely on the compliance pack to understand the conditions under which the processing may be implemented (legal basis, purpose of processing the data, which data is collected, etc.) and what its
obligations are (concerning Data Subjects’ information and data rights, as well as security measures).

**A pack designed to be widely adopted at the European level**

In its press release of 17 October 2017, the CNIL stressed that the pack is upgradable and intended to be updated after the entry into force of the GDPR. Also specified is the fact that the pack is intended to be rolled out Europe-wide in order to enable French players to position themselves in the EU market. Ms. Falque-Pierrotin (Chair of the CNIL) appears to be taking advantage of the French chairmanship of the Art. 29 Working Party to give a European dimension to the French compliance pack, and to strengthen the consensus already established by the opinion issued by the Art. 29 Working Party on 4 October 2017.

**Single Authorisation AU-054, 13 July 2017 related to the fight against external fraud in the banking and financial sector**

On 13 July 2017, the CNIL adopted a Single Authorisation AU-054 in relation to the processing of Personal Data implemented to fight against external fraud in the banking and financial sector that allows financial organizations to carry out detection of anomalies and management of operations qualified as external fraud within the meaning of article 324 of the EU Regulation 575/2013 dated 26 June 2013 on prudential requirements for credit institutions and investment firms without having to apply for a normal authorization with the CNIL.

The data processing activities covered by AU-054 are:

1. The detection of acts performed in the context of the contracting process, and the management and performance of contracts that show an anomaly or inconsistency;
2. The management and analysis of alerts coming from various sources of information (internal control processes, client claims, judicial order and reports made by employees);
3. The compilation of lists of persons duly identified as fraudsters or attempted fraudsters further to investigations.

It sets out the conditions for data retention. As such, financial institutions have 12 months from the issuance of alerts to qualify them. Any qualified irrelevant alerts will be deleted immediately. Alerts that have not received any qualification at the end of the 12-month period are deleted. In the event of a relevant alert, data relating to proven fraud shall be kept for a maximum period of five years from the closure of the fraud file. Data relating to persons entered on a list of known fraudsters shall be deleted after five years from the date of entry on that list. Where legal proceedings are initiated, the data shall
be retained until the end of the legal proceedings. They are then archived according to the applicable statutory limitation periods.

The AU-054 provides strict conditions for access to data. As a general rule, only specially authorised personnel should have access to the detection system and data collected. These include inspectors, investigators, auditors and experts, within the framework of investigations, authorised anti-fraud staff in the entity concerned or in another entity of the group responsible for combating fraud when acting on behalf of the entity, authorised personnel in charge of combating money laundering and terrorist financing within the entity.

There is an obligation to provide information at two levels:

- Data Subjects shall be informed that the controller is implementing a system designed to combat fraud which may, in particular, lead to the inclusion on a list of persons responsible for acts qualified as fraud or attempted external fraud; and

- The Data Subject may submit his or her observations if a decision giving rise to legal effects is taken in respect of him or her in connection with the conclusion or performance of the contract. If, after investigation, a decision with legal effects is taken, the Data Subject shall be informed individually of its consequences.

With regard to security and confidentiality, the controller shall take all necessary precautions to maintain the security of the processed data, in particular to prevent it from being distorted, damaged or accessed by unauthorized third parties.

**Adoption of Single Authorization No. 46 by CNIL**

The CNIL has adopted a Single Authorization No. 46 (Deliberation No. 2016-005) on 14 January 2016 related to the processing of Personal Data by public or private entities for the preparation, exercise and tracking of their litigation proceedings and for the enforcement of judgments. The Single Authorization allows for a streamlined and simplified declaration of compliance, as long as data processing complies with the conditions set forth in the CNIL decision No. 2016-005.

To benefit from this Single Authorization No. 46, the purpose of the data processing must be limited to the preparation, exercise and tracking of litigation actions and for enforcement of judgments. Data collected must not exceed: identification data (name, use name, gender, date and place of birth, nationality, address, telephone and fax numbers, email address) of respondents, victims, witnesses and judicial officers.

Data retention must be limited depending on the nature of the procedures. Data processed to manage pre-litigation should be removed upon the
amicable dispute settlement or the term of the applicable statute of limitation. Data processed to manage litigation must be removed when a decision may no longer be appealed and may already be enforced.

Recipients of such Personal Data processing must be limited to: employees responsible for the data processing entitled to prepare and manage litigation in their duties, the other persons responsible for processing the data due to their functions (e.g., auditors), subcontractors of the controller, judicial officers and ministerial officers (e.g., lawyers, bailiffs, notaries), and the relevant jurisdiction.

**Deliberation No. 2016-263 of 21 July 2016 approving the new methodology “MR-003”**

This new methodology issued by the CNIL applies to the processing of Personal Data implemented within the framework of health studies that do not require the prior and express consent of the Data Subject. The Data Controller has to notify the CNIL of its commitment to comply with the provisions of the methodology to obtain such authorization. The following categories of research can benefit from this simplified process (save for the exceptions provided by the methodology):

- clinical trials to which the Data Subjects did not object once informed;
- research to assess current care; and
- non-interventional research organized and performed on/with natural persons for the development of biological, medical or health knowledge and during which all actions are performed and products used habitually, without additional or unusual procedure of diagnosis, care or monitoring.

**CNIL’s Annual Activity Report for 2016**

On 27 March 2017, the CNIL published its Annual Activity Report for 2017 summarizing its various accomplishments in 2016, as well as the major challenges and topics that the CNIL are considering in 2017.

The Report notably provides figures on the number of complaints, investigations and sanction processes conducted in 2016:

- Of the 7,703 complaints received, 33% relate to e-reputation issues (e.g., deleting online content, fake online profiles, etc.), 33% relate to marketing issues (e.g., marketing email opt-out, etc.), 14% to labor-related issues (e.g., video surveillance, refusal to communicate the professional record, etc.), 9% to bank/credit issues (e.g., registration on the incidents payment file), and 3% to health issues (e.g., access to medical record, constitution of pharmaceutical record without consent etc.).
• Of the 430 inspections which were conducted in 2016, 94 of those were targeted at video surveillance and 101 were operated online, in accordance with the new powers granted to the CNIL by the Hamon law of 17 March 2014. A total of 82 notices (warning) have been addressed, but only 13 sanctions were pronounced and among these sanctions, four have been published.

**CNIL’s New Program of Control for 2017**

On 31 March 2017, the CNIL revealed its New Program of Control for 2017. It outlines that 2017 is a special year, as it continues to prepare for the implementation of the GDPR.

CNIL will continue the implementation of complex strategies of control, combining on-the-spot, on-evidence, on-call or on-line controls. In collaboration with the other G29 members, CNIL prepares the implementation of the cooperation procedures provided for in the GDPR.

CNIL intends to pronounce much higher penalties, as the law of October 2016 began to anticipate, multiplying by 20 the penalties that can already be pronounced by the CNIL. It also provides for new cooperation mechanisms between European authorities, starting with joint control operations.

In 2017, the focus of CNIL controls will be related to people in their everyday life and to sensitive state data files in both public and private sector including: (i) the confidentiality of health data processed by insurance companies (e.g., control the compliance of insurance companies with medical confidentiality two years after the adoption of the compliance act). (ii) Intelligence data files relating to state security, defense or public security (e.g., PASP Prevention of Public Safety Violations; GIPASP information Management and Prevention of Public Security Violations; EASP Administrative Investigations Related to Public Security STARTRAC anti-whitening file;). CNIL’s control will focus on the general functioning of these files as well as the compliance regulations. (iii) Smart TV (control the accuracy of the information collected, the processing purpose and security measures.

CNIL’s controls will be carried out as follows (i) 40% controls after warnings, demands, penalties or press releases (ii) 25% from its annual program of control, (iii) 20% from complaints, and (iv) 15% will be specifically dedicated to the verification of video surveillance and video protection devices.

2. **Emerging Privacy Issues And Trends**

a. **Current tendency in the CNIL’s sanctions**

The current tendency of the CNIL is to impose a sanction on the Data Controller for a security breach, even where the controller is not aware of the security measures implemented by the Data Processor, including most recently:
• Ruling No. SAN-2017-010 of 18 July 2017: A Personal Data breach occurred in 2016 on a car rental company site due to an error made by a provider. The CNIL pronounced a sanction of an amount of EUR 40,000, considering that the company had failed in its obligation of security of the data. An online verification enabled the CNIL agents to access from an URL address Personal Data collected from more than 35,000 persons who had signed up for a discount program via a website. The data breach was the result of an error made by the service provider during a server change operation. Nevertheless, the CNIL considered that the security breach resulted from the controller’s negligence in (i) monitoring the actions of its Data Processor and (ii) taking all necessary precautions to prevent unauthorized third parties from gaining access to the data processed. Consequently, a EUR 40,000 fine was imposed on the car rental company.

• Ruling No. SAN-2017-012 of 16 November 2017: The CNIL has pronounced a sanction of an amount of EUR 25,000 against the publisher of four sites of online administrative procedures having left freely accessible data of its users. The CNIL considered that the company had failed to ensure the security and confidentiality of its customers’ data. The CNIL agents followed the usual itinerary of administrative procedures of several websites edited by the defendant and found that once an online application form was completed, a summary page of the application was displayed. By modifying the number in the URL address of the summary page, they could access the pages of hundreds of thousands of other users of the websites. It appeared the identified defect was caused by the absence of implementation of the most basic security measures when designing the websites (URL filtering and users authentication process). Consequently, a EUR 40,000 fine was imposed.

• Ruling No. SAN-2018-001 of 8 January 2018: The CNIL pronounced a sanction of EUR 100,000 against a company (the Data Controller) for not having sufficiently secured the data of customers making online request for after-sales service. A security breach provided free access to all requests and data entered by the Data Controller’s customers via an online form. The customer service management tool was provided by the Data Processor as an “off the shelf” solution. It appeared the Data Processor never proceeded to the URL filtering basic set up which would have prevented unauthorized third parties from accessing the customer data contained in the service request management tool via the defective form. The Data Controller argued that it did not know of the existence of this form, never ordered it nor accepted it. CNIL considered that the mere fact that Data Controller uses a subcontractor does not relieve it of its obligation to preserve the security of the data processed on its behalf. The CNIL decided that DARTY should have made sure beforehand that
the tool configuration set up implemented on its behalf did not allow unauthorized third parties to access customer data. Consequently, a EUR 100,000 fine was imposed on the Data Controller.

b. 2017 Sweep Days

In October 2017, the CNIL issued a communication on its website about the sweep days carried out by 24 data protection authorities, all members of the Global Privacy Enforcement Network. The purpose of the sweep days was an audit of the websites and mobile applications in the e-commerce, banking, travel, social networking, gaming, health and education sectors, in order to assess the quality of the information provided to the persons about (i) the purpose of data collection, (ii) their rights, (iii) the sharing of their data with third parties, (iv) the security and confidentiality measures applied to their data, and (v) the right of access to their data and request their erasure.

This international audit has revealed unclear privacy policies, generally unsatisfactory information about the fate of the data and the nature of the organizations with which it is shared, the lack of information on safeguards taken to ensure the security of users’ data, the lack of clarity about the country hosting the data and protection measures implemented.

The CNIL eventually revealed some figures in this regard, including that 82% of sites and applications insufficiently inform people about the nature of the data transmitted to third parties and their identity, and provide little or no information on how data is stored and the measures taken to ensure its security and confidentiality. Generally speaking, the CNIL noted that internet users are not sufficiently informed and are not in a position to exercise their rights to access or to erase their data.

Websites that have revealed the most significant malfunctions during the audit will be subject to further investigations as part of formal control procedures. Such coordinated audit actions are a way for the CNIL and its European counterparts to prepare themselves for future joint operations that can be carried out in accordance with the GDPR.

3. Law Applicable


4. Key Privacy Concepts

a. Personal Data

LIL applies to the processing of any information (“Personal Data”) which directly or indirectly allows for the identification of an individual (“Data Subject”).
b. **Data Processing**

“Processing” is extremely widely defined and covers any operation or set of operations performed on Personal Data including collection, recording, organization, storage, consultation, use, disclosure by transmission and deletion.

LIL applies to both manual and automated data processing.

c. **Processing by Data Controllers**

LIL applies to persons who determine the purposes for which and the manner in which any Personal Data are, or are to be, processed (“Data Controller”).

d. **Jurisdiction/Territoriality**

LIL applies to:

- data processing activities carried out by Data Controllers established in France; and/or
- data processing activities carried out by Data Controllers established outside the EU that make use of equipment located in France (other than merely for the purposes of transit).

e. **Sensitive Personal Data**

LIL prohibits the processing of Sensitive Personal Data – that is, Personal Data directly or indirectly relating to racial or ethnic origins, political opinions, trade union membership, religious or philosophical beliefs, health or sexual life. However, Sensitive Personal Data can be processed if the purpose of the processing justifies it, and provided one of the following conditions is met:

- the Data Subject has given his or her express (i.e., written) consent subject to certain restrictions;
- the processing is necessary in order to protect the vital interests of an individual, and the Data Subject is unable to express his or her consent (where the Data Subject is physically or legally incapable of giving consent);
- the processing is carried out by churches or religious, philosophical, political or union organizations, for the purpose of keeping records of their members or correspondents;
- the Personal Data in question has been made public as a result of steps deliberately taken by the Data Subject;
- the processing is necessary for the management of legal claims;
- the processing is carried out by a health organization, subject to a duty of confidentiality, and is only undertaken for specific purposes;
the processing is carried out by the National Institute of Statistics and Economic Studies (“INSEE”) or the Ministry’s services, subject to specific requirements;

the processing is carried out in the context of medical research;

the Personal Data has been subject to an anonymization process which has been approved by the CNIL, and the processing is carried out under specific conditions; or

the processing is carried out in the “public interest” and has been authorized by the CNIL.

Certain Personal Data is subject to specific restrictions or prohibitions:

the processing/use of social security numbers is restricted to the payment by employers of applicable fees to social security, health and retirement organizations;

Personal Data relating to criminal records can be collected or processed, but only by judicial authorities in the exercise of their functions; and

the processing of Personal Data relating to health is subject to specific requirements if carried out in the field of research.

f. Employee Personal Data

LIL does not provide for specific rules with respect to employees’ Personal Data. However, the CNIL has published several recommendations and opinions which apply specifically in the employment context and in particular, in respect of the following matters:

data collection in the recruitment process;

monitoring of employees’ activity;

video surveillance;

badges;

use of the National Security Number;

PABX;

ethics lines;

global positioning determination ("geolocalization"); and

discrimination.

In addition, the CNIL participates in and usually follows the opinions of the Article 29 Working Party (see in particular Section 5(d) below).
5. Consent

a. General
Pursuant to LIL, consent of the Data Subject is one of the requirements for processing Personal Data.

When consent is used as a justification for processing, consent must be informed, specific and unambiguous. The consent must be drafted in French. However, consent is not necessary if the purpose is legitimate, provided that the Data Subject has been informed of the data collection and processing as soon as such operations are made.

b. Sensitive Data
Sensitive Personal Data cannot be processed without the specific and express consent of the Data Subject (see Section 4(e) above for exceptions). Express consent is satisfied by either written consent or by a double-click process, if consent is given over the Internet.

c. Minors
The consent of a parent or guardian is required for individuals under the age of 18 (otherwise, collection would be considered unfair). Further, no information on family or way of life should be collected from a minor as this would be considered excessive vis-à-vis the purpose of collection.

d. Employee Consent
The French Authority does not recognize employee consent in light of the Article 29 Working Party’s opinion on the processing of Personal Data in the employment context, which states that it is misleading for an employer to try to rely on an employee’s consent as it is unlikely to be freely given.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in France provided that it is properly structured and evidenced.

It is advisable that:

- users are clearly informed in French of the required information without having to use links; and

- users should not be able to access website content without having read and accepted a website privacy policy.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the
Personal Data; the consequences of not providing consent; the rights of the Data Subject; how long the Personal Data is to be retained (or if not possible, the criteria used to determine such retention period); where the Personal Data is to be transferred; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and anonymize the Personal Data whenever possible.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; decide and control the uses which are made of Data Subject’s Personal Data, access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data. In addition, the Law no. 2016-1321 of 7 October 2016 for a Digital Republic (“French Digital Law”) has introduced the right to be forgotten for minors and the right for Data Subjects to give instruction in relation to the processing of their data after their death.

9. Registration/Notification Requirements

Organizations that collect and process Personal Data are required to file with the local data authority (via normal or simplified notification or authorization depending on the purpose and conditions of data processing).

10. Data Protection Officers

There is no requirement for organizations to designate a data protection officer or other individual who will be accountable for the privacy practices of the organization. Nonetheless, the appointment of a data protection officer exempts the Data Controller from filing requirements (except in case of international data transfer).

11. International Data Transfers

Transfers of Personal Data from France are permitted to:

- another country within the EU or the EEA;
- Canada (under certain circumstances);
Switzerland;
• Argentina;
• Guernsey;
• the Isle of Man;
• Jersey;
• Faeroe Islands;
• Andorra;
• Israel;
• Uruguay;
• New Zealand; and
• recipients established in the US to the extent that they have chosen to sign up to the Privacy Shield Certification are generally permitted without the need for formal approval.

Transfers to other countries, or to recipients in the US who have not chosen to sign up to the Privacy Shield Certification, are prohibited unless:

• the data exporter and the data importer enter into a data transfer agreement providing for adequate protection of the data transferred; or

• the Data Subject is not an employee (and the transfer does not relate to employee data), and has previously given his or her unambiguous, informed and express consent.

When the transfer is authorized through the execution of a data transfer agreement based on unmodified EC model clauses, since 2010, the CNIL does not require the submission of the agreement for validation.

The CNIL recommends the use of data transfer agreements based on unmodified versions of the model contractual clauses approved by the European Commission (either 2001 model or 2004 model) for transfers from a Data Controller to a Data Controller or from a Data Controller to a Data Processor (new model 2010).

BCRs may also be accepted, and the CNIL encourages large multinational companies to implement BCRs to secure transfers of data outside the EU as an alternative to the execution of data transfer agreements. In 2008, the Article 29 Working Party issued three guidelines in order to help Data Controllers draft their own BCRs. BCR clubs have been formed to inform the companies in specific sectors on how to implement BCRs, and the CNIL offers assistance with their implementation. To facilitate the process, there is a
mutual recognition system whereby the Data Controller chooses a leading data privacy authority ("DPA") in Europe that will notify all other concerned DPAs of the BCR project and obtain automatic validation of the project.

The CNIL has made available on its website a report on the protection and transfer of Personal Data in the context of outsourcing projects. CNIL offers pragmatic solutions to assist companies with the transfers of Personal Data made outside the EU.

12. Security Requirements
Organizations are required to take steps to: ensure that Personal Data in their possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with sector specific requirements. Organizations may be held liable together with third-party providers in case of breach by the latter.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions (including class actions which have been introduced by the Law n° 2016-1547 dated 18 November 2016 for the Modernisation of the 21st Century Justice), criminal proceedings, and/or private rights of action. The French Digital Law (law n°2016-1321 dated 7 October 2016) has increased the sanction powers of the CNIL. The CNIL is now able to impose a maximum fine of EUR 3 million (instead of EUR 300,000 in the event of repeated failures before).

In addition, these new legal provisions introduced by the French Digital Law make a formal notice issued by the President of the CNIL a precondition for the issuing of another sanction by the sanction Committee, with one notable exception. Indeed, the CNIL can now fine a company without any prior formal notice if the violation "cannot be brought into conformity in the context of a formal notice". The first and only sanction issued by the CNIL so far in application of this new provision was a fine of EUR 40,000 against a car rental company for a data security breach on its web site.
15. Data Security Breach

On 24 August 2011, the French Government adopted an Ordinance (articles 38 and 39 of Ordinance n°2011-1012) which implemented a new security breach notification procedure under the French Data Protection Act.

At this time, only providers of public electronic communications services were covered, i.e., telecommunications providers (e.g., mobile or land communications providers), Internet access providers and voice over IP service providers (“Provider”).

A data security breach is defined broadly as “any security breach that results accidentally or in an illicit manner in the destruction, loss, alteration, disclosure or unauthorized access to Personal Data which are processed in the context of the supply to the public of electronic communications services”.

The Provider must immediately report the data breach to the CNIL (see Part A.2.a above relating to the new mandatory breach notification tele-procedure introduced by the CNIL in August 2013). If the data breach may affect the privacy or the Personal Data of individuals, the Provider must also inform the affected individuals. The Provider should also maintain an inventory of security breaches including the facts surrounding the breach, its effects and the remedial action taken. This inventory should be at the disposal of the CNIL.

There is an exemption to the notification of individuals affected by the breach if the CNIL acknowledges that appropriate protective measures have been implemented to “scramble” the data so that unauthorized persons having accessed the data may not – in fact – read the data. If the Provider does not demonstrate that such measures have been implemented, the CNIL, having considered the likely adverse effects of the breach, may require the Provider to notify the relevant individuals.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.

16. Accountability

Organizations are required to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline

The Data Controller must obtain the CNIL’s authorization prior to implementing a whistle-blower hotline.
To simplify formalities, companies may use a fast-track procedure known as Single Authorization AU-004, provided that the system complies with the requirements of the CNIL’s decision “AU-004”. AU-004 describes the permitted processing activities relating to whistleblowing, the categories of Personal Data which can be collected, to what extent they can be shared or disclosed, the confidentiality measures which have to be taken, the data retention periods and the information to provide to Data Subjects.

By a decision of June 2017, the CNIL has modified its decision AU-004 with a view to adapting it to recent changes introduced by the so-called “Sapin 2” law (the law relating to “transparency, the fight against corruption and modernization of business life”). While the scope of application of the AU-004 tended to cover very restrictive areas (financial, accounting, banking, anti-competitive practices, combating discrimination and harassment in the workplace, health, occupational health and safety, environmental protection), it now covers all reports concerning:

- a crime or misdemeanor;
- a serious and manifest violation of an international commitment duly ratified or approved by France;
- a serious and manifest violation of a unilateral act of an international organization taken on the basis of an international commitment duly ratified or approved by France;
- a serious and manifest violation of the law or regulation;
- a serious threat or prejudice to the general interest of which the whistle-blower has personally been aware;
- the obligations defined by European regulations and by the French Monetary and Financial Code or by the General Regulation of the Autorité des Marchés Financiers, which is supervised by the Autorité des Marchés Financiers or the Autorité de contrôle prudentiel et de résolution (Reports from employees);
- the existence of conduct or situations contrary to the company’s code of conduct concerning acts of corruption or trading in influence (reports from employees).

However, the facts covered by the secrecy of national defense, medical secrecy and the secrecy of relations between a lawyer and his client are excluded from the scope of this standard.

18. E-Discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is
involved. The organization will be required to advise employees of the implementation of such system, the monitoring of work tools and the storage of information.

In addition, when contemplating an e-discovery procedure that implies data transfer to the US, the company will have to take into account the French “blocking statute”. The blocking statute (Law n°68-678 of 26 July 1968) was amended by Law n°80-538 dated July 1980. It is designed to protect French companies and France’s economic interests. It states that subject to international convention, it is forbidden for any person, to request, search or communicate in writing, orally, or any other form, documents or information of an economic, commercial, industrial, financial, or technical nature for the purpose of constituting evidence for, or in the context of, foreign judicial or administrative proceedings. Failure to comply with this provision carries a maximum sanction of six months’ imprisonment and/or EUR 18,000 fine.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to: inform employees of monitoring policies being implemented in the workplace; give employees the opportunity to opt out of the spam-filtering solution on the basis of legitimate interest; and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies
The use of cookies must comply with data privacy laws. As such, consent of Data Subjects may have to be obtained before cookies can be used and deployed. Some types of cookies that track or monitor the user may not be permitted.

CNIL revised its guidance on the use of cookies in a Deliberation published on 5 December 2013. The Deliberation also includes practical recommendations on how to comply with the new guidance in practice.

CNIL now recognizes that consent to the use of cookies may result from an Internet user merely continuing to browse on the website to the extent that he/she has been expressly informed of the use of cookies, their purpose and the possibility of opposing such use (e.g., through the implementation of a banner on the landing page). This new position is to be welcomed insofar as CNIL had previously adopted a less than pragmatic approach requiring website editors to obtain Internet users’ express prior consent, with a box to be ticked or a click to accept, before cookies could be installed.

The scope of the new guidance is very broad and includes, inter alia, advertising cookies, tracking cookies used in social networks and cookies installed and read when viewing a website, reading an email or downloading an application or software.
The only cookies exempted are technical cookies the only purpose of which is to permit or facilitate electronic communication, cookies that are strictly necessary for providing a service expressly requested by a user and audience cookies that verify certain criteria provided by the Deliberation (most cookies on the market today do not meet these criteria).

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent.
Germany

Holger Lutz
Frankfurt
Tel: +49 69 29908 508
holger.lutz@bakermckenzie.com

Matthias Scheck
Munich
Tel: +49 89 55238 200
florian.tannen@bakermckenzie.com

Michael Schmidl
Frankfurt
Tel: +49 89 55238 211
michael.schmidl@bakermckenzie.com

Matthias Scholz
Munich
Tel: +49 89 55238 242
matthias.scholz@bakermckenzie.com

Michaela Weigl
Frankfurt
Tel: +49 69 29908 508
michaela.weigl@bakermckenzie.com

Julia Kaufmann
Munich
Tel: +49 89 55238 242
julia.kaufmann@bakermckenzie.com

Simone Bach
Frankfurt
Tel: +49 69 29908 508
simone.bach@bakermckenzie.com
1. Recent Privacy Developments


As elaborated in the EU GDPR Chapter, the General Data Protection Regulation (“GDPR”) will start to apply on 25 May 2018 across all EU Member States. However, the GDPR does not automatically replace and repeal the current FDPA in Germany. Rather, the German legislator had to determine how to reform the FDPA in light of the GDPR, in particular which provisions must be repealed, which provisions can be retained and which provisions must be amended. This is because although the GDPR was intended to harmonize the EU data protection laws, the GDPR contains around 50 opening clauses that allow or even require the national legislator to enact provisions around data privacy which would apply in addition to the provision of the GDPR, but only on a local Member State level. For example, Art. 88 of the GDPR allows the Member States to enact laws with more specific rules on the processing of employee data. Also, according to Art. 37 (4) of the GDPR, the Member States may enact laws with further requirements to appoint a Data Protection Officer, in addition to the requirements set out in Art. 37 (1) of the GDPR.

For this purpose, on 30 June 2017 Germany has adopted the Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (‘the Act’). The Act will enter into effect together with the GDPR on 25 May 2018.

The most important changes for companies provided by the Act are laid out in Article 1 of the Act (which will enter into effect as the “new FDPA”) and comprise:

- **Appointment of a data protection officer:** Under the new FDPA, the obligation to appoint a data protection officer goes beyond the requirements of the GDPR. The German legislator (with slight amendments) re-enacted the previous provision under the current FDPA. Accordingly, all organizations are required to appoint a data protection officer if they employ more than nine persons with automated processing of Personal Data.

- **Processing of Special Categories of Personal Data:** Subject to certain exceptions, processing of Special Categories of Personal Data is generally prohibited under the GDPR. In addition to the exceptions for legitimate processing under Article 9 of the GDPR, the German legislator created some further exceptions, including, e.g., in the field of employment and social security law, for public health purposes, or for scientific and statistic research purposes.
Global Privacy and Information Management Handbook
Germany

• Rights of the Data Subjects: Under the new FDPA the rights granted to Data Subjects under the GDPR are somewhat restricted, e.g., limitations apply to the obligation to inform Data Subjects in the event of data processing for a purpose different from the purpose of collection, or where Personal Data has not been obtained from the Data Subject directly.

• Employee Data protection: The provision of the new FDPA governing the processing of Personal Data in the employment context is widely identical to the respective provision of the current FDPA. However, the Act specifically clarifies the conditions under which an employee’s consent can form the legal basis for data processing and it sets out requirements concerning the processing of Special Categories of Personal Data. Furthermore, the Act clarifies that, under certain circumstances, the processing of Personal Data in the employment relationship can also be permissible based on collective agreements. As is the case under the current FDPA, the same requirements apply also in cases where employee data, including Special Categories of Personal Data, are processed without being stored or meant to be stored in a filing system.

Some opinions have criticized the Act as being not fully compliant with the GDPR. Hence, it remains to be seen whether the German legislator will (have to) readjust the provisions in the future.

Guidance from Data Protection Authorities on interpretation of the GDPR

The Data Protection Conference (DPC) – a voluntary association of independent federal and state data protection authorities in Germany – has published several jointly agreed interpretation guidelines on the GDPR. In these short papers the DPC provide guidance on several key issues of the GDPR, such as the record of processing operations, supervisory powers and sanctions, processing for marketing purposes, data transfers to third countries, data protection impact assessments, etc. Additional guidance papers are available from the Bavarian Data Protection Authority. However, all guidance is subject to future – possibly deviating – interpretation on EU level.

Guidance from Data Protection Authorities on obtaining consent

In March 2016, the Duesseldorfer Kreis, an association comprising the 16 Data Protection Authorities ("DPA") in Germany, issued guidance on obtaining consent from Data Subjects. The guidance provides helpful instructions and recommendations for drafting consent forms when obtaining consent in written or electronic form (see also Section 5 below).

A valid consent requires clear and unambiguous wording, so that Data Subjects understand that they are consenting to certain data processing activities. For example, the words “I acknowledge that…” do not suffice.
Rather, wording such as “I consent to…” or “I agree that…” is required. The consent wording must inform Data Subjects in a transparent and easy-to-understand manner about the relevant data processing activities. Generally, opt-in is required; pre-ticked boxes or other opt-outs are not sufficient. The consent wording – if embedded in a broader contractual declaration – should generally be placed directly above the signature line. The signature will then relate to the main contractual declaration as well as the consent. Only in certain cases, e.g., where health data is collected, might a valid consent require a separate signature. The consent wording must be clearly recognizable as such. It must not be mixed with general information on data processing without being separated out and prominently featured (e.g., by bold or different colored text). The consent wording should inform the Data Subject that he/she is entitled to withdraw his/her consent. Non-compliance with these requirements may result in consent being invalid.

In some respects, the guidance appears to be slightly stricter than German case law on point (e.g., in that the guidance requires opt-in whereas two decisions of Germany’s Federal Court of Justice (form 2008 and 2009) suggest that an opt-out consent may be sufficient). But in an informal discussion with one of the German DPAs, the respective official stated that in exceptional cases (e.g., in case of the two decisions of the Federal Court of Justice), an opt-out solution may still be sufficient and that the guidance is not intended to contradict the decisions of the Federal Court of Justice.

**Guidance from Data Protection Authorities on monitoring of employee email and internet use**

In February 2016, German DPAs issued guidance for private sector organizations explaining when and how employers may monitor their employees’ work email accounts and internet usage. The applicable legal framework depends on whether employers permit or prohibit their employees to use workplace email and internet services for personal use (private use).

If employers prohibit private use, the only relevant law is the German Federal Data Protection Act (“FDPA”) and there will be more scope for monitoring of:

- **Internet usage:** Employers may undertake spot checks of protocol data in order to check whether employees use the Internet for company purposes only. This should – as a first step – be done without collecting Personal Data (such as IP addresses or other data which allow the identification of individuals). For example, compiling blacklists and/or whitelists on the basis of anonymized protocol data would be preferable.

- **Emails:** Employers may take note of incoming and outgoing company emails and may, for example, ask employees to forward certain emails (but not for an auto-forwarding of all emails unless an employee is absent and an out-of-office reply is insufficient). When employers recognize the
personal character of emails, employers must stop reading the respective emails and must also not forward or print them. A full monitoring of internet use and/or emails is only permitted to investigate crimes and requires a concrete suspicion of misuse as well as adherence to the principle of proportionality.

If employers permit or tolerate private use, the FDPA applies but – according to the German DPAs and the predominant opinion in case law and of legal scholars – the German Telecommunications Act (“TCA”) and the Telemedia Act (“TMA”) also apply. These impose further restrictions on monitoring activities:

- As a general rule, data which is subject to the telecommunications secrecy provisions of the TCA (e.g., protocol data) may only be accessed with the employee’s consent, unless one of the very narrow statutory exceptions applies.

- Monitoring of internet usage: If employers want to monitor their employees’ internet use, they should conclude a works council agreement which outlines the permitted personal use of the company’s IT systems (or they should include similar provisions in individual employment contracts and/or a policy document). In addition, employers must obtain the employees’ individual consent which must include the type and scope of the monitoring to any planned monitoring. The employers may then undertake spot checks of protocol data to check that employees adhere to the rules for personal internet use. Despite the consent, an evaluation of protocol data by reference to individuals is only permitted if there is a concrete suspicion (e.g., of a violation of the rules for personal Internet use).

- Monitoring of emails: The same applies to the monitoring of an employee’s email account. In addition, it should be stipulated (in a works council agreement/employment contract/policy) if and how the employer may access work emails stored in an employee’s email account that contains both company emails and personal emails.

- Refusing to consent: Employees must be able to refuse their consent to the monitoring of their internet and email usage without facing any employment-related disadvantages. However, if they refuse their consent, they will not be allowed to use the work internet or email account for personal purposes.

Additionally, the guidance contains standard works council agreements and consent forms which may be consulted when drafting these documents or a monitoring policy. German employers would be wise to structure their monitoring activities to comply with the guidance issued.
Consumer protection associations can bring cease and desist actions for data protection law infringements

In February 2016, the new “Law for the Improvement of Civil Enforcement of Consumer Protection Rules under Data Protection Law” (which amends the German Act on Injunctive Relief) came into effect. It gives consumer protection and competition associations in Germany their own right to pursue data protection violations. Now such consumer protection associations which are registered with the German Ministry of Justice or the EU Commission or, under certain circumstances, associations for the promotion of commercial or independent professional interests, or the Chambers of Industry and Commerce are entitled to bring cease and desist actions against companies.

However, the new law’s applicability is limited as not all data protection violations – only violations of “consumer protective data protection law” – may be pursued by way of associations suits. Consumer protective data protection law includes, among others, provisions that govern the collection, processing and use of Personal Data for the purpose of (i) advertising, (ii) market or opinion research, (iii) credit scoring, (iv) profiling, address and other data trading and (v) similar commercial purposes.

Eligible associations are now entitled to seek interim injunctions both in order to enjoin and to suspend data protection law infringements. The DPAs have a right to be heard in the legal proceeding against the infringing companies. Eligible associations will be able to bring such actions to actively force companies to comply with German data protection laws aiming at the protection of consumers. In light of the recent “Google Spain” and “WeltImmo” decisions of the European Court of Justice the amendment of the German Act on Injunctive Relief may affect companies located outside of Germany as well those that have an establishment or representative in Germany and are processing data of Data Subjects in Germany (for the Law Applicable, see Section 3 below). The General Data Protection Regulation (“GDPR”) will expand the application of the European data protection law even more and will likely further increase the impact of this new right to bring such cease and desist action by eligible associations.

2. Emerging Privacy Issues and Trends

Enforcement actions

- In 2016, the DPA in Hamburg has issued fines against three companies for failing to implement alternative data transfer mechanisms following the invalidation of the European Commission Safe Harbor adequacy decision in October 2015.

Since the invalidation of the Safe Harbor adequacy decision, the DPA has investigated the data transfer methods of about 35 internationally active companies that used to rely on Safe Harbor for transferring Personal
Data to the US. According to the DPA, the inspections have shown that the vast majority of companies had already put in place alternative transfer mechanisms, namely Standard Contractual Clauses (see also Section 11 below). However, a number of companies were found to be in violation of the requirement, and were subsequently fined. Apparently, the DPA imposed rather low fines in these instances (fines range from EUR 8,000 to EUR 11,000 for each company) because the companies in question promptly implemented Standard Contractual Clauses after having been informed they were in breach. However, the DPA has stated that “for future infringements, stricter measures have to be applied”.

Despite the fact that the Irish DPA has initiated court proceedings to clarify the validity of Standard Contractual Clauses before the Court of Justice of the European Union (“ECJ”), the German DPA highlighted that Standard Contractual Clauses are still a valid transfer mechanism for the time being. However, this might change in the near future as on 3 October 2017 the Irish DPA obtained a decision of the Irish High Court that the validity of the Standard Contractual Clauses will be submitted to the Court of Justice of the European Union for a preliminary ruling.

- In the summer of 2015, the Bavarian DPA issued five-figure Euro fines against both the seller and the purchaser for an unlawful transfer of customer data in the course of a sale of business. In connection with an asset deal, the seller of an online shop had transferred all of its assets, including customer data, to the purchaser. It did not notify the affected customers of the transfer, let alone obtain their consent. Following the transfer, the purchaser used the transferred customer email addresses for direct email marketing.

  Importantly, the purchaser was also ordered by the DPA to delete the unlawfully transferred customer data, meaning it paid money for a crucial asset it could not use after all. Generally, as the acting Bavarian DPA pointed out, such a transfer of Personal Data requires the Data Subject’s consent or, at least, the prior notification of the Data Subject coupled with an opportunity to opt out of the transfer, which opt-out was not exercised. Unlike commonly assumed, the asset deal itself did not legitimize the data transfer.

- Also in the summer of 2015, the Bavarian DPA imposed a significant five-figure Euro fine against a company engaging as a principal in commissioned data processing. The company had failed to define concrete technical and organizational data security measures in its respective data processing agreement, instead making only general statements and repeating the legal text (see also Section 13 below).

  In case companies engage external service providers, they must have written data processing agreements in place. In addition to such written
form, the law requires certain minimum content to be included in the agreement. Especially of importance are the so-called technical and organizational measures, i.e., the data processing agreement must in particular describe the data protection measures in detail. However, in practice many contracts on commissioned data processing only repeat the purposes of data security provided by law or are limited to a few general remarks.

The DPA has now stated that technical and organizational measures cannot be defined by using only general terms, but measures must be tailored to the individual case. In particular, the specifics of the contractual provisions must take into account the data security concept of the respective external service provider and the particular data processing systems and define these measures in concrete and specific terms.

**Recent case law**

- In July 2017, the Federal Labour Court in Germany (decision 2 AZR 681/16) was concerned with the question whether or not an employer’s extraordinary termination of the employment contract was valid due to the fact that the employee had excessively used the corporate internet access and IT systems for private purposes. The problem was that the employer had obtained proof of such use by installing a key logger on the computer used by the employee that logged all of the employee’s keyboard entries and regularly took screen shots. The court held that the proof could not be admitted to justify the extraordinary termination because the use of the key logger violated the employee’s right of informational self-determination and there was no legal basis to justify the monitoring. In particular, the monitoring did not take place in order to investigate a committed crime of the employee in accordance with Section 32 FDPA and the groundless surveillance was disproportionate.

  Since Section 32 FDPA will substantially continue to apply under the new legal regime (i.e., Article 88 GDPR in connection with Section 26 of the new FDPA, c.f. Section 1 – Recent Privacy Developments), the importance of this decision will remain also for future monitoring activities by employers is violation of applicable Data protection law.

- In June 2016, the Higher Administrative Court of Hamburg had to judge on the legality of an order granted by the Hamburg DPA against a Social Media Provider located in Ireland to allow its users to use pseudonyms on its profiles. While the DPA takes the view that the Social Media Provider’s “real name” policy violates the right to privacy, the court has taken the position that at this time it is not clear whether the DPA’s order was granted on a legal basis. This would depend on the interpretation of the EU Data Protection Directive 95/46/EC. Under current case law of the
ECJ it has not been clarified whether the EU Data Protection Directive would permit a German DPA to proceed with an order pursuant to national laws and regulations against the Data Controller located in Ireland. Uncertainty remains, as the division of powers between the national data protection supervisory authorities and the power of intervention of the German DPAs in cases where a parent company holds multiple offices within the European Union which have different tasks, needs to be clarified on an EU level. The court therefore has not granted an order, as the question of such legal powers of DPAs within the European Union is already pending in another case in which the German Federal Administrative Court has submitted a respective question to the ECJ.

3. Law Applicable

The current Data protection landscape in Germany will be substituted by the GDPR and national legislation (i.e., the “new FDPA”) supplementing the GDPR with regard to the numerous opening clauses contained in the GDPR. The new FDPA will enter into effect together with the GDPR on 25 May 2018. Until then the (current) FDPA outlines the general requirements and obligations relating to the collection, processing and use of Personal Data by private bodies and by federal authorities and bodies. For state authorities and bodies, each German state (Bundesland) has its own state data protection act. If there are specific data privacy provisions, in particular sector-specific laws, the FDPA is generally superseded by such specific provisions and applies only in cases where there are gaps in the law, e.g., the German TMA, the Social Act No. 10 for pharmaceutical companies, or the Postal Act for postal services.

With respect to private bodies, the FDPA applies if the private body collects, processes or uses information relating to an individual in data processing systems or in or from non-automated filing systems, unless the information is collected, processed or used solely for personal or domestic activities. From a territorial perspective, the FDPA applies to private bodies located in Germany. The FDPA is not applicable in so far as a private body is located in another Member State of the EU/EEA, except where the relevant data collection, processing and use is carried out by an establishment in Germany. In this context, a recent decision of the ECJ must be considered which further defines the term “establishment” and expands it to a representative. The FDPA applies to data collected, processed or used in Germany by a private entity located outside the EU/EEA using, for the purposes of processing Personal Data, equipment, automated or otherwise, situated in Germany. In another decision of the ECJ against a global internet search engine provider located in the US, the ECJ held that EU Member State data protection law applies if a legal entity located in the US processes Personal Data of EU citizens and if a subsidiary of this US legal entity that is located in the EU is
involved in the business operations of the US legal entity by providing marketing support, even though this subsidiary was not involved in the actual data processing activities. In the aftermath of these decisions, there is a risk that German DPAs and German courts apply the FDPA even broader, even if the black-letter law requirements for its application are not fulfilled. Furthermore, the GDPR expressly states that it applies to the Processing of Personal Data in the context of the activities of an establishment of a Controller or a Processor in the European Union, regardless of whether the processing takes place in the European Union or not.

4. Key Privacy Concepts

a. Personal Data
The FDPA (as will the GDPR) applies to the “collection”, “processing” and/or “use” of “Personal Data”, i.e., any information relating to personal or material circumstances of an identified or identifiable individual (“Data Subject”).

b. Data Processing
“Collection” means the acquisition of Personal Data about the Data Subject.

“Processing” is extremely widely defined and covers the recording, alteration, transfer, blocking, and erasure of Personal Data.

“Use” describes any utilization of Personal Data other than Processing.

The GDPR applies to the same Data processing activities without distinguishing in terminology; any operation performed on Personal Data will be considered a “processing” of Personal Data.

c. Processing by Data Controllers
The FDPA applies to any person or body which collects, processes or uses Personal Data on his, her or its own behalf, or which commissions others to do the same (“Data Controller”). The GDPR, in addition, imposes certain obligations also on the Data Processor.

d. Jurisdiction/Territoriality
As further described in Section 3 above, the FDPA applies to:

- Data Controllers established in Germany that collect, process and/or use Personal Data in Germany;
- Data Controllers established outside Germany but within an EEA Member State that collect, process and/or use Personal Data in Germany through the Data Controller's German branch/establishment; and
- Data Controllers established outside the EEA that collect, process and/or use Personal Data by using equipment located within Germany for such purposes (other than merely for the purpose of transit).
Data Controllers established outside the EEA that collect, process and/or use Personal Data within Germany generally have to appoint a representative in Germany.

The GDPR will also apply to the processing of Personal Data of Data Subjects who are in the European Union by a Controller or Processor not established in the European Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the European Union; or (b) the monitoring of their behavior as far as their behavior takes place within the European Union.

e. **Sensitive Personal Data**

The FDPA imposes additional requirements for the collection, processing and/or use of special categories of Personal Data ("Sensitive Personal Data") – that is, Personal Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health or sexual life. Specifically, the collection, processing and/or use of Sensitive Personal Data is prohibited unless certain conditions are met, including:

- the Data Controller obtains the explicit consent of the Data Subject (see Section 5(b) below);
- the collection, processing and/or use is necessary to protect the vital interests of the Data Subject or of a third party where the Data Subject is physically or legally incapable of giving consent;
- the data has evidently been made public by the Data Subject;
- the collection, processing and/or use is necessary in order to assert, exercise, or defend legal claims, and there is no reason to assume that the Data Subject has an overriding legitimate interest in excluding the collection, processing and/or use;
- the collection, processing and/or use is necessary for the purposes of scientific research, and the scientific interest in carrying out the research project substantially outweighs the Data Subject’s interest in excluding such collection, processing and/or use, and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort;
- the collection is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services and the processing is undertaken by a health professional or person with the equivalent duty of confidentiality as a health professional; or
the collection, processing and/or use is necessary for the activities of non-profit-seeking trade unions or organizations of a political, philosophical, or religious nature and where the data concerned only belongs to the organizations’ members or persons who maintain regular contact with the organizations in connection with the purposes of their activities.

The GDPR similarly forbids the processing of Special Categories of Personal Data generally and only allows it under some limited exceptions.

**f. Employee Personal Data**

Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information, religious denomination) and Personal Data.

An employee’s Sensitive Personal Data may generally only be processed with the employee’s explicit consent (as the other conditions that allow for the processing of such data mentioned in Section 4(e) above will usually be irrelevant in a standard employment relationship). Exceptions apply if the collection, processing or use of such data is allowed or required by law. For example, information regarding religious denomination must be processed for church tax deduction (pursuant to relevant tax provisions).

An employee’s Personal Data may be processed by a Data Controller in certain circumstances, including if (i) the processing activities are necessary for the performance of the employment contract (i.e., if they are required for the fulfillment of primary or collateral contractual or pre-contractual duties), or – arguably – (ii) they are necessary to safeguard justified interests of the Data Controller and there is no reason to assume that the employee has an overriding legitimate interest in his/her Personal Data being excluded from processing or use.

A fallback justification for processing both Sensitive Personal Data and Personal Data in the employment context is the provision of consent by the Data Subject. However, it is debatable whether an employee can validly give his or her consent in an employment relationship (see Section 5(d) below).

The new FDPA (on the basis of the opening clause in Article 88 GDPR) specifies the conditions under which employees may validly consent in the processing of their Personal Data by their employers and defines the conditions under which Special Categories of Personal employee Data may be processed.

5. Consent

a. General

Both, under the current FDPA and the GDPR, consent of the Data Subject is generally not mandatory for the collection, processing and disclosure of
Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances (see also Section 1).

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the previously identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

Although neither the GDPR, nor the FDPA contain any express language requirement, the concept of informed consent generally requires the information as well as the consent language itself to be in the German language in order to enable the German Data Subject to understand without doubt to which he/she consents. Where Data Subjects are sufficiently proficient in English (or in any other language) consent may also be sought in English (or the other relevant language).

If consent is to be given in writing simultaneously with other declarations, special prominence must be given to the declaration of consent. Further guidance was provided by the German DPAs, as elaborated in Section 1 above.

b. Sensitive Data

German law and the GDPR recognize Sensitive Data as a special category of Personal Data and, as such, is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed with the express consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances (see Section 4(e) above).

c. Minors

It is debatable whether the ability to consent depends on the ability to understand, i.e., the capacity to understand the consequences of giving consent (prevailing opinion of the German DPAs) or legal capacity. According to the DPAs, depending on the manner, extent, and purposes of the data processing concerned, an ability to understand can be assumed for minors of around 16 years old. Thus, following the DPAs’ opinion, for minors under the age of 16, consent should be obtained from a parent or legal guardian. According to a recent decision of the German Federal Supreme Court, the consent of minors regarding the collection of Personal Data for marketing purposes in connection with a sweepstake is invalid. The Federal Court of Justice recently ruled that a public health insurance company illegally exploits
the inexperience of minors if it collects a significant amount of Personal Data for marketing purposes in connection with a sweepstake. According to the Federal Court of Justice, minors are less capable of foreseeing the consequences and disadvantages of their consent to the collection of their Personal Data.

The GDPR clarifies that in relation to the offer of information society services directly to a child on the basis of the child’s consent, the processing of the Personal Data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

d. Employee Consent

German DPAs have raised doubts as to whether consent given in the context of an employment relationship can be considered valid. First, the DPAs question whether the consent would qualify as voluntary given that the employee may feel forced to consent due to the subordinate nature of his/her relationship with his/her employer. Second, some DPAs argue that consent would be misleading where statutory permission to collect, process, and use Personal Data is available. However, a recent decision by the Federal Labor Court provides arguments that employee consent might be valid as long as (i) the consent is in writing, (ii) the consent is based on sufficient information, and (iii) there is no indication for pressure or coercion.

Under the regime of the GDPR and the new FDPA it is clarified that employee consent is a possible legal basis provided that the consent is actually freely given, which may in particular be the case if the employee receives a benefit or employer and employee pursue the same interest.

e. Online/Electronic Consent

In Germany, electronic consent is permissible and can be effective if properly structured and evidenced. A simple digital signature and/or a simple mouse-click will generally suffice in the context of advertising, “telemedia services” or if telecommunication services are at issue. Consent given by way of a simple mouse-click is sufficient only if the following conditions are met:

- the Data Subject is given the necessary information relating to the consent (e.g., on the scope of use of the relevant Personal Data);
- there is an unambiguous and deliberate act by the Data Subject expressing consent to the collection, processing or use;
- the consent is logged;
- the text of the consent is accessible at any time by the Data Subject; and
the Data Subject is enabled to revoke his or her consent for the future at any time.

German DPAs have issued opinions in individual cases where the DPAs have allowed the use of electronic consent outside of the above mentioned areas of law. This more liberal view is in line with the requirements of the FDPA, which only requires written consent unless the circumstances of the individual case warrant a different form (e.g., in an online context where there is a large number of users, obtaining written consent would be regarded as too burdensome).

The GDPR does not require a certain form for providing consent. Consent can be given in any form provided that the Controller is able to demonstrate that the Data Subject has consented to the processing of his or her Personal Data. According to the recitals of the GDPR, this could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the Data Subject’s acceptance of the proposed processing of his or her Personal Data. On the other hand, silence, pre-ticked boxes or inactivity should not constitute consent.

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes of collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; and where the Personal Data is to be transferred.

Under the GDPR notice requirements are even expanded and include, e.g., information about the legal basis for the processing and, where applicable, the legitimate interests pursued by the Controller or by a third party.

7. Processing Rules

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; Personal Data should be anonymized or pseudonymized whenever possible; Data Subjects should be provided with the option to use a pseudonym or remain anonymous whenever possible; Personal Data should be deleted/anonymized once the stated purposes have been fulfilled and legal obligations have been met.

The processing rules remain basically unchanged under the GDPR.
8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and withdraw a consent previously given.

Under the GDPR, these Data Subjects’ rights will be retained and in some respects further strengthened. In addition, the GDPR will introduce additional rights, such as the right to be forgotten, or a right to data portability.

9. Registration/Notification Requirements

An organization that collects and processes Personal Data may be required to register with the competent DPA. When an organization appoints a data protection officer, it is no longer required to register with the DPA (except for certain very limited data processing activities). The majority of registration requirements with the DPA can therefore be avoided by appointing a data protection officer even if such an appointment is not legally required.

Under the GDPR, the general registration/notification requirements no longer apply. Instead, the GDPR introduces an obligation of the Controller to conduct a data protection impact assessment where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, and to consult the supervisory authority prior to the processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk.

10. Data Protection Officers

In Germany, an organization must appoint a data protection officer if (i) it employs more than nine persons with automated processing of Personal Data, (ii) 20 or more persons with any other types of Personal Data processing activities, or (iii) it is subject to the prior checking procedure which is particularly required if (a) sensitive data is processed or (b) the processing of Personal Data is intended to evaluate the Data Subject’s personality, including his/her abilities, performance or conduct, unless such data processing activities are covered by a statutory obligation or the Data Subject’s consent or are necessary to perform a contract with the Data Subject.

Under the GDPR, the Controller and the Processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b)
the core activities of the Controller or the Processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale; or (c) the core activities of the Controller or the Processor consist of processing on a large scale of special categories of data pursuant to Article 9 GDPR and Personal Data relating to criminal convictions and offenses referred to in Article 10 GDPR. In accordance with the opening clause in Article 37 (4) GDPR, in Germany, the obligation to appoint a data protection officer goes beyond the requirements of the GDPR and continues to apply, e.g., to all organizations employing more than nine persons with automated processing of Personal Data.

11. International Data Transfers

Transfers of Personal Data from Germany to other EEA countries are generally permitted without the need for further approval, provided such transfers would be legal within Germany. The same applies with respect to transfers to Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay, which are subject to European Commission findings of adequacy in relation to their data protection laws (subject to the fulfillment of certain pre-conditions).

Transfers to the US are permitted where the recipient has registered under the Privacy Shield arrangement, provided the transfers would be legal within Germany and provided that the recipient actually adheres to the Privacy Shield rules. Transfers to the US or any other countries outside the EEA that do not provide an adequate level of data protection are at the moment still legal if based on unmodified versions of the relevant EU Standard Contractual Clauses, always provided that the transfer would be legal within Germany. In the above-mentioned cases, no DPA notification or approval is required by law. However, the Irish High Court has recently decided to submit to the Court of Justice of the European Union the question of the validity of the Standard Contractual Clauses for a preliminary ruling. Whether or not the Standard Contractual Clauses will continue to serve as legal basis for international data transfers in the future depends on the outcome of this case.

Any data transfers based on modified versions of the relevant EU Model Clauses or, on a data transfer agreement entirely different from the relevant EU Model Clauses, must be submitted to the competent DPA for approval. Approval is also required for data transfers based on Binding Corporate Rules from the Federal DPA and the following German state DPAs: Berlin, Brandenburg, Lower-Saxony (Niedersachsen), North Rhine Westphalia (Nordrhein-Westfalen), Rhineland-Palatinate (Rheinland-Pfalz), Saarland, Saxony-Anhalt (Sachsen-Anhalt), Schleswig-Holstein, Thuringia (Thüringen). Other German states merely require a registration of Binding Corporation Rules.
Transfers of Personal Data to countries outside the EEA may further take place without additional measures to ensure an adequate level of data protection at the recipient’s end where:

- the Data Subject has validly consented to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or to take steps at the Data Subject’s request with a view to entering into a contract with the Data Subject;
- the transfer is necessary for the performance of a contract between the Data Controller and a third party in the interest of the Data Subject;
- the transfer is necessary due to important public interest grounds;
- the transfer is necessary for the establishment, exercise or defense of legal claims; or
- the Personal Data is available from a public register (if certain requirements are met).

However, such exceptions must be interpreted and applied restrictively.

The GDPR introduces additional legal bases, such as an approved code of conduct together with binding and enforceable commitments of the Controller or Processor in the third country, or an approved certification mechanism.

12. Security Requirements
Organizations are required to take steps to: ensure that Personal Data in its possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

Similar requirements apply under the GDPR, whereby the GDPR expressly obligates both, the Controller and the Processor, to implement appropriate technical and organisational measures.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Both, under the current FDPA and the GDPR, organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data, and to comply with sector specific requirements. In case of the occurrence of a data breach (see also 15 of this section), the outsourcing organization shall be held liable together with the third-party provider.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

In addition to the above, the GDPR significantly raised the amounts of possible fines which may now amount to up to EUR 20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year.

15. Data Security Breach

With effect as of 1 September 2009 a statutory security breach notification was introduced in Section 42a FDPA, which resembles a US-type “Security Breach Notification”. The same security breach notification was implemented in Section 15a TMA.

Pursuant to these rules, companies are now required to report any illegal transfer of or illegal access to the following types of data, or any knowledge thereof obtained by third parties, always provided that such access or transfer would lead to severe adverse effects on the rights or legitimate interests of the relevant Data Subject:

- Sensitive Personal Data;
- Personal Data which is subject to professional confidentiality obligations (e.g., confidentiality obligations applicable under statutory law to attorneys, doctors, etc.);
- Personal Data concerning criminal acts or administrative offenses or suspicion regarding the same; or
- Personal Data relating to bank accounts or credit card accounts.

In cases involving a large number of Data Subjects, other public-oriented measures (such as announcements in two nationwide newspapers) may replace the information of the concerned Data Subjects.

The notification obligation does not require that the security breach is committed intentionally or maliciously. It also does not matter if the Data Controller itself, one of its Data Processors (if any) or a third party causes the security breach. Scenarios for potential security breaches are thus manifold, for example: a hacker breaks into the company’s database; a fraudster gains access to the company’s data processing systems by phishing user passwords; laptops or storage media are lost or stolen; or an email with Personal Data is sent to the wrong recipient.

The security breach notification generally needs to be provided to the competent DPA and all affected Data Subjects. While the notification to the
A competent DPA has to be made even if the data breach is not eliminated or in cases of pending criminal prosecution, the notification to the Data Subjects may be withheld until appropriate measures to safeguard the data have been taken and the notification would no longer endanger criminal prosecution.

The notification of the Data Subject should contain a description of the nature of the unlawful disclosure as well as recommendations for measures to mitigate any possible negative effects. The notification to the competent DPA must, in addition, describe any detrimental consequences of the unlawful disclosure as well as the preventive measures to mitigate the negative consequences of the security breach.

If notifying all Data Subjects requires disproportionate efforts, the notification may be replaced by a notification to the general public, e.g., by means of half-page announcements in at least two nationwide newspapers or other measures having a similar effect.

The notification needs to be provided “without undue delay”. This does not necessarily mean that the notification must be provided immediately. Rather, the Data Controller is given some time to examine the facts and to seek legal advice.

A similar security breach notification obligation was implemented in Section 93 para. 3 in connection with Section 109a of the TCA with effect as of 3 May 2012. Therefore, all service providers within the meaning of the TCA must inform the Data Subject without undue delay of the violation of the protection of Personal Data if it can be assumed that the violation constitutes a serious harm to the rights or legitimate interests. The notification must include at the very least the following information:

- the type of violation of the protection of Personal Data;
- details of contacts points, where further information is available; and
- recommendations regarding measures that limit the adverse consequences of the violation of the protection of Personal Data.

Companies that render publicly available telephony services must, in addition to notifying the Data Subject, inform the Federal Network Agency and the Federal Commissioner for Data Protection and Freedom of Information without undue delay in case of a violation of the protection of Personal Data. Furthermore, those companies must comply with additional requirements.

An organization that is involved in a data breach situation may be subject to a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.
Further information can be found in our Global Data Breach Notification Handbook.

Under the GDPR, similar notification requirements apply in the case of a data breach, whereby the notification requirements are not limited to certain kinds of Personal Data. The Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data breach to the supervisory authority, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition, the Controller shall communicate the Personal Data breach to the Data Subject without undue delay when the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons.

16. Accountability
Organizations in Germany are required to: conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

The accountability principle is strengthened even more under the GDPR. The GDPR explicitly states that the Controller shall be responsible for, and be able to demonstrate compliance with the other principles relating to the processing of Personal Data (e.g., lawfulness, fairness and transparency), thereby introducing extensive new documentation obligations.

17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Germany, provided they are in compliance with local laws. In particular, the Data Protection Officer must be involved early on and, if a works council exists, the works council has a co-determination right. The subject matters that can be reported by the Whistle-blowing hotline must be restricted and anonymous reporting must not be encouraged.

The GDPR does not directly address the issue of whistle-blowing. The general requirements as to the legitimacy of processing Personal Data must be observed, in addition to any Labour law requirements.

18. E-Discovery
When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved. In addition, an organization is required to advise employees of the
implementation of an e-discovery system, the monitoring of work tools, and
the storage of information.

The GDPR allows the processing of Personal Data if the processing is
necessary for compliance with a legal obligation to which the Controller is
subject. However, whether this justification may be invoked depends on
whether such legal obligation exceptionally exists for German organizations
as the concept of e-discovery is generally alien to German law.

19. Anti-Spam Filtering

When implementing an anti-spam filter into its operations, an organization is
required to inform employees of monitoring policies being implemented in the
workplace and give employees the opportunity to review the isolated emails
designated as spam before elimination. While not mandatory, an organization
may be required to give employees the opportunity to opt out from the anti-
spam filter.

Under the GDPR the situation is likely to remain the same.

20. Cookies

There are no specific laws/rules that regulate the deployment of cookies, but
the general laws (especially the TMA) apply. Depending on the type of cookie,
consent of Data Subjects by active indication may be required before cookies
can be used. Please note that some types of cookies that track or monitor the
user may not be permitted.

The GDPR also not specifically addresses the use of cookies. However, the
same is, inter alia, the subject matter of the draft ePrivacy Regulation that was
proposed by the European Commission in January 2017. According to the
draft, the use of cookies will require the user’s consent, unless the cookie is
required to provide the service to the customer.

21. Direct Marketing

Both, under the current FDPA and the GDPR, an organization that plans to
engage in direct marketing activities with a Data Subject may be required to
obtain the Data Subject’s prior express (opt-in) consent, which cannot be
inferred from a Data Subject’s failure to respond or opt out. An organization
may be required to obtain consent for a specific activity (see Section 1 for
further details).

The draft ePrivacy Regulation also generally requires prior opt-in consent for
sending direct electronic marketing communications.
1. Recent Privacy Developments

In 2016 and 2017, the Hellenic Data Protection Authority (“HDPA”) participated in the Article 29 Data Protection Working Party and took part in the preparation and drafting of guidelines for the new legal framework introduced by the General Data Protection Regulation (GDPR). It continues to take preparatory steps to comply with the new obligations and responsibilities deriving from GDPR.

In 2017, HDPA issued the following decisions (among others): (i) it sanctioned companies for violating the legal provisions for sending unsolicited advertising messages by email and for making telephone calls with or without human intervention for the purpose of promoting products and services; (ii) it ruled on the petitions against the refusal of Google to satisfy the request to abolish the links from the results of Google Web Search; (iii) it prohibited the use of biometrical data of candidates to an international educational organization; (iv) it ruled on the means of information of debtors by legal entities appointed to inform debtors on their debts; and (v) ruled on the issue of employee monitoring.

2. Emerging Privacy Issues and Trends

The most important event will be the GDPR starting to apply on 25 May 2018.

Key obligations under GDPR will be to objectively demonstrate processing of Personal Data in accordance with GDPR, keep records of processing activities (where applicable), adopt privacy by design and by default principles; conduct data protection impact assessments, appoint a Data Protection Officer (where applicable), and notify data breaches.

With regard to Data Subjects’ rights, GDPR tightens the rules for consent and provides for the right to erasure and right to data portability

Failure to comply with GDPR may result in severe fines up to 20 million Euro or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is higher.

3. Law Applicable

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (“PIPPD”), as amended and in force today, implementing the Data Protection Directive (95/46/EC). As of 25 May 2018, the GDPR will apply instead. There have not been any official declarations about Greece’s existing data protection laws in light of the GDPR nor have drafts of a new national data protection law supplementing GDPR been published. There is, however, a legislative committee looking at opening clauses under GDPR.

4. Key Privacy Concepts

a. Personal Data
Pursuant to the definitions provided by PIPPD, “Personal Data” means any information relating to a Data Subject. A “Data Subject” means any natural person, to whom the data refers and whose identity is identified or may be identifiable, i.e., his/her identity may be determined directly or indirectly, in particular by reference to an identity card number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, political or social identity.

b. Data Processing
Pursuant to the definition provided by PIPPD, “Processing of Personal Data” means any operation or set of operations which is performed upon Personal Data by public administration or by a public law entity or private law entity or an association or a natural person, whether or not by automatic means, such as collection, recording, organization, preservation or storage, alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, interconnection, blocking (locking), erasure or destruction.

c. Processing by Data Controllers
PIPPD applies to any person (public administration or by a public law entity or private law entity or an association or a natural person) who determines the purposes and means of the Processing of Personal Data (“Data Controller”). PIPPD also applies to those persons who process Personal Data on behalf of the Data Controller, such as natural or legal persons, public authorities or agencies or any other organizations (“Data Processor”).

d. Jurisdiction/Territoriality
PIPPD applies to any Processing of Personal Data provided that such Processing is carried out:

- by a Data Controller or a Data Processor established in Greek territory or in a place where Greek law applies by virtue of public international law; or

- by a Data Controller who is not established in the territory of either an EU Member State or a member of the European Economic Area (“EEA”) but in a third country and who, for the purposes of Processing Personal Data, makes use of equipment, automated or otherwise, situated in the Greek territory, unless such equipment is used only for the purposes of transit through such territory.
e. **Sensitive Personal Data**

Pursuant to the definition provided by PIPPD, “Sensitive Data” means data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, social welfare and sexual life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas.

Pursuant to PIPPD the collection and Processing of Sensitive Data is prohibited. Exceptionally, the collection and Processing of Sensitive Data, as well as the establishment and operation of the relevant file, is permitted by the HDPA which is granted only if one of the following conditions occur:

- the Data Subject has given his/her written consent, unless such consent was extracted in a way contrary to the law or morality, or if the law provides that any consent given may not lift the relevant prohibition;

- the Processing is necessary to protect the vital interests of the Data Subject or the interests provided for by the law or by a third party, if the Data Subject is physically or legally incapable of giving his/her consent;

- the Processing relates to Personal Data made public by the Data Subject or is necessary for the recognition, exercise or defense of rights in a court of justice or before a disciplinary body;

- the Processing relates to health matters and is carried out by a health professional subject to the obligation of professional secrecy or relevant codes of conduct, provided that such Processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services;

- the Processing is carried out by a public authority and is necessary for the purposes of (i) national security, (ii) criminal or correctional policy and pertains to the detection of offenses, criminal convictions or security measures, (iii) protection of public health or (iv) the exercise of public control on fiscal or social services;

- the Processing is carried out exclusively for research and scientific purposes, provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken; or

- the Processing concerns data pertaining to public figures, provided that such data is in connection with the holding of public office or the management of third parties’ interests and is carried out solely for journalistic purposes. HDPA may grant a permit only if such Processing is absolutely necessary to ensure the right to information on matters of public interest as well as in the framework of literary expression and
provided that the right to protection of private and family life is not violated in any way whatsoever.

Pursuant to PIPPD, the Data Controller is released from the obligation to obtain from the HDPA prior approval for the collection and Processing of Sensitive Data, in case:

- the Processing is carried out exclusively for purposes relating directly to an employment contract or a contract for work or to the provision of services to the public sector and such Processing is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the above-mentioned contractual relationships and the Data Subject has been previously informed;

- the Processing involves clients’ or suppliers’ data provided that such data is neither transferred nor disclosed to third parties. Insurance companies, pharmaceutical companies, credit or financial institutions are not exempted from the obligation of notification. Courts of justice and public authorities are not considered third parties, provided that such a transfer or disclosure is imposed by law or a judicial decision;

- the Processing is carried out by societies, enterprises, associations and political parties and relates to Personal Data of their members or companies, provided that the latter have given their consent and that such data is neither transferred nor disclosed to third parties. Courts of justice and public authorities are not considered third parties, provided that such a transfer or disclosure is imposed by law or a judicial decision;

- the Processing involves medical data and is carried out by doctors or other persons rendering medical services, provided that the Data Controller is bound by medical confidentiality or other obligation of professional secrecy provided for in the law or code of practice and that such data is neither transferred nor disclosed to third parties. Courts of justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision;

- the Processing is carried out by lawyers, notaries, land registrars and bailiffs or companies formed by the aforementioned and involves the provision of legal services to their clients, provided that the Data Controller is bound by an obligation of confidentiality imposed by law and that the data is neither transferred nor disclosed to third parties, except for those cases where it is necessary and it is directly related to the fulfillment of a client’s mandate; or

- the Processing is carried out by judicial authorities or services with the exception of the judicial or public prosecution authorities and authorities...
which act under their supervision in the framework of attributing justice or for their proper operational needs.

f. **Employee Personal Data**

According to PIPPD, if Processing is carried out exclusively for purposes relating directly to an employment or project relationship or to the provision of services to the public sector and is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the aforementioned relationships and the Data Subject has been notified in advance, the Data Controller is discharged from the obligation to file a notification with the HDPA and also from the obligation to obtain HPDA’s permission for the Processing of its employees’ Sensitive Data.

Apart from the above exception, all other requirements set by PIPPD must be satisfied also for the Processing of both employees’ Sensitive and non-Sensitive Personal Data.

HDPA, having taken into consideration the various issues arising from the Processing of Personal Data in the employment context and among others, the opinion of the Article 29 Working Party, has issued its Decision 115/2001 whereby HDPA interprets the existing regulatory framework and indicates how the various issues are likely to be considered in future cases that might be brought before it. Decision 115/2001, among others, sets out the principles for the protection of employees’ Personal Data (including those of former employees or candidate employees) as follows:

- the collection and Processing of employees’ Personal Data must be carried out with lawful means and in a way that ensures the respect of employees’ privacy, personality and dignity in the working environment;

- the collection and Processing of employees’ Personal Data is allowed exclusively for purposes directly connected to the employment relationship and provided that such Processing is necessary for the fulfilment of both sides’ obligations arising either from the law or from the employment contract. The purposes for which the Processing of employees’ Personal Data is carried out must be clear and definite. The Processing of employees’ Personal Data for reasons that do not involve the employment relationship directly or indirectly is prohibited. Employees should be notified in advance of the above purposes of the Processing and should be able to understand them. Moreover, the giving of consent by the employee cannot legitimize the Processing for purposes other than the ones described above;

- Decision 115/2001 specifically mentions that due to the inherent inequality of the parties in an employment contract and to the position of the employee, the requirement of a consent being given freely by the
employee, which is a necessary element of permissible Processing, can be questioned in the employment context;

- the employees’ Personal Data that is processed should be adequate, relevant and not excessive in relation to the purposes for which it is collected and processed, should not be kept for longer than is necessary for such purposes and should be kept up to date;

- the employees may not waive the rights granted to them under PIPPD and any such waiver is null;

- the exercise of rights provided for by PIPPD can in no way have negative consequences for the employees (such as negative evaluation of the employee or termination of the employment contract);

- decisions by the employer in relation to the conduct or the efficiency of the employees should not be taken exclusively on the basis of an automated Processing of Personal Data; and

- Personal Data collected and processed in order to monitor the safe operation of systems in the working environment may not be used for the control of the employees’ conduct.

5. Consent

a. General

“The Data Subject’s Consent” (“Consent”) constitutes any free, explicit and specific declaration of will, which is given in a clear way and in full awareness. By such Consent the Data Subject, having been previously informed, agrees that Personal Data relating to him/her may be processed.

The giving of Consent by the Data Subject is required in order for the Processing of Personal Data to be permissible according to the law. In exceptional circumstances, however, the Processing of Personal Data may be carried out, even if no Consent has been given by the Data Subject, if the other requirements provided for by PIPPD are met.

Written Consent for the Processing of non-Sensitive Personal Data is not required, although Consent in writing is the most practical and safest way to secure compliance with the requirements of the law.

Although PIPPD does not expressly set any language requirements for Consent, on the basis of the above definition of Consent, such Consent must be given in a language that the Data Subject fully understands.

Also, as the giving of Consent presupposes that the Data Subject has been informed about the Processing in advance, in a proper and clear way, and is fully aware of the conditions under which he/she gives his/her Consent, it follows that the relevant information should be given to the Data Subject in

\[\text{Baker McKenzie} \ | \ 285\]
his/her language or at least in a language that he/she fully understands and the Consent may be revoked anytime with no retroactive effect.

b. Sensitive Data
Where Consent is relied upon to justify the Processing of Sensitive Data, it must be obtained in writing prior to the Processing.

c. Minors
There is no specific regulatory prohibition or any guidance from the HDPA on the collection of Personal Data from children. The Processing of Personal Data related to minors has to be made under the requirements of PIPPD. Notification and Consent requirements have to be obtained from the parents exercising parental care and representing their child in every affair or legal action.

d. Employee Consent
All the requirements set by PIPPD for the giving of Consent by any Data Subject shall equally apply to Consent given by employees. As in all other cases, in the employment context the giving of Consent constitutes the rule for a legitimate Processing of Personal Data.

Nevertheless, as mentioned above, HDPA has acknowledged the possible invalidity of Consent given in the employment context, due to the fact that the position of the employee may not allow the free giving of such Consent. However, HDPA has not provided any specific guidelines as to when Consent may be considered to have been freely given.

HDPA in Decision 115/2001 has stressed, however, that the giving of Consent by an employee cannot provide a remedy for non-compliance with the principles of a legitimate Processing (e.g., consent in relation to Processing for purposes not connected with the employment contract) and therefore it generally follows from Decision 115/2001 that the Consent is valid when it refers to the Processing of Personal Data for which all other requirements of the law are met.

e. Online/Electronic Consent
HPDA issued Directive 2/2011, which sets out the requirements for the legitimate granting of Consent by electronic means (“Electronic Consent”) for the Processing of Personal Data of a subscriber or user by a Data Controller within the framework of Article 11 of Law 3471/2006 on the Protection of Personal Data and Privacy in the Electronic Communications Sector, i.e., for effecting communications for the purpose of direct marketing or other advertising purposes by using communication systems without human intervention (emails, SMS, MMS, etc.).
6. Information/Notice Requirements

The Data Controller must inform the Data Subject of the following when Personal Data is collected:

- the identity (name, precise address and telephone number) of the Data Controller and, if applicable, of its representative in Greece;
- the purposes of Processing;
- the Personal Data or categories of Personal Data being processed by the Data Controller;
- the recipients or categories of recipients of the Personal Data; and
- the Data Subject’s right of access to the Personal Data and the right to object to the Processing of Personal Data relating to the Data Subject.

The Data Subject must be informed of any change in the above information promptly and in any event prior to any further use or Processing of the changed Personal Data.

If Personal Data is disclosed to a third party, the Data Subject must be informed in writing prior to such disclosure.

When Personal Data is collected directly from the Data Subject, the Data Controller must provide the information at the time of collection. If Personal Data is collected from other sources, the Data Subject should be informed promptly and in any case prior to any further use or Processing of the Personal Data.

If the Data Subject gives his/her required Consent or assistance to the Data Controller for the collection of Personal Data, then the Data Subject must receive the above information in writing.

If the Data Subject’s Consent is not required for the collection and Processing of Personal Data, the Data Subject must be informed about the Processing in the most appropriate and unambiguous way, so that the Data Subject is freely and adequately informed, e.g., by hanging a notice in the place of business or by delivering printed material.

The above obligation of the Data Controller to provide information to the Data Subject may be lifted by a decision of the HDPA if the Processing of the Personal Data is carried out for purposes of national security or for the investigation of particularly serious crimes.

Without prejudice to the right of access and to the right to object to the Processing of Personal Data, the above obligation to inform the Data Subject does not exist if the Processing takes place exclusively for journalistic purposes and refers to public figures.
No language requirements are stipulated in PIPPD, however, the relevant information should be given to the Data Subject in the language spoken, or at least clearly understood, by the Data Subject.

7. Processing Rules

According to PIPPD, the Processing of Personal Data is allowed only if the Data Subject has given his/her Consent. In the specific exceptional cases listed below, Processing is allowed without the giving of Consent:

- if Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- if Processing is necessary for compliance with a legal obligation to which the Data Controller is subject;
- if Processing is necessary in order to protect the vital interests of the Data Subject, where the latter is physically or legally incapable of giving consent;
- if Processing is necessary for the performance of a task of public interest or of a task falling within the scope of exercise of public power and performed by a public authority or assigned by the latter either to the Data Controller or to a third party to whom the Personal Data is disclosed; or
- if Processing is absolutely necessary for the purposes of satisfaction of the legitimate interest pursued by the Data Controller, or by the third party or parties to whom the Personal Data is disclosed, provided that such interest obviously overrides the interests and rights of the Data Subjects and the fundamental freedoms of the Data Subjects are not offended.

The Data Controller must also ensure that:

- Personal Data is collected in a fair and legitimate way, for specified, explicit and legitimate purposes and further processed fairly and legitimately in view of those purposes;
- Personal Data is adequate, relevant and not excessive in relation to the purposes for which they are processed;
- Personal Data is accurate and up-to-date; and
- Personal Data is kept in a form that allows the identification of the Data Subjects to whom such Personal Data refers, only as long as it is necessary for the purpose for which it was collected and processed.

The Processing of Personal Data must be confidential and must be carried out exclusively by persons supervised and acting only on the basis of instructions from the Data Controller or the Data Processor. The Data Controller must...
select persons with relevant professional skills, who provide sufficient guarantees in respect of technical expertise and personal integrity ensuring compliance with confidentiality requirements.

The Data Controller must implement appropriate organizational and technical measures to secure data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access as well as any other form of unlawful Processing. Such measures must ensure a level of security appropriate to the risks presented by Processing and the nature of the data processed.

In addition to the above, the other requirements set by PIPPD for the Processing of Personal Data must be complied with.

8. Rights of Individuals

Right of access: A Data Subject has the right to be provided, on request and without any delay, with information on his/her Personal Data that is processed by the Data Controller. The information provided by the Data Controller must be in an intelligible form and include:

- all the Personal Data related to the Data Subject making the request as well as their source(s);
- the purposes for which the Personal Data is processed;
- the recipients or categories of recipients of the Personal Data;
- the development of the Processing during the period from the last notification or information to the Data Subject; and
- the logic involved in an automated Processing.

If the Data Controller fails to reply within 15 days or his/her reply is not satisfactory, the Data Subject may appeal before the HDPA. If the Data Controller refuses to satisfy the Data Subject’s request, the Data Controller must notify his/her reply to the HDPA and inform the interested party who can then appeal before the HDPA.

A Data Subject has the right to:

- be informed by the Data Controller prior to the Processing of his/her Personal Data;
- object in writing to the Processing of his/her Personal Data and receive a response from the Data Controller within 15 days and to have Personal Data rectified, non-transferred, blocked or erased where the Processing of that Personal Data has not been conducted in accordance with the law;
• apply to any competent court for the suspension or non-application of an act or decision affecting him/her, based solely on automated Processing of Personal Data intended to evaluate his/her personality and especially his/her effectiveness at work, creditworthiness, reliability and general conduct;

• to claim full compensation for any material damage suffered as well as for moral damages suffered as a result of a violation of the provisions of PIPPD by any natural person or legal entity; and

• to prevent the Data Controller from using his/her Personal Data for the purposes of direct marketing.

9. Registration/Notification Requirements

The Data Controller is required to file a notification with the HDPA before commencing any manual or automated data Processing. The notification requires detailed information including the following:

• the name, or the trade name or distinctive title of the Data Controller as well as his/her address;

• the address where the file or the main equipment supporting the Processing is situated;

• a description of the purpose for which the Personal Data included in the file or to be included in the file are processed;

• the kind of Personal Data that is processed or intended to be processed or included or intended to be included in the file;

• the time period during which the Processing of the Personal Data is expected to be carried out or the file is expected to be maintained;

• the recipients or categories of recipients to whom the Personal Data is or might be disclosed;

• any eventual transfer of Personal Data to other countries and the purpose of such transfer; and

• the basic characteristics of the system and of the safety measures of the file or of the Processing.

The above information is registered in a Register of Files kept by the HDPA. Any modification of the information referred to above must be communicated, in writing and without any delay, to the HDPA.
Pursuant to PIPPD, the Data Controller is released from the obligation to make a notification to the HDPA in case:

- the Processing is carried out exclusively for purposes relating directly to an employment contract or a contract for work or to the provision of services to the public sector and such Processing is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the above-mentioned contractual relationships and the Data Subject has been previously informed;

- the Processing involves clients’ or suppliers’ data, provided that such data is neither transferred nor disclosed to third parties. Insurance companies, pharmaceutical companies, credit or financial institutions are not exempted from the obligation of notification. Courts of justice and public authorities are not considered third parties, provided that such a transfer or disclosure is imposed by law or a judicial decision;

- the Processing is carried out by societies, enterprises, associations and political parties and relates to Personal Data of their members or companies, provided that the latter have given their consent and that such data is neither transferred nor disclosed to third parties. Courts of justice and public authorities are not considered third parties, provided that such a transfer or disclosure is imposed by law or a judicial decision;

- the Processing involves medical data and is carried out by doctors or other persons rendering medical services, provided that the data Controller is bound by medical confidentiality or other obligation of professional secrecy provided for in the law or code of practice and that such data is neither transferred nor disclosed to third parties. Courts of justice and public authorities are not considered third parties provided that such a transfer or disclosure is imposed by law or a judicial decision;

- the Processing is carried out by lawyers, notaries, land registrars and bailiffs or companies formed by the aforementioned and involves the provision of legal services to their clients, provided that the Controller is bound by an obligation of confidentiality imposed by law and that the data is neither transferred nor disclosed to third parties, except for those cases where is necessary and is directly related to the fulfillment of a client’s mandate; or

- the Processing is carried out by judicial authorities or services with the exception of the judicial or public prosecution authorities and authorities which act under their supervision in the framework of attributing justice or for their proper operational needs.
10. Data Protection Officers

PIPPD provides that the Processing of Personal Data should be carried out exclusively by persons supervised by and acting on the basis of instructions from the Data Controller or the Data Processor. Indirectly, it can be inferred from this requirement that the Data Controller or the Data Processor must appoint specific persons who will undertake the task of Processing Personal Data. There is no provision indicating that the above persons appointed by the Data Controller or the Data Processor should also be notified to the HDPA, although the standard registration/notification form (prepared by the HDPA) requires that the contact details of a natural person nominated by the Data Controller be included therein, for the purpose of providing additional information that may be required by the HDPA.

11. International Data Transfers

Pursuant to PIPPD, the transfer of Personal Data is permitted: (i) for EU Member States; and (ii) for non-EU Member States pursuant a permit granted by the HDPA if it deems that the country in question guarantees an adequate level of protection. A permit by the HDPA is not required if the European Commission has decided on the basis of the process of Article 31, paragraph 2 of Directive 95/46/EC of the parliament and the Council of 24 October 1995 that the country in question guarantees an adequate level of protection in the sense of Article 25 of the aforementioned Directive.

The transfer of Personal Data to a non-EU Member State that does not ensure an adequate level of protection is exceptionally allowed pursuant to a permit by the HDPA, provided that one or more of the following conditions occur:

- the Data Subject gives his/her consent for the transfer, unless such consent has been extracted contrary to law or morality;
- the transfer is necessary: (i) for the protection of the vital interests of the Data Subject, provided he/she is physically or legally incapable of giving consent; or (ii) for the conclusion and performance of a contract between the Data Subject and the Data Controller or between the Data Controller and a third party in the interests of the Data Subject;
- the transfer is necessary in order to address an exceptional need and safeguard a superior public interest, especially for the performance of a co-operation agreement with the public authorities of the other country, provided the Data Controller adduces sufficient safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of corresponding rights;
- the transfer is necessary for the establishment, exercise or defense of a right before the court; or
• the transfer is made from a public register which according to the law, is intended to provide information to the public and which is open to consultation either by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in the law for consultation are fulfilled in the particular case.

The Data Controller shall provide adequate safeguards with respect to the protection of the Data Subjects’ Personal Data and the exercise of their rights, when the safeguards arise from conventional clauses which are in accordance with the regulations of PIPPD. A permit is not required if the European Commission has decided, on the basis of Article 26, paragraph 4 of Directive 95/46/EC that certain clauses offer adequate safeguards for the protection of Personal Data.

12. Security Requirements
The Data Controller must implement appropriate technical and organizational measures for the safety of the Personal Data and also to protect Personal Data against accidental or unlawful destruction or accidental loss or unauthorized alteration, disclosure or access, as well as any other form of unlawful Processing. Such measures must ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data. HDPA proposes that Data Controllers adopt security plans, security policies, disaster, recovery and contingency plans.

13. Special Rules for the Outsourcing of Data Processing to Third Parties
Where the Data Controller outsources the Processing to a Data Processor who is not dependent on the Data Controller, the Processing must be carried out under a contract which:

i. is made in writing;

ii. requires the Data Processor to act only on the basis of the instructions of the Data Controller and comply with the security and confidentiality obligations of the law equivalent to those imposed on the Data Controller.

14. Enforcement and Sanctions
Sanctions for breach of the Data Controllers’ duties arising from PIPPD include administrative sanctions, penal sanctions and civil liability.

**Administrative sanctions**

The following administrative sanctions may be imposed:

a. a warning with an order for the violation to cease within a specified time limit;
b. a fine ranging from EUR 880.41 to EUR 14,673.51;
c. a temporary revocation of the permit;
d. a definitive revocation of the permit; or
e. the destruction of the file or a discontinuance of the Processing and the
destruction of the relevant Personal Data.

The sanctions in items b, c, d, and e above will only be imposed following an
administrative hearing before the HDPA. The sanctions in items c, d, and e
will be imposed in the case of serious or repeated violation. A fine may be
imposed in conjunction with the sanctions in items c, d and e above.

Penal sanctions

There are various penal sanctions provided for in PIPPD depending on the
breach of its provisions. The relevant punishment may be imprisonment from
10 days to 5 years and fines ranging from EUR 2,934.70 to EUR 29,347.03.
The penalties are as follows:

i. any person (or in the case of a legal entity the legal representative(s))
processing Personal Data without a notification to the HDPA (where such
notification is required) is punishable with imprisonment of up to three
years and a penalty from EUR 2,934.70 to EUR 14,673.51;

ii. any person (or in the case of a legal entity the legal representative(s))
processing Sensitive Personal Data without permission by the HDPA or in
violation of the terms and conditions of the HDPA’s permission is
punishable with imprisonment of at least one year and a penalty from
EUR 2,934.70 to EUR 14,673.57;

iii. any person (or in case of a legal entity the legal representative(s))
interconnecting files without notification to the HDPA, is punishable with
imprisonment of up to three years and a penalty from EUR 2,934.70 to
EUR 14,673.57. Any person interconnecting files without the permission
of the HDPA (where such permission is required) or in violation of the
permission granted, is punishable with imprisonment of at least one year
and a penalty from EUR 2,934.70 to EUR 14,673.57;

iv. any person (or in case of a legal entity, the legal representative(s)) that
interferes with Personal Data files or takes knowledge of such Personal
Data or alters, damages, destroys, processes, transfers, communicates
or gives access to such Personal Data to third parties or exploits the
Personal Data in any way, is punishable with imprisonment and a fine; or

v. a Data Controller who fails to comply with the requirements of PIPPD with
regard to transfers of Personal Data, is punishable with imprisonment of
at least two years and pecuniary penalty ranging from EUR 2,934.70 to EUR 14,673.51.

Where violations under items i. and v. are due to negligence, the liable person is punishable with imprisonment of up to three years and pecuniary penalty. Furthermore, if such violations were committed in order for the liable person to obtain, for himself/herself or for any other party, an illegal financial benefit or in order to damage a third person, then the liable person is punishable with imprisonment from 5 to 10 years and a pecuniary penalty from EUR 5,869.40 to EUR 29,347.03.

If the breach of certain provisions of PIPPD has created a risk to the democratic constitution or to national security, the punishment may include imprisonment of up to 20 years and a fine ranging between EUR 14,673.51 and EUR 29,347.03.

Civil liability

Any natural person or legal entity who, in breach of PIPPD, causes material damage will be liable for damages in full. If damages are non-pecuniary (e.g., moral damages) compensation may be payable. In the case of moral damages, minimum compensation is set at EUR 5,869.40, unless the plaintiff claims a lesser amount or the breach was due to negligence. Such compensation is awarded irrespective of the claim for damages.

Recent penalties imposed by HDPA for non-compliance with PIPPD:

• EUR 75,000 fine imposed on a legal entity for sending a large number of emails to a large number of Data Subjects for promotional/advertising purposes in violation of the PIPPD requirements on Data Subject’s consent;

• EUR 50,000 fine imposed on a financial institution due to a failure to safely destruct data files and for violation of Data Subjects’ right to access their data;

• EUR 30,000 fine imposed on a private company for violation of the Data Subjects’ right to object;

• EUR 30,000 fine imposed on a financial institution for violation of the obligation to ensure lawful Processing of data (Processing of non-accurate and out-of-date data) and Data Subjects’ right to object;

• EUR 30,000 fine imposed on a company providing telecommunication services for violation of Data Subjects’ right to object and unlawful interconnection of files;

• EUR 15,000 fine imposed on a private company for violation of Data Subjects’ right to access their data;
• EUR 10,000 fine imposed for unlawful publication of sensitive data;
• EUR 4,000 fine imposed for violation of Data Subject’s right to information; and
• Decisions of Greek Civil Courts granting Data Subjects monetary awards ranging from EUR 3,000 up to EUR 15,000 for moral damages caused by the violation of PIPPD.

15. Data Security Breach
Apart from the principles of confidentiality and security of any Processing set by PIPPD and apart from HDPA’s guidance on security measures, there has been no specific decision or guidance issued by HDPA in relation to specific notification requirements in cases of security breaches.

16. Accountability
We have not been able to trace any law or decision of the HDPA requiring the conduct of privacy impact assessment prior to implementing new information systems for the Processing of Personal Data.

17. Whistle-Blower Hotline
We have not been able to trace any law or decision of the HDPA setting principles or specific requirements for the implementation of whistle-blowing schemes in Greece. Therefore, for a whistle-blowing scheme to be lawful, it should be in compliance with all the principles and requirements set forth by PIPPD.

18. E-Discovery
When implementing an e-discovery system, a Data Controller is required to inform the users (e.g., employees) and comply with the principles of lawful Processing of Personal Data set by PIPPD.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution, a Data Controller is required to inform employees of monitoring policies being implemented and comply with the principles of lawful Processing of Personal Data set by PIPPD.

20. Cookies
The use of cookies must comply with the principles set by PIPPD.

21. Direct Marketing
Pursuant to Article 11 of Law 3471/2006 on the Protection of Personal Data and Privacy in the electronic communications sector, “the use of automated calling systems without human intervention, facsimile machines or email for
the purposes of direct marketing of goods or services or any advertising purposes may only be allowed in respect of subscribers who have given their prior explicit consent”. Exceptionally where a natural or legal person obtains from its customers their electronic contact details for email, in the context of the sale of a product or service, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner to such collection and use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use. Moreover, the practice of sending email for the purposes of direct marketing of goods and services disguising or concealing the identity of the sender or on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease is prohibited.

In addition, the decision of the HDPA no. 26 dated 26 April 2004, on the conditions under which the Processing of Personal Data for the purposes of direct marketing or advertising is permissible, provides that a free, explicit and specific consent is required, by which the Data Subject, after having been properly informed, agrees in advance to the Processing of his/her Personal Data for direct marketing purposes (i.e., an opt in).

In exceptional cases, Processing Personal Data for direct marketing purposes is lawful, even if no consent is given by the Data Subject, provided that: (i) such Processing is absolutely necessary for the purposes of the legitimate interests pursued by the Data Controller; (ii) such legitimate interests of the Data Controller clearly override the interests of the Data Subject; and (iii) the fundamental rights and freedoms of the Data Subject are not offended.

In its above decision, the HDPA sets the following conditions under which the above exception (i.e., Processing without consent) shall apply:

- the Personal Data comes from directories intended for public access and it is certain that the Data Subjects included therein have given their consent for inclusion in such directories, or comes from publicly accessible sources intended to provide information to the public, provided that the legal requirements for access to such sources have been observed or the Data Subject himself/herself has published his/her details for marketing or similar purposes;

- the Data Controller has received information from the Registry kept by the HDPA concerning the persons that do not wish for their Personal Data to be included in files of data that is processed for the purposes of promotion of sales of goods or services from a distance and has excluded such persons from his/her files;
the Data Controller only keeps the Personal Data that is absolutely necessary for the specific purposes and such Personal Data consists solely of the name, address and profession of the Data Subjects; or

the purpose of the Processing is restricted to advertising or promotion of sale of goods or the provision of services from a distance and is not contrary to good morals.

Further, the above decision of the HDPA provides, among other requirements, that the Data Controller must provide information to the Data Subject at the time of collection and during the first transmission of the Personal Data in accordance with the relevant provisions of PIPPD and the decisions of the HDPA on provision of information to Data Subjects. Moreover, recipients of Personal Data collected for a purpose relevant to the direct commerce may be persons that need such data to conduct lawful activities.
Hong Kong

Susan Kendall
Hong Kong
Tel: +852 2846 2411
susan.kendall@bakermckenzie.com

Paolo Sbuttoni
Hong Kong
Tel: +852 2846 1521
paolo.sbuttoni@bakermckenzie.com
1. Recent Privacy Developments

The key legislation regulating data privacy in Hong Kong is the Personal Data (Privacy) Ordinance ("PDPO"). Significant amendments to the PDPO were passed in 2012, in particular to include stricter requirements on direct marketing.

Since these reforms, there has not been any new privacy related legislation in Hong Kong. There are, however, three key developments that we wish to highlight for 2016/17:

(1) Continued focus on direct marketing enforcement

Since 2015, we have seen increasing enforcement of the PDPO direct marketing provisions, which indicates a hard line on compliance taken by the regulator, the Privacy Commissioner for Personal Data ("Commissioner"), and the courts.

(2) Relevance of GDPR compliance for Hong Kong companies

In anticipation of the EU’s General Data Protection Regulation ("GDPR") coming into force on 25 May 2018 (which has extraterritorial effect), the Commissioner’s office has been carrying out a comparative study between the GDPR and the PDPO.

The Commissioner commented in September 2017 that his office will publish guidance to help organisations understand the GDPR’s standards.

(3) Industry specific cybersecurity requirements

There is currently no single overarching law relating to cybersecurity in Hong Kong. However, with the increase in data breaches and threat of cyber attacks, Hong Kong’s financial services regulators, the Securities and Futures Commission ("SFC") and the Hong Kong Monetary Authority ("HKMA"), have both released detailed specific guidance on cybersecurity.

In March 2016, the SFC published a Circular to all Licensed Corporations on Cybersecurity, which suggests a number of controls to combat the threat of cyberattacks, including implementing strong governance frameworks and effective incidence, and crisis management procedures. More recently, the SFC issued a Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading in May 2017. The proposals include new guidelines setting out 20 baseline cybersecurity requirements that internet brokers must comply with, to reduce and mitigate hacking risks associated with internet trading, including establishing preventive controls, detective controls and a cybersecurity risk management framework.

In May 2016, the HKMA announced its “Cybersecurity Fortification Initiative” ("CFI"), which aims to raise the level of cybersecurity of banks in Hong Kong.
A key element of the CFI is a “Cyber Resilience Assessment Framework” which seeks to establish a common risk-based framework for banks to assess their own risk profiles and determine the level of defense and resilience required.

Further, in December 2016, the HKMA launched an industry-wide “Enhanced Competency Framework on Cybersecurity”, which sets out the qualifications and certifications that staff undertaking cybersecurity roles should have, and details the suggested Continuing Professional Development requirements of such staff.

2. Emerging Privacy Issues and Trends

**Decrease in privacy complaints from 2015 to 2016**

In 2016, the Commissioner received 1,838 complaints, which represents a drop of 7% in complaints from the record high 1,971 complaints received in 2015.

The majority of the complaints (82%) were in relation to the use of Personal Data without consent and collection of Personal Data.

**Data protection enforcement**

Since 2015, we have seen enforcement of the direct marketing provisions that came into force in 2013. In 2015 and 2016, the Commissioner issued 53 warnings and 73 enforcement notices to organizations, and referred 112 cases to the police for criminal investigation and prosecution. Over the past few years, companies have been convicted for:

- Failure to comply with a request from a Data Subject to cease use of his/her Personal Data in direct marketing;
- Failure to take specified steps under the PDPO in relation to direct marketing, including to obtain the Data Subject’s consent before using his/her Personal Data for direct marketing; and
- Failure to inform the Data Subject of his/her right to opt out of direct marketing without charge.

These convictions arose out of complaints to the Commissioner and demonstrate the public’s growing sensitivity to data protection and the hard line of the courts. It is anticipated that we will continue to see more enforcement actions in the future. These fines are all low (ranging from HKD 5,000 to HKD 30,000). However, the cases all involve a limited amount of Personal Data. As potential penalties are fines of up to HKD 1 million and five years’ imprisonment, there is a likelihood of higher fines, in particular where cases involve large amounts of Personal Data.
Decrease in data breaches reported from 2015 to 2016

The Commissioner reported that in 2016, 89 data breach incidents affecting approximately 104,000 Hong Kong individuals were reported to the Office of the Privacy Commissioner for Personal Data (“PCO”). This represents a drop from the 98 incidents involving 871,000 individuals in 2015. The incidents involved the loss of documents and portable devices, hacking, inadvertent disclosure of Personal Data by fax, email or post, and system failure.

3. Law Applicable

The PDPO was enacted on 20 December 1996, and was amended by the Personal Data (Privacy) (Amendment) Ordinance in 2012. The amendments dramatically increased penalties, introduced new offenses particularly focused on direct marketing and unauthorized disclosure of Personal Data and introduced other changes to strengthen the law.

The PDPO is a principle-based law. Schedule 1 of the PDPO sets out the six data protection principles (“DPPs”), which govern the collection, use, processing, security, retention/destruction and access to Personal Data. The requirements under the PDPO also apply in the employment context.

The PCO is the regulatory body that oversees the enforcement of the PDPO. Contraventions of the PDPO may lead to criminal sanctions (fines and/or imprisonment). The maximum penalty for failure to comply with an enforcement notice is a fine of up to HKD 100,000 (approximately USD 12,900) and two years’ imprisonment. Penalties for direct marketing offenses may be a fine of up to HKD 1 million (approximately USD 129,000) and five years’ imprisonment.

Hong Kong also has an anti-spam law, the Unsolicited Electronic Messages Ordinance (“UEMO”), which came into effect on 22 December 2007. The UEMO regulates the sending of unsolicited commercial electronic messages in Hong Kong.

4. Key Privacy Concepts

a. Personal Data

The PDPO defines “Personal Data” as any data relating directly or indirectly to a living individual and from which it is practicable to ascertain the identity of the individual and which is in a form in which access to or processing of the data is practicable.

“Data”, which the definition of Personal Data encompasses, is defined as any representation of information (including an expression of an opinion) in any document. Personal Data must therefore be in a documented form for it to fall within the scope of the PDPO.
b. Data Processing
The PDPO defines “processing” to mean and include amending, augmenting, deleting or rearranging Personal Data, whether by automated means or otherwise. The PDPO also has a concept of data “use” which includes the disclosure or transfer of Personal Data.

The PDPO specifies that data users are liable for the actions of its Data Processors (e.g., service providers that process data on behalf of a data user). Further, it requires data users to adopt contractual or other means to prevent:

- Personal Data transferred to a Data Processor from being kept longer than is necessary for the processing; and

- unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the Data Processor for processing.

c. Processing by Data Controllers
The PDPO applies to “data users”, that is persons who, either alone or jointly or in common with other persons, control the collection, holding, processing or use of the Personal Data. However, a person is not a data user if he or she holds, processes or uses Personal Data solely on behalf of another person and he or she does not hold, process or use the Personal Data for any of his or her own purposes. Data Processors are not directly regulated in Hong Kong, therefore, the data user is liable for the actions of its Data Processors.

d. Jurisdiction/Territoriality
The PDPO applies to any collection, holding, processing or use of the Personal Data in Hong Kong. It also applies to all such data users who either have their principal place of business or registered address in Hong Kong.

e. Sensitive Personal Data
The PDPO does not specifically define Sensitive Personal Data. All types of Personal Data are subject to the same rules. Note, however, that the PCO issued non-binding guidance in July 2015 on the collection and use of “biometric data”, which it appears to treat as a more sensitive category of data. In addition, through its guidance, the PCO treats Hong Kong identity card (“HKID”) copies and numbers as a more sensitive category of data. Collection and use of HKID numbers must comply with the Code of Practice on the Identity Card Number and Other Personal Identifiers.

f. Employee Personal Data
The Code of Practice on Human Resource Management, issued by the Commissioner and updated in April 2016, applies to employee-related Personal Data. The Commissioner also issued “Privacy Guidelines: Monitoring and Personal Data Privacy at Work” (also revised in April 2016)
that deals with privacy issues where employees are subject to monitoring. In relation to recruitment, employers cannot seek Personal Data from job applicants, unless there is a position which is or may become vacant.

5. Consent Requirements

a. General
Except with respect to direct marketing, consent of a Data Subject is not required so long as the data user informs the Data Subject at the time of or before collection of the purpose for which the Personal Data is to be used and the classes of persons to whom the data may be transferred. The Personal Data must be used only for that purpose or a directly related purpose for which it was collected and transferred only to those classes of persons notified as possible transferees on or before collection of the Personal Data. If the Personal Data is to be used in any other way, express consent of the Data Subject is required. A data user is exempted from obtaining such express consent in certain situations prescribed in the PDPO.

Consent must be given by the Data Subject for the use of Personal Data for direct marketing or for the transfer of the Personal Data to a third party for that third party’s direct marketing purpose. Further, if Personal Data is used for direct marketing purposes, the UEMO may apply to the sending and the format of commercial electronic messages.

b. Sensitive Data
As mentioned above, there are no specific rules that govern Sensitive Data. As such, Sensitive Data is subject to the same consent requirements as other Personal Data.

c. Minors
Consent of minors is not specifically addressed in any laws in Hong Kong.

d. Employee Consent
The general consent requirements also apply in the employment context.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in Hong Kong if it is properly structured and evidenced.

6. Information/Notice Requirements
Specific requirements apply. A data user must take “all practicable steps” to give the notice on or before the first collection of Personal Data if the data user or its agent collects data from the Data Subject. It is customary to do so in Hong Kong by way of a “Personal Information Collection Statement” or “PICS”.

Data users should include the following information in a Personal Information Collection Statement:

- whether or not it is voluntary or obligatory to provide the data and the consequences of not providing the data;
- the purposes for which the data is collected;
- the categories of persons to whom the data may be transferred;
- that the Data Subject has rights of access and correction; and
- to whom access and correction requests and inquiries in relation to the data user’s data protection policies and procedures should be directed.

Specific information requirements also apply where the data is to be provided for direct marketing purposes. These are detailed in Section 21.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfil the identified purpose(s) for which the Personal Data was collected; and delete anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

When engaging Data Processors, data users are required by the PDPO to adopt contractual or other means to prevent any Personal Data transferred to the Data Processor from being kept longer than is necessary for processing of the data (DPP 2), and prevent unauthorized or accidental access, processing, erasure, loss or use of the Personal Data transferred to the Data Processor for processing (DPP 4).

8. Rights of Individuals

Under DPP 6 of the PDPO, a person whose data is held by a data user is entitled to:

i. ascertain whether the data user holds data about them; and
ii. request a copy of and corrections to that data.

The above applies to all Personal Data held by the data user. Exemptions, such as legal professional privilege, apply.

A data user is required to comply with a data access request within 40 days after receiving the request. If it is unable to comply within that time, it must inform the requestor in writing that it is unable to do so and give reasons. Such explanation must be provided before the 40 days expire, and the data user must also fully comply with the request as soon as reasonably practicable after the expiry of the 40-day reply period.
The copy of Personal Data supplied must be such Personal Data as is held at the time when the request is made. Any processing of the data between the time the data access request is received and before the copy is supplied that would have been undertaken, irrespective of the receipt of the request, is not affected by this requirement. In other words, there is no requirement to stop normal data processing activities because a data access request has been received.

9. Registration/Notification Requirements

Data Processors (e.g., service providers that process data on behalf of a data user) are not directly regulated under the PDPO and a data user is fully responsible for the actions of its Data Processors. Currently, an organization that collects and processes Personal Data is not required to file with the appropriate data authority.

10. Data Protection Officers

In Hong Kong, an organization is not required to designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

However, DPP 1 does require data users to provide Data Subjects with the name or job title, and address, of the individual who will handle data access/correction requests.

11. International Data Transfers

Under Section 33 of the PDPO, the data user cannot transfer Personal Data, except in certain circumstances, including the following:

- the data user has reasonable grounds for believing that the destination jurisdiction has substantially similar provisions to the PDPO;
- the Data Subject consents in writing to the transfer; or
- the data user has exercised due diligence to ensure that the Personal Data will not be treated in a manner which will contravene the PDPO.

The above requirements are not yet effective and do not currently form part of the law in Hong Kong. However, in December 2014, the Privacy Commissioner issued voluntary Guidance on Personal Data Protection in Cross Border Transfers (“Guidance”). In the Guidance, the Commissioner recommended for the Hong Kong Government to have a renewed focus on implementing Section 33. The Guidance sets out the Privacy Commissioner’s views on compliance to prepare for the eventual implementation of Section 33. However, no timeline has yet been set by the Government for implementation of the section.
12. Security Requirements

DPP 4 of the PDPO requires that all practical steps be taken by a data user to ensure that Personal Data it holds is protected against unauthorized or accidental access, processing, erasure, loss or use.

If a data user engages a Data Processor to process Personal Data on its behalf, the data user must adopt contractual or other means to prevent the unauthorized or accidental access, processing, erasure, loss or use of the transferred data.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

Specific rules apply. For further details on data processing, refer to the Commissioner’s information leaflet on Outsourcing the Processing of Personal Data to Data Processors. The Guidance on Personal Data Erasure and Anonymization contains tips on outsourcing to third parties. Industry specific guidance applying to the insurance and finance industries has been issued by the regulators of those sectors.

14. Enforcement and Sanctions

Potential civil and criminal penalties, as well as private rights of action may apply.

15. Data Security Breach

The Commissioner published a Guidance Note on the Data Breach Handling and the Giving of Data Breach Notifications (“Breach Guidance Note”) which was updated in October 2015.

The Breach Guidance Note provides data users with practical steps to be taken in the event that the security of Personal Data is subject to, or is at the risk of loss, unauthorized or accidental access, processing, erasure or use (“Data Breach”). The Breach Guidance Note confirms that Data Breach notification is voluntary; however, it suggests that data users should have a Data Breach handling policy in place as a matter of good practice.

In the event of a Data Breach, the Breach Guidance Note sets out four steps to be taken by the data user:

- immediately gather essential information relating to the breach (i.e., when, where and how the breach occurred, what was the cause of the breach and the extent of Personal Data involved);
- adopt appropriate measures to contain the breach (i.e., changing passwords, modifying access rights, and notification of law enforcement agencies);
• assess the risk of harm to the Data Subject (i.e., risk to personal safety, identify theft, financial loss, risk of humiliation, damage to reputation or loss of business or other opportunity); and

• consider issuing a Data Breach notification (particularly where the assessment has shown a risk of personal safety).

In the event of notification, the Breach Guidance Note also provides guidance on who the notification should be given to, what should be included in the notification, when to issue the notification and how to notify the Data Breach.

In the event that the Commissioner is notified, the Breach Guidance Note also provides a Data Breach Notification Form that can be used to give the Commissioner notice of a Data Breach.

16. Accountability

An organization has no legal obligation to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. However, there is a noticeable trend in non-binding guidance recently issued by the PCO to recommend conducting privacy impact assessments before collecting certain sensitive data, such as biometric data, or in circumstances where there is a possibility for excessive collection of Personal Data, such as when using drones.

17. Whistle-Blower Hotline

There are no laws/rules that govern whistle-blower hotlines in Hong Kong.

18. E-Discovery System

To the extent that the e-discovery system involves the collection, holding, processing or use of Personal Data, privacy issues may arise. The data privacy issues are not, however, confined to e-discovery and will apply in ordinary discovery as well.

19. Anti-spam filter solution

The introduction of a spam-filtering solution is permitted in Hong Kong but would be subject to the guidelines on Monitoring and Personal Data Privacy at Work. Employers should inform employees of their monitoring policy or policies.

20. Cookies

There is no specific law/rule that governs the use and deployment of cookies in Hong Kong.
21. Direct Marketing

Information and Consent Requirements

If a data user intends to use, or provide to a third party (i.e., transfer), Personal Data for direct marketing purposes, the data user must notify the Data Subject of the following and obtain his/her consent before using the data:

- that the data user intends to use or transfer the data for direct marketing purposes;
- that the Data Subject’s consent is required before the data user does so;
- the kind of Personal Data to be used or transferred (e.g., name and email address);
- the classes of marketing subjects to which the direct marketing will relate (e.g., specific categories such as travel and telecommunications);
- in the case of transfer, of the classes of persons to whom the data will be provided (e.g., specific categories such as financial services institutions, telecommunications providers); and
- in the case of transfer and if the data is to be provided “for gain”, that the data is to be so provided (“for gain” is defined in the PDPO as the provision of Personal Data in return “for money or other property”, e.g., commissions and fees).

For use of data for direct marketing, this information may be provided orally or in writing, and the Data Subject’s consent may be written or oral (although if consent is given orally, the data user must send a written confirmation to the Data Subject within 14 days). For transfer of data, this information must be provided in writing and written consent must be obtained.

The duty to inform the Data Subject of the above information is “absolute” and irrespective of whether the Personal Data is collected from Data Subjects directly or from other sources (e.g., from public registers or third parties).

It is important to note also that if the Personal Data is transferred to a third party for that third party to carry out direct marketing on behalf of the data user, then consent to the transfer is not required.

Transitional Provisions

The new requirements to notify the Data Subject and obtain consent to use of data do not apply if the data user satisfied the following transitional requirements prior to 1 April 2013:

- it had explicitly informed a Data Subject that it intended to use the Data Subject’s data for direct marketing for a class of marketing subjects (e.g.,
specific categories such as travel and telecommunications – a generic
description is not sufficient);

• it had been using the Personal Data for that purpose;
• it had not been requested by the Data Subject to cease using the data for
that purpose; and
• it had not otherwise contravened the PDPO in relation to that use.

The transitional provisions apply only to use of data, not to provision of data to
a third party, for direct marketing purposes. Therefore, from 1 April 2013
consent will be required for providing (i.e., transferring) Personal Data to third
parties for direct marketing.

First Use of Data

A data user is required, when using Personal Data for direct marketing
purposes for the first time, to notify the Data Subject that the data user is
obliged to cease using their Personal Data on request and provide a means
for the Data Subject to object. If the Data Subject, at any time after collection
of their Personal Data, requests that a data user stop using or transferring its
Personal Data for marketing purposes, then the data user must cease such
activities. The maximum penalty for violations of this requirement has been
increased from HKD 10,000 (approximately USD 1,290) to HKD 500,000
(approximately USD 64,000) and up to three years’ imprisonment.

Penalties

Non-compliance with any of the information or consent requirements, using
Personal Data without consent, or failing to cease use after an objection has
been received, all carry penalties. The penalties for offenses with respect to
use of Personal Data for direct marketing is punishable by a fine of up to HKD
500,000 (approximately USD 64,000) and three years’ imprisonment. The
penalties for offenses with respect to provision of Personal Data for direct
marketing are also punishable by a fine of up to HKD 500,000 (approximately
USD 64,000) and three years’ imprisonment, however if the transfer is for gain
(i.e., payment), the maximum fine is HKD 1 million (approximately USD
129,000) and five years’ imprisonment. It is a defense for the data user to
show that it took all reasonable precautions and exercised all due diligence to
avoid commission of the offense.

Guidance on Direct Marketing

On 15 January 2013, the Commissioner published the New Guidance on
Direct Marketing (“New Guidance”), which provides some practical guidance
on compliance with the new direct marketing regime.
Consent

Under the PDPO, “consent” is defined to include “an indication of no objection”. The New Guidance provides that there must be “explicit” action taken on the part of the Data Subject to qualify as “an indication of no objection”. In other words, silence will not constitute consent. For example, consent can be in the form of an opt-in (e.g., by asking a customer to check a tick box when signing a form) or an opt-out (e.g., by providing a customer with the opportunity to opt-out of receiving marketing and confirming that he/she agrees to the use of data in direct marketing). An opt-out is only valid where an active step is taken by the Data Subject to submit their data such as signing a form or clicking “I accept”.

The “opt-out later” or “deemed consent” approach that was acceptable in the past is no longer sufficient. For example, where a company informs a customer in writing of the use or provision of Personal Data for direct marketing and states that “any objection has to be made by sending back the objection slip”, such a non-response from the Data Subject would not amount to valid consent.

The New Guidance also provides that “bundled consent” should be avoided. “Bundled consent” is where direct marketing consent language is inseparable from other provisions in an application form or contract terms and there is no option for the customer to object to the direct marketing use and still obtain the other services applied for. Data users should not design application forms and contracts in a way which makes it impracticable for a customer to refuse the use of their Personal Data for direct marketing purposes (for example, by providing only one space to sign on an application form for a product/service).

Classes of Marketing Subjects

The examples provided in the New Guidance suggest that the description must be very specific. Companies should make reference to the distinctive features of the goods, facilities or services so that customers may ascertain the types of goods, facilities or services about which they may receive direct marketing with a “reasonable degree of certainty”. For example, “telecommunications network services offered by ABC Company” would be acceptable, but “retail services and products provided by ABC Company” would not be acceptable as it is too broad for customers to comprehend the actual classes of goods, facilities or services. The information must be provided in an easily readable and easily understandable manner.

Individuals in a Business Capacity

The New Guidance draws a distinction between marketing targeted at individuals or their employing corporations. This is significant as it goes beyond the strict interpretation of the Amendments. Where Personal Data is collected from individuals in their “official capacity” (for example, as in-house
legal counsel) and the product or service is clearly meant for the exclusive use of the corporation by whom the individual is employed, the Commissioner takes the view that the requirements of the new direct marketing regime will not apply. However, if that same individual is sent details of products or services targeted to them as an individual, the direct marketing requirements will apply.

Transfer to Affiliates

The New Guidance clarifies that it is a misconception that a data user may freely transfer Personal Data to its parent company and subsidiaries/associated companies for direct marketing purposes. Now that the new direct marketing regime is in effect, a data user is required to obtain written consent from a Data Subject prior to providing Personal Data to any other person or entity for the purposes of direct marketing, including affiliates. There are no transitional provisions applicable to transfers of data for a third party’s direct marketing purposes.
Hungary

Ines K. Radmilovic
Budapest
Tel: +36 1 302 3330
ines.radmilovic@bakermckenzie.com

Adam Liber
Budapest
Tel: +36 1 302 3330
adam.liber@bakermckenzie.com

Mate Kovacs
Budapest
Tel: +36 1 302 3330
mate.kovacs@bakermckenzie.com
1. Recent Privacy Developments

Changes in legislation

(a) The status and scope of local legislation supplementing GDPR:

On 29 August 2017, the Hungarian Ministry of Justice published the draft Hungarian GDPR Implementation Act for public consultation purposes. The draft legislation seems to adopt a minimalist approach, restricting the scope of material changes to the bare minimum necessary to comply with the requirements of the GDPR. The main provisions of the draft legislation can be summarized as follows:

- it extends the provisions of the GDPR on manual processing to non-manual systems even if the Personal Data is not contained or intended to be contained in a filing system;
- it contains no special provisions concerning data processing in the employment context;
- it maintains the currently applicable rules regarding the processing of health data, including the obligation to obtain written consent for such processing;
- it grants to the deceased person’s close relatives the exercise of the right to erasure and to obtain restriction on processing, upon a request made within five years following the death;
- it requires the Data Controller to review its data processing activities every three years if the law does not establish any time limits for retaining the data. In that case, the review must be documented and presented to the Hungarian DPA upon its request;
- extends the penalty provisions to SMEs by removing the exemption which small and medium-sized undertakings had to date, under which they could receive only a warning (rather than a fine) for their first non-compliance with the law;
- it no longer requires local filing and/or approval requirements concerning data processed under the GDPR. However, the draft provides that the Hungarian register will be archived and that the DPA may use the previous filing’s details in connection with investigations concerning data processing started before 25 May 2018.

The relevant bill will be submitted to the Hungarian Parliament by October 2017 and is expected to be adopted by the end of 2017.
(b) Local regulator guidance and activities:

**Significant guidance issued by Hungarian DPA**

**Hungarian DPA guidance concerning basic requirements of data processing in the employment context**

This guidance summarizes the Hungarian Data Protection and Freedom of Information Authority’s (“Hungarian DPA”) current practice concerning the processing of employee data. It covers job applications, fitness checks, whistleblowing, employee monitoring, use of biometric entry systems and investigations.

The Hungarian DPA guidance articulates the following requirements in connection with data processing in the employment context.

**General employee data processing requirements**

The guidance says that *the purpose limitation* and the *necessity of data processing* are essential requirements for the processing of employee data. Data processed in the employment context must provide substantive information and be necessary for the establishment, maintenance and termination of the employment relationship. The processing purposes must be clearly specified and disclosed to the Data Subject employees. The fairness of data processing requires the employer to observe the personal – including privacy – rights of the employees.

The guidance confirms that employers may not rely on consent as a legal basis for the processing of employee data – unless the employee has a genuine free choice and is subsequently able to withdraw the consent without detriment. The Hungarian DPA holds the view that this is only rarely the case in the employment context, due to the subordinate relationship between the employer and the employee. The employer must therefore rely on other legal bases to process employee data in the employment context, such as a statutory legal basis or the legitimate interest test based on Article 7 (f) of the European Data Protection Directive. If relying on the latter, the employer must define its legitimate interest(s) being pursued, conduct the test, document it, and then disclose the result of the test to the employees. The employer must develop its internal by-laws regarding the details of data processing activities based on its legitimate interests and provide proof that the data processing complies with the law. In the context of investigations, the guidance says that the principle of proportionality and the presence of the employee when inspecting his/her emails or records might be important safeguards of the Data Subject employees’ interests.

In relation to *data transfers*, the guidance confirms that affiliate companies in the same corporate group are “third persons”. Resultantly, providing them access to employee data is considered a “data transfer”. Also, generally, the
owner of the employer may not have access to employee data processed by the employer, unless such access is duly legitimised. If the employer cannot legitimise such data transfers by explicit consent – because its voluntary nature may be questioned – then the employer must ensure the adequacy of employee data transfers abroad. The guidance says that Privacy Shield is a valid data transfer mechanism to ensure the adequacy of data transfers to the United States.

The employer must provide a privacy notice to its employees about the processing of their data, including the monitoring measures applied. The guidance refers back to the recommendation of the Hungarian DPA released on 9 October 2015, which details the Data Subject notice requirements. In relation to each processing purpose, the employer must provide information about the persons having access to the employee data.

The guidance says that employee data processing is exempt from registration with the Hungarian DPA if done in the context of any contractual relationship relating to employment, where such data processing is based on statutory provisions. However, the Hungarian DPA has now changed its previous practice relating to job applicants, saying that job applicants’ data processing must be registered with the Hungarian DPA, unless the data is obtained directly from the Data Subject, is used only for the purpose of the job application and is not disclosed to “third persons”.

The guidance makes it clear that, based on the Hungarian DPA’s interpretation of applicable law requirements, Hungarian laws will apply to the data processing activities of subsidiaries located in other EEA countries and in third countries, if the processed data relates to a Hungarian employment relationship. The Hungarian DPA bases its position on Article 4 (1)(a) of the EU Privacy Directive and the Costeja decision of the EU Court of Justice in Case C 131/12, extending the scope of the Directive’s application. The Hungarian DPA will deem the data use to occur in Hungary and that local Data Subjects are affected, such that Hungarian law applies to the processing activities of foreign subsidiaries. This includes also the use of whistleblowing schemes whose operation is extended to Hungary. The Hungarian DPA will not accept the argumentation that such data processing takes place in a third country (e.g., by the head of the corporate group) if data processing occurs in the context of employment in Hungary.

**Specific Employee Data Processing Requirements**

The guidance also covers several specific data processing activities typically occurring at the workplace. Those are summarized below.

*Job applications, fitness and background checks*

The guidance states that “anonymous” job advertisements, which do not disclose the employer’s identity, are illegal because the applicant has no
information about the identity of the Data Controller. In its practice, the Hungarian DPA takes the view that the Data Subject rights of job applicants always prevail over the employer’s interest in remaining anonymous.

Job applications may be stored only until the end of the particular application process and related records (including the application or notes taken by the employer) must be deleted, unless the applicant subsequently consents to the retention of that data for a lawful purpose (such as future job openings). The employer must inform the applicant about the outcome of the job application process.

The guidance also confirms that the employer has the right to check public records of social networking sites for information about job applicants. However, the employer may not save or store the applicant’s social networking profile, check any information disclosed in closed groups on such sites or ask third persons to do so. The employer must provide prior notice to the candidate that it will check his/her public activities on social networking sites. Information which the employer derives from such sites may be checked or used only if it is relevant in the context of the employment decision.

The employer must transparently inform employees about the purpose of fitness checks, as well as about the scope of Personal Data processed. If the check is conducted by a third person (e.g., a medical practitioner), then the employer may not access the fitness check record, but may only be told the third party’s conclusion as to whether the employee is fit or unfit for a particular job position. The Hungarian DPA considers that the results of psychometric and personality tests may be provided only in an anonymized format unless the Data Subject provides the employer directly with the test results.

Relative to criminal background checks, the employer must rely on and accept the criminal record certificate (“Hatósági Erkölcsi Bizonyítvány” in Hungarian) provided by the candidate. (Said certificate does not indicate convictions or past convictions subject to a criminal record exemption.) The employer may not obtain data directly from the criminal register or request the candidate to present a copy of his/her full criminal register records to the employer.

**Employee Monitoring**

In the context of CCTV surveillance, the guidance confirms that covert monitoring is illegal; use of CCTV must be clearly announced. The employer may not monitor public areas via CCTV. CCTV records generally may be stored for three working days or that period specified by Act CXXXIII of 2005 on Security Services. The employer may keep the CCTV records beyond that period only if it can justify doing so based on the legitimate interest test. The employer must implement detailed by-laws concerning CCTV monitoring and disclose those to the employees.
Monitoring of email must be legitimized by the legitimate interests and the conditions of email checks must be regulated by the employer in detail. In order to secure the legitimate interest and rights of employees, each relevant employee must be informed about and be present when the email check is conducted. The employer may not check the contents of employees' private emails.

If the employer permits the private use of an employer owned laptop, it must provide a separate hard disk partition, because the employer is not authorized to check or image employees’ private files. The employer must secure that private files are excluded from imaging and checks. The employer must implement by-laws stating the details and purposes of checks based on the result of the legitimate interest test.

The monitoring of internet use is permitted on the basis of the result of the legitimate interest test. The monitoring measures should record only the visited website addresses, without recording the activities of the employee on that site. The detailed conditions of internet use monitoring must be specified in the employer's internal by-laws.

Biometric systems

The guidance says that the use of biometric entry systems can be justified only in exceptional cases. Generally, biometric time-recording systems may not be used because less restrictive means/alternatives are available for employee data processing.

Whistleblowing

The Hungarian DPA confirms that adopting a code of conduct is not a precondition to implementing a whistleblowing scheme in Hungary. The notice about the operation of the whistleblowing scheme must be published in the Hungarian language. However, such publication via an intranet site does not comply with the employee notice requirement. Data processing through the operation of whistleblowing schemes must be registered with the Hungarian DPA.

The guidance mentions that the entry into force of the General Data Protection Regulation will not cause any substantive changes in the requirements articulated by the Hungarian DPA. The Hungarian DPA did not set any specific deadline for compliance with the requirements articulated by the notice. Employers can expect that the Hungarian DPA will examine their compliance with data protection requirements. Hungarian employers are therefore strongly advised to review their current privacy practices and check their internal regulations and by-laws for compliance.
Hungarian DPA guidance on website and online shop operations

The guidance explains the basic requirements regarding the use of cookies, as well as applicable notice and user consent requirements.

Under the guidance, before implementing cookies or similar technologies placing information on the users’ end device, the website operator must:

- map the cookies that it wishes to use on its site and
- determine whether notice or consent is required for the use of each.

The guidance confirms that the website operator is liable for the use of third-party cookies which transmit information – such as user behavior data – to third parties. Accordingly, the website operator must have the user’s consent to allow the use of cookies collecting and transmitting user information to third parties. The guidance says that special attention must be given to the use of social plug-in modules monitoring user behavior or tracking other user activities. The website operator must be aware of the scope of the data collected by third-party cookies, including the data categories collected and the relevant processing purposes, such as analytics, advertising or market research. The operator also must be transparent about data collection practices relative to use of its website.

Cookies Notice

The website operator must provide a transparent notice to users regarding the use of cookies. The notice must cover all cookies used, regardless of whether consent is required their use.

Said notice must indicate:

- the name of each relevant cookie, enabling identification of the website operator’s and each third party’s cookies;
- the data types for each relevant cookie and their expiry date; and
- the explanation in plain language of the function of each cookies.

The DPA recommends that website operators should provide general information about cookies and practical information about how the user may find and control cookie settings in his/her browser.

The website operator must provide a cookie notice to users when they first visit the site. Said notice must be repeated if there is a change in the notice. A multilayered notice – i.e., a condensed notice in a pop-up window with a link providing access to the full cookie information – is generally acceptable.

The guidance says that the website operator must implement a mechanism for the deactivation of the notice (pop-up/layer) with active user behavior
acknowledging the receipt of the information. This requirement also applies to cookies covered by the cookie consent exemption. The operator must provide easy access to the relevant cookie notice also following the deactivation of the pop-up or layer. If the use of the cookie requires consent and said requirement relates to a particular functionality, then the operator may provide the relevant cookie notice when the user uses said functionality. Also, the website operator must provide to users information enabling them to make an informed choice regarding the use of cookies and transmission of data to third persons.

Consent to Use of Cookies

The guidance says that the use of user-input cookies, authentication cookies, user centric security cookies, multimedia player session cookies, load balancing session cookies and user interface customization cookies does not require any consent.

However, if the cookie consent exemption does not apply – such as in connection with the use of third-party cookies or tracking cookies – then the website operator must secure the user’s voluntary consent to the use of such cookies and must obtain separate consent relative to the use of each relevant cookie for the use of which consent is required. In such cases, the Hungarian DPA will not accept the website operator’s bundling of consent, covering several cookies at the same time, because the Hungarian DPA considers that consent bundling does not enable voluntary consent. Instead, the Hungarian DPA suggests that the website operator should implement a consent mechanism providing separate checkboxes for each relevant cookie. The Hungarian DPA guidance also underlines that the operator must obtain prior consent before placing each relevant cookie on the user's end device. This means that the user may not have access to the relevant functionality before he/she has granted consent to the cookie used on that functionality.

The guidance says that the website operator must use inactive social media plug-ins and implement steps that restrict data transfers to social networks, unless the user explicitly consents to the transmission of the information to the social network, e.g., by sharing an article on a social media plug-in. This means that the user must activate the relevant plug-in after having received from the operator a notice about the scope of data collections and transfers, including whether behavioral information is collected and transmitted to third persons.

2. Emerging Privacy Issues and Trends

Practice of the Hungarian DPA

The Hungarian DPA continues to interpret the Information Act in a generally conservative manner, although the Hungarian DPA is becoming slowly, but gradually business friendly, and consequently, showing a willingness to
accept reasonable business arguments raised by Data Controllers. The Hungarian DPA emphasizes enforcement of the restrictive Information Act as prescribed by the Data Protection Directive and as interpreted by the Article 29 Data Protection Working Party.

The Hungarian DPA is entitled to impose sanctions for the violation of the Hungarian data protection rules. In the past years, the Hungarian DPA examined the lawfulness of data processing in connection with, among others, manpower-leasing (i.e., temporary agencies), online dating services, real estate agency services, organization of promotions, and claims enforcement. In 2015, the Hungarian DPA focused on claims enforcements and debt-recovery services, the organization of product presentation events and on online direct marketing services.

In 2016, the Hungarian DPA primarily reviewed privacy notices and enforced information provisions. For the 2017 calendar year, the Hungarian DPA has not disclose its enforcement priorities. The DPA published guidance and communications to Data Controllers and Processors to commence GDPR compliance preparatory actions.

Most of the resolutions adopted by the Hungarian DPA have been published on its website.

The Hungarian DPA initiated 14 administrative proceedings and imposed fines of HUF 20.1 million in 2016.

3. Law Applicable


• Act No. I of 2012 on the Labor Code (“Labor Code”), which applies to employee related data processing

• Act C of 2003 on Electronic Communications (“Electronic Communications Act”)

• Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators

• Act CVIII of 2001 on Electronic Commerce and on Information Society Services (“E-Commerce Act”)

• Act No. C of 2012 on the Criminal Code (“Criminal Code”)

• Act No. CXIX of 1995 on the Handling of Names and Addresses for the Purposes of Scientific Research and Direct Marketing
• Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities
• Act No. XLVII of 1997 on the Protection of Personal Data Regarding Healthcare and Related Issues (“Healthcare Data Protection Act”)
• Act No. CCXXII of 2015 on the General Rules on Electronic Administration and Trust Services
• Act No. CLXV of 2013 on Complaints and Public Interest Disclosure (“Whistleblowing Act”)

Further, sector-specific legislation, such as banking laws, social security laws, tax laws, etc., contain additional data protection rules, particularly relating to the legality of data processing and the data retention obligation of Data Controllers.

Although the recommendations of the previous Data Commissioners and those of the new Hungarian DPA do not qualify as law, they are generally followed in practice. Further, the Hungarian DPA tends to consider and follow the recommendations of the Article 29 Data Protection Working Party, established under the Data Protection Directive.

4. Key Privacy Concepts

a. Personal Data
The Information Act applies to the processing of any information relating to or otherwise connected to an identified or identifiable natural person (“Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity. Any conclusion concerning the natural person that can be drawn from the processed information also qualifies as protected Personal Data (“Personal Data”). In the course of data processing, such information is treated as Personal Data as long as the Data Subject remains identifiable. Thus, the term Personal Data is widely defined.

b. Data Processing
The Information Act defines data processing similar to the way it has been defined under the Data Protection Directive. However, the Information Act uses the term “data controlling” for that activity. The term “data processing” means limited, rather technical data processing activities performed by Data Processors, as described below. For the purpose of this summary, we use the term “Data Processing” within the meaning of the Data Protection Directive.

“Data Processing” is widely defined and includes collecting, recording and storing, processing, utilizing (including transferring and publishing), altering, and preventing further use of the Personal Data. Photographing, sound and
video recording and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples, and retinal images) would also qualify as processing. The Information Act applies to manual, partially automated and automated Data Processing.

c. Processing by Data Controllers
The Information Act applies to those persons, including any natural or legal person or organization which alone or jointly with others determines the purpose for which and the manner (including the means used) in which any Personal Data is or will be processed and who executes the Data Processing, or who appoints someone to process Personal Data (“Data Controller”). A Data Controller is responsible for the Data Processing, including for the activities of its Data Processors. When deciding whether a person qualifies as a Data Controller or a Data Processor, the Hungarian DPA tends to classify a person who has even a minor decision-making right in respect of Data Processing as a Data Controller and not as a Data Processor.

The Information Act also applies to “Data Processors”. According to the Information Act, a Data Processor performs technical data processing activities at the instruction of the Data Controller. Processing by a Data Processor is defined by the Information Act as the performance of technical tasks related to Data Processing operations, regardless of the methods or means used or of the place of the location of the application. Data Processors are not entitled to make decisions on the merits of data processing (e.g., may not decide to transfer Personal Data to a third party, unless instructed by the Data Controller). The Data Processor may subcontract its data processing activities and employ further Data Processors with the consent of the Data Controller. The Information Act prohibits the employment of Data Processors having business interest in any business activity for which Personal Data is or will be used by the Data Controller.

d. Jurisdiction/Territoriality
The Information Act applies to the processing of Personal Data (including automatic or manual data processing) on the territory of Hungary, unless the Data Processing is carried out solely for the Data Subject’s own (household) purposes (such that said Act does not apply to the private data processing activities of individuals). Furthermore, the provisions of the Information Act are applicable if a foreign Data Controller (processing Personal Data outside the EU) employs a Data Processor whose registered address or place of business (branch) or habitual residence is situated in Hungary or if it makes use of equipment situated in Hungary, unless such equipment is used solely for the purpose of data traffic exclusively within the territory of the European Union. In such a case, the Data Controller must appoint a representative in Hungary. If Personal Data is transferred outside Hungary, the general rule is that the Information Act applies to data transfer.
The territorial scope of the E-Commerce Act, which also contains some data protection rules, is broader than the territorial scope of the Information Act. This legislation may be relevant when a service provider situated outside the European Union directs e-commerce and/or information society services to Hungary.

e. **Sensitive Personal Data**
The Information Act imposes additional requirements relating to the processing of “Sensitive Personal Data”, that is, Personal Data relating to racial, national, or ethnic origin, political opinions or political party membership, religious or other convictions, membership in a society, association or trade union, health condition, abnormal addiction, sexual orientation, and criminal records.

Sensitive Personal Data may be processed only if:

- the Data Subject gives his/her written consent to the Data Processing;
- the Data Processing is required under an international convention or by an Act of Parliament for the purpose of enforcing a fundamental constitutional right, or for national security purposes, crime prevention, or criminal investigation;
- the Data Processing is otherwise required by an Act of Parliament in the interest of the general public – e.g., it is performed by a health care professional for such purposes which are defined by law; or
- the Data Processing is otherwise authorized based on Section 6 of the Data Processing Act.

f. **Employee Personal Data**
The Labor Code contains only a few general rules on employment related Data Processing. In the absence of specific rules, in case of employment related Data Processing, in addition to the Labor Code, the Information Act must also be applied.¹

Under the Labor Code, an employee (or job applicant) may be requested to make a statement or to disclose information only if it does not violate his/her personal rights and which is deemed necessary for the conclusion, maintenance or termination of the employment relationship. The opportunity to

---

¹ For example, the new Labor Code provides an opportunity to check/control employee’s work during working time. However, the Labor Code contains only some general rules and does not provide a detailed description on how and to what extent employers may exercise their control rights. As exercising the control rights affects the data protection rights of the employees and in certain cases, also the rights of third parties, the Information Act has to be considered as well and applied together with the Labor Code.
require an employee (or job applicant) to take an aptitude test, provide background information or to perform a detailed background check is limited.

An employer has a general obligation to inform its employees concerning the processing of their Personal Data. Although an employer may monitor employees in connection with the performance of their obligations, the employer must notify its employees concerning the means and methods the employer uses for this purpose. The private life of employees may not be monitored or violated in any manner.

The data protection and personal rights of employees may be restricted if deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. The means and conditions for any restriction of personal rights and their expected duration must be communicated to the employees in advance.

Data Processing by the employer may be conducted if it is (i) authorized or (ii) required by law. The statutory authorization to process Personal Data of an employee (including Sensitive Personal Data), however, covers only the minimum Data Processing activities which are strictly required to perform the employment relationship and to comply with statutory obligations.

Also, the Hungarian DPA – based on its published guidelines – is of the view that the consent of the employees may serve as legal grounds for Data Processing only in cases where the voluntary nature of the employee’s consent may clearly be ensured. However, the Hungarian DPA’s position is that such cases will be rare, due to the subordinated position of the employee vis-à-vis the employer. In line with this, the Hungarian DPA has also stated that an employer should rely on a statutory legal basis, such as its prevailing legitimate interest to process employee data, as the legal ground for the Data Processing. In that regard, the employer must perform and document the balance of interests test, and has the burden of proving that enforcement of that legitimate interest is proportionate to any resulting limitation of the employee’s privacy rights.

As the Labor Code contains only a few rules on this issue, employers must prepare a privacy policy in which the most important rules, such as those on the usage of company equipment, the controlling rights of the employer, etc., are stated. The employer, by the adoption and distribution of an adequate privacy policy, can simultaneously ensure compliance with its statutory information obligation and ensure that it is entitled to exercise its monitoring rights as described in the policy.
5. Consent

a. General

Consent of the Data Subject is one of the legal grounds for processing Personal Data in Hungary based on the informational self-determination right of the Data Subject.

The Information Act provides for exemptions to the consent requirement in cases where the processing of Personal Data is necessary for the purposes of the legitimate interest pursued by the Data Controller or by a third party and enforcing those interests is considered proportionate to the limitation of the right to the protection of Personal Data or where processing is for compliance with a legal obligation. Consent by the Data Subject must always be voluntary, informed (i.e., based on accurate and detailed information), explicit and unambiguous. To be unambiguous, the consent must be a clear indication of the Data Subject’s agreement to the processing of Personal Data relating to him, without limitation or with reference to specific operations, though consent is not required in certain prescribed circumstances.

Consent may be express or implied; the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to cover only the identified purpose(s). A new consent is required for purposes which were not previously identified and consented to.

There is no requirement that consent must be in writing (unless sensitive data is processed). It may be provided orally or in other forms/formats. In addition, the Data Subject also has the right to withdraw consent at any time in given circumstances.

b. Sensitive Data

Where consent is relied upon to justify the processing of Sensitive Personal Data, it must have been obtained in writing prior to the processing.

c. Minors

Under general Hungarian law rules, a person under the age of 18 is usually considered a minor, who may make valid legal declarations (e.g., conclude contracts) if the minor’s legal representative (i.e., parent, guardian, etc.) consents to those declarations. Minors between the ages of 14 to 18 have limited legal capacity to conclude certain contracts. The Information Act contains a special rule applicable to minors over 16. Under that rule, the consent of such a minor is valid without the consent or subsequent approval of the minor’s legal representative.
d. **Employee Consent**

The Labor Code states that the employer may disclose Personal Data to a third party only in the cases specified by an Act of Parliament or with the employee’s consent. In that context, a related company of the employer or another member of the group of companies which the employer is a member of also qualifies as a third party. The Labor Code does not require that consent be given in written form, but in its practice the Hungarian DPA strongly recommends obtaining the employee’s wet signature on the consent.

However, in its guidance, the Authority stated that the employee’s consent may serve as the legal grounds for Data Processing only in cases where the voluntary nature of the employee’s consent may clearly be ensured. This guidance indicates that employers should rely on other legal grounds when processing their employees’ Personal Data, e.g., statutory authorization and/or the legitimate interests pursued by the employer as Data Controller, provided that enforcing these interests is considered proportionate to the limitation of the employee’s right to protection of Personal Data.

e. **Online/Electronic Consent**

In cases where the Information Act requires written consent, the consent may be given in an electronic document signed by an advanced electronic signature (in this case, an electronic consent qualifies as a written consent). Electronic signatures, however, are not widely applied in Hungary. According to the practice of the Hungarian DPA, pre-checked boxes may not be used to signify the affirmative consent of the Data Subject. Also, the Hungarian DPA’s practice is to require obtaining separate consent for each individual data processing operation because bundled consent is not considered to have been voluntarily provided. In the context of consent for Personal Data disclosure for direct marketing purposes, the Hungarian DPA takes the position that the Data Subject must have the right to choose among the particular Data Controllers to whom data may be transferred for marketing purposes.

6. **Notice Requirements**

An organization that collects Personal Data must provide clear and detailed information to Data Subjects about all relevant aspects of data processing, including: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the legal bases and purposes for collecting Personal Data; (iv) the organization’s privacy practices (which must be given in a clear and transparent way); (v) the identity of the third parties to which the organization will disclose the Personal Data; (vi) the rights of and the legal remedies available to the Data Subject; (vii) how the Personal Data is to be retained; (viii) where the Personal Data is to be transferred; (ix) where the Personal Data is to be stored; and (x) how to contact the privacy officer or other person who is accountable for the organization’s policies and practices. The Data
Controller must inform the Data Subject if the Data Controller relies on the legitimate interest test as a legal basis of data processing. If the provision to the Data Subject of such notice proves impossible or would involve disproportionate costs to the Data Controller, the notice may be published in a way which makes it publicly accessible to the Data Subjects. On 9 October 2015, the Hungarian DPA issued a detailed recommendation on Data Subject notice requirements, providing guidance to Data Controllers on the scope of information to be provided to the Data Subjects.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion, blocking and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

The general rule is that every data processing activity must be notified to the Hungarian DPA and the Data Processing may not be commenced before the earlier of the receipt of the Hungarian DPA’s confirmation of said notification or the ninth day following the submission of such notification, provided that the notification contains all the relevant information required by law. There are several, strictly interpreted exemptions, however, which include Data Processing for the purposes of maintaining (i) an employment, (ii) a customer (but excluding electronic communications service providers, financial organizations (such as banks or insurance companies) and public utility companies) or (iii) a supplier relationship.

10. Data Protection Officers

The appointment of a data protection officer is required by law in the case of financial organizations, public utility companies, telecom companies, and health care institutions.
11. International Data Transfers

Notwithstanding the medium or the manner of the data transfer, Personal Data (including Sensitive Personal Data) may be transferred outside Hungary to non-EU countries only if:

- the Data Subject gives his/her explicit consent;
- the Data Transfer is necessary in order to protect the vital interests of the Data Subject or a third person and consent could not have been obtained; or
- the Information Act provides a legal basis for the data processing and an adequate level of protection is ensured in connection with the international data transfer.

An adequate level of protection is achieved:

- if the European Commission, in its decision, determines that the third country in question ensures an adequate level of protection (such as the Privacy Shield mechanism);
- if the transfer is prescribed by a bilateral treaty containing guarantees for the rights of Data Subjects, their rights to remedies, and for the independent control of processing;
- even if neither of the above is complied with, to enforce the provisions of an international legal aid treaty (such as MLATs) or of a treaty on the avoidance of double taxation, under the terms of those treaties;
- an adequate level of data protection may be ensured by the use of EU model clause agreements; or
- since 1 October 2015, through the use of binding corporate rules (“BCRs”) which have received the national authorization of the Hungarian DPA.

The Information Act does not allow the transfer of Personal Data to third countries where adequate protection is ensured through ad hoc contractual clauses. In practice, Data Controllers rely on adequacy decisions, use the relevant EU model clauses issued by the European Commission for international data transfers or rely on BCRs once authorized by the Hungarian DPA.

If there are no laws authorizing the transfer, the consent of the Data Subject will be required. Transfer of data to EEA Member States is treated as a transfer within Hungary if Personal Data is transferred in order to process it.
12. Security Requirements
Organizations must take steps to: (i) ensure that Personal Data in its possession and control is protected from unauthorized access and use; (ii) implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved. The Information Act requires additional security measures to be introduced in relation to the automatic data processing activities. This must cover measures securing:

- the prevention of unauthorized input of data;
- the restriction of use of data transfer devices by unauthorized persons;
- the control and recording of data transfers to organizations that are or may be made by data transfer devices;
- the monitoring and supervision of the input of Personal Data into automated data processing systems by recording the identity of the person who made such input and the time when such input was made;
- the recovery of the systems in case of any malfunction; and
- the maintenance of a log file and a report of malfunctions or failures.

13. Special Rules for Outsourcing of Data Processing to Third Parties
In 2013, the Hungarian DPA examined international data transfer requirements and indicated that if data is transferred to a third country based on the Data Subject’s explicit consent, the Data Subject must clearly state that he/she has understood the possible risks arising from the data transfer and agrees to such transfer of his/her Personal Data. Accordingly, prior to obtaining his/her consent to such data transfer, the Data Controller must inform the Data Subject that his/her Personal Data could be transferred to third countries which do not provide the necessary level of protection of Personal Data.

Regarding the transfer of employees’ Personal Data to third countries, the Hungarian DPA stated that the consent of the employees may serve as the legal grounds for data processing only if the voluntary nature of the employee’s consent may clearly be ensured. The Hungarian DPA also stated that an employer is expected not to transfer its employees’ Personal Data to countries without adequate levels of data protection.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, authority investigations/audits, authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

There is no obligation under Hungarian laws for organizations that are involved in a data breach situation to inform the Data Subjects or authorities about the breach, except for a specific regime applicable only to electronic communications services providers as regulated in the Electronic Communications Act. The organization may be required to gather information about the breach, assess the potential risk of harm to the Data Subjects, take steps to prevent future similar breaches and assist authorities with any investigation relating to the breach.

If, during a data protection audit, a security breach is discovered by the Hungarian DPA, the Data Controller could be subject to various sanctions for non-compliance with the processing rules. If the Data Subject discovers such a breach, he or she may claim damages as a result of the breach.

An organization that is involved in a data breach situation may be subject to suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions.

Data Controllers must keep a register of data breaches, including any measures introduced by the Data Controller to remedy such breaches. This new provision applies only to Data Controllers. But existing data processing agreements will need to be amended because Data Processors also will be required to register data breaches on behalf of the Data Controller. Thus, the processing agreement should contain detailed provisions regulating how the Data Processor should comply with such obligations relating to the recordal of data breaches.

16. Accountability

Subject to regulatory guidance, organizations may be obliged to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. Organizations may also be required to furnish to privacy regulators evidence relating to the effectiveness of the organization’s privacy management program.
17. Whistle-Blower Hotline

Under the Whistle-blowing Act, an employer and its owner(s) are authorized by law to establish a whistle-blowing system, should they wish to operate one, to investigate reports about violation of laws or rules of conduct issued by the employer, provided that such rules of conduct protect a public interest or a significant private interest. In order to investigate whistle-blowing reports, the employer may process and transfer to third parties participating in the investigation the Personal Data indicated in the report of the reporter and of the person(s) to whom the report refers. Reporting persons may include employees, contractors or any third person having a legitimate interest in making the report or in remedying the reported situation.

The Whistle-blowing Act requires that the data processing related to the whistle-blowing system must be notified to the Hungarian DPA. In addition, the employer must disclose on its corporate website the rules of conduct of the whistle-blowing system, as well as a detailed description of the reporting procedure, in Hungarian.

The Whistle-blowing Act permits data to be transferred abroad only if adequate protection of the transferred data is ensured and the foreign Data Controller and Data Processor make a contractual commitment to comply with the provisions of the Whistle-blowing Act.

18. E-Discovery

The implementation of an e-discovery system without the informed consent of the Data Subject raises serious data protection and privacy issues. Even if the Data Subject has granted consent, certain discovery measures may still be considered infringing (e.g., monitoring of private emails).

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented. Though not mandatory, employers may give employees the opportunity to opt out from the spam-filtering solution and the opportunity to review the isolated emails designated as spam.

20. Cookies

There are no specific laws/rules that regulate the deployment of cookies except for those applicable only to electronic communications service providers and laid down in the Electronic Communications Act, and hence, the use of cookies must comply with data privacy laws. In general, consent of Data Subjects must be obtained before cookies may be used. Some types of cookies that track or monitor the user may not be permitted under Hungarian law. On 17 February 2017, the Hungarian DPA released cookie guidance
relating to website and online shop operations, explaining the basic requirements regarding the use of cookies and applicable notice and user consent requirements.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject must obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond to the request for his/her consent. An organization must obtain consent for a specific marketing activity. Bundled consent is not considered valid consent.
Iceland

Áslaug Björgvinsdóttir
Reykjavík
Tel: +354 5 400 334
aslaug@logos.is

Hjördís Halldórsdóttir
Reykjavík
Tel: +354 5 400 300
hjordis@logos.is
1. Recent Privacy Developments

The Data Protection Authority ("DPA"), the institution responsible for monitoring the application of the Data Protection Act in Iceland (the "Act" or the "Data Protection Act"), registers over 1,500 complaints each year. The most notable rulings in recent years are the following:

- On 18 May 2017, the DPA issued decision No. 2016/1214. The decision concerned electronic monitoring by a furniture store and its processing of a "black list", containing information on customers that were not allowed into the store. According to the defendant this monitoring was done in order to safeguard its legitimate interests, namely to control who could enter the store and to prevent theft. The DPA concluded that the electronic monitoring outside the premises, including the monitoring and collection of car number plates did not comply with the Act. The "black list" was also deemed to be non-compliant with the Act.

- In December 2016, the DPA issued two rulings on the right to be forgotten, cases No. 2015/1015 and 2016/181. In the first ruling, No. 2015/1015, the complainant requested that news articles and a picture of him that had been published in the media, would be removed from a data base run by the National and University Library of Iceland. The DPA ruled that the publishing was in conformity with the Library’s role according to specific legislation about the Library. However, as the processing concerned media coverage, which is mainly excluded from the Act, the DPA concluded that it was for the courts to decide on the line between the freedom of speech and the right to privacy and the case was therefore dismissed. In the latter case, No. 2016/181, which was very similar, the DPA ruled that the processing by a search engine as a Data Controller infringed the Act and that the references in question were to be removed from the search engines.

- On 24 February 2016, the DPA ordered a Data Controller to pay fines in the amount of ISK 10,000 (approx. EUR 77) for each day that the Data Controller fails to comply with the instructions given by the DPA. The DPA had previously ordered the Data Controller, a photographer, to remove photos of a Data Subject from the photographer’s website, but the photographer had not acted on the instructions. This is one of the very few cases where the DPA has ordered a Data Controller to pay daily fines.

- On 25 February 2015, the DPA ruled on two cases involving a “fraud button” on the Social Insurance Administration’s webpage. In both cases, No. 2014/832 and No. 2014/1068, the DPA held that as notifications could be sent anonymously, the Data Subject’s right, e.g., to know where the information came from, could not be safeguarded. As such, all
collection and processing of such Personal Data were held to be in breach of the Data Protection Act.

- In a ruling by the DPA, dated 9 February 2015 in case No. 2014/884, a former employee complained to the DPA that his former employer had not terminated his email account and that emails from his account were being forwarded to the company’s general email address. The DPA found that this was contrary to rules No. 837/2006 on electronic surveillance, as the employer could not prove that the employee had specifically provided his consent for the transfer.

In recent years, no significant amendments have been made to the Data Protection Act. In 2014, two minor amendments were, however, introduced which state that (i) health science research is now subject to specific permission in accordance with the Act on Scientific Research in the Biomedical Field No. 44/2014 and (ii) information that falls under the scope of the Data Protection Act may be handed to a Public Archive for preservation according to the Act on Public Archives No. 77/2014.

The forthcoming changes by the EU General Data Protection Regulation (“GDPR”) will be implemented into Icelandic legislation. The implementation is however subject to full Parliamentary review before becoming effective in Iceland. The below does not reflect the rules coming in under GDPR.

2. Emerging Privacy Issues and Trends

- **Mandatory Breach Notification**: There is no mandatory requirement in the Data Protection Act to report data security breaches or losses to the DPA. However, a notice is considered as good practice, particularly if the security breach is major.

- **Direct Marketing**: Based on Article 46 of the Icelandic Electronic Communications Act No. 81/2003 (the “ECA”), the use of automated calling systems, facsimile machines or electronic mail for direct marketing is only allowed if a subscriber has given prior consent. Electronic mail addresses obtained in the context of the sale of a product or service may, however, be used for direct marketing of own goods or services if customers are given the opportunity to object to such use of addresses free of charge when they are listed and similarly each time a message is sent, if the customer has not initially refused such use. Users who use public telephone services as part of their marketing must respect designations in a telephone directory indicating that the subscriber in question does not wish to receive such calls to his/her number (“Do Not Call” Registry).

- **Cloud Computing and Social Media**: No specific legislation has been passed, however, all processing, whether in relation to cloud computing
or social media, must comply with the Data Protection Act. In relation to cloud computing, the DPA has stressed the importance of Data Controllers evaluating in each case whether the use of the cloud fulfills the requirements of the Data Protection Act, in particular concerning security measures and access to data.

- **Electronic Signatures**: The Act on Electronic Signatures No. 28/2001, which implemented Directive 1999/93/EC of the European Parliament and of the Council on a Community Framework for Electronic Signatures, stipulates that fully qualified electronic signatures shall have the same effect as handwritten signatures. Furthermore, it is stipulated that other electronic signatures can be legally binding. Icelandic legislation faithfully follows the definitions of the European Directive.

- **Binding Corporate Rules**: International companies are allowed to transfer Personal Data between operating bases, across borders, if the company has applied the so-called Binding Corporate Rules. Such rules are intended to ensure that within each company falling under their scope, all Personal Data is given adequate protection. Their binding value is based on the companies’ unilateral commitment to the rules. However, for the transfer of data across borders to be lawful under the Binding Corporate Rules, it must have been authorized by the DPA.

- **Data Protection Enforcement**: The DPA has the power to impose daily fines until it concludes that the necessary improvements have been made. If the Authority’s decision to impose daily fines is referred to the courts, then the fines will not begin to accrue until a final judgment has been rendered. The Authority can assign to the Chief of Police the task of temporarily suspending the operations of the party in question and sealing its place of operation without delay. The Director of Public Prosecutions and the National Commissioner of the Icelandic Police have the power of prosecution.

3. **Law Applicable**

The key legislation on data privacy in Iceland is the Data Protection Act. An English translation of the Act can be found on the DPA’s website, [http://www.personuvernd.is/information-in-english/greinar/nr/438](http://www.personuvernd.is/information-in-english/greinar/nr/438)

Since the Data Protection Act entered into force, the DPA has issued some public guidelines and rules. Among others are rules on how to obtain an informed consent for processing of Personal Data in scientific research in the health sector (rules No. 170/2001), rules on the obligation to notify and processing of Personal Data which requires a permit (rules No. 712/2008), rules concerning the security of Personal Data (rules No. 299/2001), rules on employers’ supervision of employee’s emails (advertisement No. 1001/2001)
and rules on the transfer of Personal Data over borders (advertisement No. 228/2010).

In future, the GDPR is intended to become applicable in Iceland. The below does not reflect the rules coming in under GDPR

4. Key Privacy Concepts

a. Personal Data

Personal Data in the Data Protection Act is defined as any data relating to a Data Subject who is identified or identifiable, i.e., information that can be traced directly or indirectly to a specific individual, deceased or living, according to Article 2. The definition in the Act is based on the standard definition of Personal Data.

b. Data Processing

Data processing is defined as any operation or set of operations, which is performed upon Personal Data, whether the processing is manual or automatic, according to Article 2 of the Act.

c. Processing by Data Controllers

Data Controllers may process Personal Data when any of the following conditions are met, according to Article 8 of the Act:

1. the Data Subject has unambiguously agreed to the processing or given his/her consent;

2. the processing is necessary to honor a contract, to which the Data Subject is a party, or to take measures at the request of the Data Subject before a contract is established;

3. the processing is necessary to fulfill a legal obligation of the Data Controller;

4. the processing is necessary to protect vital interests of the Data Subject;

5. the processing is necessary for a task that is carried out in the public interest;

6. the processing is necessary in the exercise of official authority vested in the Data Controller or in a third party to whom data is transferred; or

7. the processing is necessary for the Data Controller, or a third party, or parties to whom data is transferred, to be able to safeguard legitimate interests, except where overridden by fundamental rights and freedom of the Data Subject, which shall be protected by law.
Where Sensitive Personal Data is processed, one of the above conditions must be met as well as one of a further list of additional conditions, according to Article 9 of the Act. Those additional conditions are:

1. the Data Subject gives his/her consent to the processing;
2. the processing is specifically authorized in another act or law;
3. the Data Controller is required, by contracts between the Social Partners, to carry out the processing;
4. the processing is necessary to protect the vital interests of the Data Subject or of another party who is incapable of giving his/her consent in accordance with item 1;
5. the processing is carried out by an organization with a trade-union aim or by other non-profit organizations, such as cultural, humanitarian, social or ideological organizations, on the condition that the processing is carried out in the course of the organization’s legitimate activities and relates solely to the members of the body or to individuals who according to the organization’s goals are, or have been, in regular contact with it; it is however prohibited to disclose such Personal Data to a third party without the Data Subject’s consent;
6. the processing extends only to information that the Data Subject has personally made public;
7. the processing is necessary for a claim to be established, exercised or defended because of litigation or other such legal needs;
8. the processing is necessary because of a medical treatment or because of the routine management of health care services, provided that it is carried out by an employee of the health care services who is subject to an obligation of secrecy; or
9. the processing is necessary for the purposes of statistical or scientific research, provided that the privacy of individuals is protected by means of specific and adequate safeguards.

d. Jurisdiction/Territoriality
According to Article 6 of the Act, it applies to Data Controllers and Data Processors and the processing of Personal Data: (i) if it is conducted on behalf of a Data Controller established in Iceland, if the processing is carried out in the EEA, an EFTA country or a country or a place that the DPA lists in a notice in the Law and Ministerial Gazette; (ii) if the Data Controller, who is established in a country outside of the EEA or EFTA, makes use of equipment and facilities situated in Iceland; and (iii) about financial and credit standing data concerning legal persons using equipment in Iceland even if the Data Controller is not established in Iceland.

e. **Sensitive Personal Data**
Sensitive Personal Data is defined in Article 2 of the Act as the following data:

a. data on origin, skin color, race, political opinions, religious beliefs and other life philosophies;

b. data on whether an individual has been suspected of, indicted for, prosecuted for or convicted of a punishable offense;

c. health data, including genetic data and data on use of alcohol, medical drugs and narcotics;

d. data concerning sex life (and sexual behavior); and

e. data on trade-union membership.

There are special requirements for processing Sensitive Personal Data, as stated in Section 4 (c).

f. **Employee Personal Data**
The Act does not include a specific definition of Employee Personal Data.

5. **Consent**

a. **General**
Consent is the most common ground for processing of Personal Data. Different requirements are however made in order for consent to be a valid ground, depending on the nature of the Personal Data being processed.

According to Article 2 of the Data Protection Act, a consent is defined as a specific, unambiguous declaration, which is given freely by an individual, signifying that he/she agrees to the processing of particular Personal Data relating to him/her, and that he/she is aware of the purpose of the processing, how it will be conducted, how data protection will be ensured, that the individual can withdraw his/her consent, etc.

Silence does not amount to consent. The Data Subject must be aware of what he/she is consenting to and what consequences the processing of the information has or can have for him/her and the Data Subject must give its consent him or herself.

Consent regarding processing of general Personal Data can sometimes be based on actions of the Data Subject. A consent regarding processing of Sensitive Personal Data must however always be in the form of a declaration where the Data Subject signifies that he/she agrees to the processing in question.

There are no formalities to obtain consent to process Personal Data under the Act and the Act does not require the consent of the Data Subject to be in
writing unless the processing is for scientific research, according to Article 11 of Rule No. 170/2001 on informed consent in scientific research in the health sector.

However, as the consent must be informed, the Data Subject must be given sufficient information regarding the processing of its Personal Data and an opportunity to object to it. The burden of proof is placed on the Data Controller to show that this requirement is satisfied. Therefore, for evidential purposes, written consent is recommended in practice.

b. Sensitive Data
Sensitive Personal Data is specifically defined in the Act, as stated in Section 4 (e). Processing of Sensitive Personal Data is only allowed if one of the requirements in Article 8 is met as well as one of the requirements in Article 9 of the Act, such as the Data Subject has given his/her consent to the processing or the processing is authorized in another act of law.

c. Minors
Minors under 18 years old cannot give a valid consent. According to Article 51 of Act No. 71/1997 on legal competence, parents of a child not possessing legal competence is in charge of the child’s personal affairs. Consent must therefore be acquired from a child’s parent.

d. Employee Consent
There is no specific definition of Employee Personal Data or Employee Consent in the Act. Therefore, the rules in Article 8 and 9, referred to above, apply.

e. Online/Electronic Consent
Consent can be given online or electronically, however, the consent must fulfill the conditions stipulated in Article 2.

6. Information/Notice Requirements
When a Data Controller obtains Personal Data directly from the Data Subject, notice must be provided to the Data Subject, according to Article 20 of the Act. Notice must also be provided to a Data Subject when Personal Data is obtained from someone other than the Data Subject, according to Article 21.

When a Data Controller obtains Personal Data directly from the Data Subject, the following information must be provided to the Data Subject, according to Article 20 of the Act:

1. the name and address of the Data Controller and, where relevant, its representative in Iceland;

2. the purposes of the processing;
3. other information, in so far as such further information is necessary, having regard to the specific circumstances in which the data is processed, to enable the Data Subject to protect his or her interests, including information on:

   a. the recipients or categories of recipients of the data;
   b. whether he/she is obliged or not to provide the requested data, as well as the possible consequences of failure to reply; and
   c. the provisions of the Act regarding the Data Subject’s right of access, as well as the Data Subject’s right to rectification and deletion of wrong or misleading data.

If the Data Subject has already received this information, it does not need to be provided again.

When Personal Data is obtained from someone other than the Data Subject, the Data Controller must concurrently provide the following information to the Data Subject, according to Article 21 of the Act:

1. the name and address of the Data Controller and, where relevant, its representative in Iceland;
2. the purpose of the processing;
3. other information, in so far as such further information is necessary, having regard to the specific circumstances in which the data is processed, to enable the Data Subject to protect its interests, including information on:
   a. the types or categories of the data being processed;
   b. where the data comes from;
   c. the recipients or categories of recipients of the data; and
   d. the provisions of the Act regarding the Data Subject’s right of access, as well as the Data Subject’s right to rectification and deletion of wrong or misleading data on it.

When Personal Data is obtained from someone other than the Data Subject, a notice is not required if:

1. it is impossible to inform the Data Subject or if it would place a heavier burden upon the Data Controller than can reasonably be demanded;
2. it may be assumed that the Data Subject is already aware of the processing;
3. recording or disclosure of the data is laid down by law;
4. the Data Subject’s interests, i.e., of receiving notice of the data, are deemed secondary to vital public or private interests, including its own interests.

There is no obligation to specify the names of the entities or individuals to whom the information is being disclosed, but the categories of the recipients must be disclosed. According to DPA practice, the country of the recipients should also be disclosed if the Personal Data is to be transferred to recipients established outside of EU/EEA (or outside those countries or places which the DPA considers to provide adequate level of Personal Data protection – see Section 11).

7. Processing Rules

When processing Personal Data, all of the following shall be observed, according to Article 7 of the Act:

1. that the Personal Data is processed in a fair, apposite and lawful manner, and that its use is in accordance with good practices of Personal Data processing;

2. that the Personal Data is obtained for specified, explicit, apposite purposes and not processed further for other and incompatible purposes, but further processing of such data for historical, statistical or scientific purposes shall not be considered as incompatible, provided that proper safeguards are adhered to;

3. that the Personal Data is adequate, relevant and not excessive in relation to the purposes for the processing;

4. that the Personal Data is reliable and kept up to date when necessary, Personal Data which is unreliable or incomplete, having regard to the purposes for its processing, shall be erased or rectified; and

5. that the Personal Data is preserved in a form which does not permit identification of Data Subjects for longer than is necessary for the purposes for the processing.

8. Rights of Individuals

Data Subjects have the right to be informed of the processing of their Personal Data, and of whether the data is collected from them or from third parties according to Articles 20 and 21 of the Act – see Section 6.

The Data Subject can also require the following information from the Data Controller, according to Article 18 of the Act:

1. what data on him/her is being or has been processed;

2. the purpose of the processing;
3. who receives, has received or will receive data on him/her;
4. where the data has been obtained; and
5. what security measures are applied to the processing, provided that this will not diminish the security of the processing.

There are, however, a few exemptions from the duty to inform the Data Subject in Article 19 of the Act. These include data which is solely used for statistical processing or scientific research, provided that the processing cannot have direct influence on the Data Subject’s interest.

The Data Subject has the right to request rectification and deletion of incorrect and misleading Personal Data according to Article 25 of the Act. The Data Subject can also object, on compelling legitimate grounds relating to his or her particular situation, to the processing of Personal Data relating to him/her, save where otherwise provided by national legislation, according to Article 28 of the Act.

9. Registration/Notification Requirements

Each Data Controller who uses electronic technology to process Personal Data must notify the DPA of the processing, using a form intended for that purpose, in a timely manner before beginning the processing, according to Article 31 of the Act. There are no notification costs. Any changes that are made after the original notification shall also be notified.

According to Article 6 of the DPA’s rule No. 712/2008 on the obligation to notify and the processing of Personal Data which requires a permit, the following categories of processing of non-sensitive data are exempted from the obligation to notify:

1. processing which is contingent on a permit from the DPA;
2. processing carried out in the regular or standard course of activities, relating solely to those who have a connection to the activities or the relevant field of work, e.g., business associates, employees, members;
3. processing necessary to fulfill the legal obligations of the Data Controller;
4. processing necessary to fulfill a contract to which the Data Subject is a party, or an agreement between labor market organizations;
5. processing extending only to data that has been and is accessible to the public, provided that it is not aligned to or combined with other Personal Data which has not been made accessible; and
6. processing resulting from electronic surveillance, conducted for the purposes of security and property protection only, provided that the legal obligations regarding duty of information and warning have been fulfilled.
The aforementioned exemptions do not apply to the following categories of electronic processing of Personal Data:

- processing regarding conduct and individual evaluation, e.g., of performance of employees;
- processing for the purposes of aligning individuals to personal profiles; and
- processing involving systematic recording of telephone calls.

If the processing of general or Sensitive Personal Data is likely to present specific risks to the rights and freedoms of Data Subjects, the DPA can decide that the processing may not begin until it has been examined by the DPA and approved by the issuance of a special permit, according to Article 33 of the Act. The DPA has issued rule No. 712/2008 on the obligation to notify and the processing of Personal Data which requires a permit, in which it is stipulated when a permit is required for processing of Personal Data.

Transfer of Personal Data to countries that do not provide adequate levels of Personal Data protection is prohibited, unless certain conditions are met, according to Article 30 of the Act. The DPA can, however, authorize such transfer if it determines that special circumstances warrant it (see Section 11).

10. Data Protection Officers

There is no specific requirement under the Act to appoint data protection officers.

In the event the Data Controller does not have an establishment in Iceland, but the Act is still applicable, the Data Controller must, however, designate a representative established in Iceland, according to Article 6 of the Act. In such case the provisions of the Act relating to Data Controllers apply to the representative.

11. International Data Transfers

The transfer of Personal Data to another country that provides an adequate level of Personal Data protection is permitted, according to Article 29 of the Act. A country that complies with the EU Directive 95/46/EC is considered to provide an adequate level of protection. The same applies to those countries or places which the DPA has listed in advertisement No. 228/2010. They are EEA and EFTA Member States, Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Jersey, New Zealand, Switzerland, Uruguay, Israel, and the Isle of Man, as well as adherents to the EU-US Privacy Shield Principles.

The transfer of Personal Data to a country that does not provide an adequate level of protection is prohibited, according to Article 30 of the Act, unless:

1. the Data Subject has consented to the transfer;
2. it is necessary for the fulfilment of obligations under international law or as a result of Iceland’s membership of an international organization;

3. such a transfer is authorized in another legislative act;

4. the delivery is necessary to establish or fulfill a contract between the Data Subject and the Data Controller;

5. the transfer is necessary to establish or fulfill a contract in the interest of the Data Subject;

6. the delivery is necessary in order to protect the vital interests of the Data Subject;

7. if dissemination is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or

8. the data in question is accessible to the general public.

The DPA can authorize the transfer of data to a country that does not provide an adequate level of protection if it determines that special circumstances warrant it, even if the conditions of the provision are not met, according to paragraph 2 of the Article. In such cases the nature of the data, the planned purpose of the processing and its duration are among the factors that must be taken into account. The DPA can authorize the transfer of data to third countries even if they have not been thought of as providing the citizens with an adequate level of privacy protection. This is contingent upon the Data Controller having, in the opinion of the DPA, provided sufficient guarantees to meet these concerns. The DPA can, for example, require that the Data Controller enters into a written contract with the recipient and that the contract contains certain standard contractual clauses in conformance with a decision which the DPA has advertised in the Law and Ministerial Gazette, having considered the decisions of the Commission of the European Union.

12. Security Requirements

According to Article 11 of the Act, the Data Controller must implement appropriate technical and organizational measures to protect Personal Data against unlawful destruction, against accidental loss or alteration and against unauthorized access. Having regard to the state of the art and the cost of their implementation, such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. The Data Controller is responsible for having risk analysis and security measures which are implemented in the processing of Personal Data, and which conform with the laws, rules and instructions given by the DPA on how to ensure information security, including standards that the DPA decides must be followed. The Data Controller is responsible for risk analysis being reviewed routinely and security measures upgraded to the extent necessary to
fulfill these security requirements. The Data Controller must document how he produces a security policy, conducts a risk analysis and decides on security measures to be implemented. The DPA must be granted access to information regarding these issues at any time.

The Data Controller shall also, according to Article 12 of the Act, routinely conduct internal audits on the processing of Personal Data to ensure processing activities and security measures comply with prevailing laws and regulations. These internal audits shall be conducted routinely. The frequency and intensity of the audits shall be relative to the danger associated with the processing, the nature of the data processed, the technology used to ensure the security of the data and the cost associated with conducting the audits. They shall nonetheless be conducted at least annually.

Where data is to be processed by a Data Processor, the Data Controller must ensure that the Data Processor in question is able to carry out the required security measures and conduct internal audits, according to Article 13 of the Act.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

When processing is carried out by a Data Processor, the Data Controller must verify that the Data Processor in question is able to carry out the required security measures and conduct internal audits, according to Article 13 of the Act. The Data Controller must enter into a written agreement with the Data Processor with specific obligations, i.e.:

1. the Data Processor must act only on instructions from the Data Controller and the obligations set out in the Act will also be incumbent on processing carried out by the Data Processor;

2. anyone acting in the name of the Data Controller or the Data Processor, including the Data Processor itself, and who has access to Personal Data, may only process Personal Data according to the instructions of the Data Controller, unless legislative acts stipulate otherwise; and

3. if the Data Processor is established in another state within the European Economic Area than the Data Controller, then it must also be stipulated in the contract that the laws and regulations of the state in which the Data Processor is established will govern the security measures to be applied to the processing of Personal Data.

14. Enforcement and Sanctions

The DPA is responsible for the enforcement of the Data Protection Act, according to Article 37 of the Act.
Infringements of the provisions of the Act and of regulations issued according to it are punishable by means of fines or a prison term of up to three years, unless more severe sanctions are provided for in other acts of law, according to Article 42 of the Act. The same punishment applies if the instructions of the DPA are not observed. If an offense is committed as part of the operations of a legal person, that legal person can be fined, as provided for in Chapter II A of the General Penal Code.

If a Data Controller or a Data Processor has processed Personal Data in violation of the Act, rules or instructions by the DPA, then the Data Controller must compensate the Data Subject for the financial damage suffered as a result of this, according to Article 43 of the Act. A Data Controller will, however, not be required to compensate for any detriment which it proves can neither be traced to its or its Data Processor’s mistake or negligence.

The DPA can order the cessation of processing of Personal Data, including collection, documenting or disclosure, order the erasure of Personal Data or the deletion of records, wholly or partially, prohibit further use of data or instruct the Data Controller to implement measures that ensure the legitimacy of the processing, according to Article 40, paragraph 1 of the Act.

If a processing is discovered that violates provisions of the Act, or those administrative rules which are issued according to it, the DPA can assign to the Chief of Police the task of halting temporarily the operations of the party in question and seal its place of operation without delay, according to Article 40, paragraph 2 of the Act.

If someone does not comply with the above-mentioned instructions of the DPA, then it can revoke a permit that it has granted according to the provisions of the Data Protection Act until it concludes that the necessary improvements have been made, according to Article 40 of the Act.

15. Data Security Breach

There is no mandatory requirement in the Data Protection Act to report data security breaches or losses to the DPA or to the Data Subject.

However, a notice is considered as good practice, particularly if the security breach is major.

16. Accountability

The Data Controller shall ensure that the processing of Personal Data is always in compliance with the Act. A Data Processor can also be held liable.

17. Whistle-Blower Hotline

There are no obligations or regulations specific to whistle-blowing hotlines; however, the general data protection rules would apply with respect to the
processing of any Personal Data that results from the operation of such hotlines. The DPA has, at least in two official answers to inquiries to the DPA, referred to Opinion 1/2006 of the Article 29 Data Protection Working Party when interpreting general provisions of the Act regarding Whistle-Blower Hotlines.

18. E-Discovery
There are no special rules in Iceland regarding e-discovery.

19. Anti-Spam Filtering
There are no special rules in Iceland regarding anti-spam filtering.

20. Cookies
There are no provisions in Icelandic legislation which particularly deal with the use of cookies or location data. IP addresses are considered Personal Data as well as location data. If the use of cookies leads to the use of IP addresses, or other Personal Data, the processing of such data and location data must comply with the Act. The processing is therefore not permissible unless one of the listed conditions is met, in most instances the Data Subject must consent to the processing of such data.

21. Direct Marketing
Based on the ECA, the use of automated calling systems, including email, for direct marketing is only allowed if a subscriber has given prior consent, according to Article 46 of the ECA. If the email addresses have been obtained in the context of the sale of a product or service they may be used for direct marketing of own goods or services if customers are given the opportunity to object to such use of addresses free of charge when they are listed and similarly each time a message is sent, if the customer has not initially refused such use.

Apart from that, unsolicited electronic communications in the form of direct marketing are not allowed for subscribers who do not wish to receive these communications.

The sending of email for purposes of direct marketing, where the name and address of the party responsible for the marketing is not clearly indicated, is prohibited, according to Article 46 of the ECA.

Registers Iceland, which registers a range of information on Iceland’s residents and real properties, also maintains a registry of those individuals who object to their names being used for marketing purposes, according to Article 28 of the Data Protection Act. Controllers engaged in direct marketing, and those who use a list of names, addresses, email addresses, phone numbers and similar data, or disclose them to a third party in connection with
a similar enterprise, shall, prior to using such a list for the described purposes, compare it with the Registers Iceland’s registry, in order to prevent direct mail from being sent to, or phone calls being made to, those who have objected to it. The DPA can make exemptions from this duty in special cases.
India

Probir Roy Chowdhury
Bangalore
Tel: +91-80-43503618
probir@jsalaw.com

Sajai Singh
Bangalore
Tel: +91-98450 78666
sajai@jsalaw.com
1. Recent Privacy Developments

**Supreme Court recognizes Right to Privacy as Fundamental Right**

In a historic verdict delivered by a nine judge constitution bench, the Supreme Court of India (“Court”) unanimously recognized the “Right to Privacy” as a fundamental right guaranteed under the Constitution of India (“Constitution”). This decision was delivered by the Court on 24 August 2017 in the matter of *Justice K.S. Puttaswamy v. Union of India*¹ (“Puttaswamy”), and came about as a result of numerous petitions challenging the validity of the Indian Government’s “Aadhaar” program – an ambitious project that aims to build a personal identity and biometric information based database of every Indian.

In its decision, the Court upheld the right to privacy as an intrinsic and essential element of human dignity. The Court called upon the State to implement a robust data privacy regime, whereby any intervention or restraint on an individual’s privacy is subject to the three-fold test. The contents of this three-fold test emanate from the substantive and procedural mandate of the Constitution, and may be summarized as follows:

- **Legal Basis:** The first requirement is for any intervention or restraint on privacy to be based on a law in force.
- **Legitimate Aim:** Second, such intervention or restraint must be based on a legitimate aim of the State. In other words, the law that supports an intervention or restraint on privacy must be reasonable, and must not suffer from an inherent arbitrariness.
- **Proportionality:** The third test laid down by the Supreme Court was that of proportionality, or the requirement for the State’s actions against an individual to be proportionate to the objective sought to be fulfilled by the law.

The decision in Puttaswamy is expected to have a profound and far reaching impact on India’s constitutional landscape. The observations of the Court will affect not only Aadhaar, but also LGBT rights, India’s data protection framework, censorship, State sponsored surveillance, data collection practices of multinational companies and free speech.

2. Emerging Privacy Issues and Trends

**Committee of Experts Appointed to Prepare Data Protection Bill**

On 31 July 2017, the Ministry of Electronics and Information Technology, Government of India (“MeitY”) appointed a Committee of Experts (“Committee”) to evaluate the shortcomings of India’s existing data protection framework.

---

¹ W.P (Civil) No. 494 of 2012
framework, and to formulate and propose suitable legislation to address these issues. The 10 (ten) member Committee is headed by Justice B N Srikrishna (a former judge of the Supreme Court of India), and includes members from MeitY, the Department of Telecommunications ("DoT"), legal think tanks and members of the academic community.

The Committee is expected to publish a first draft of the Data Protection Bill in early 2018. In recent interviews, members of the Committee have stated that the forthcoming law will hinge on Data Subject consent.

3. Law Applicable

The Information Technology Act, 2000 ("IT Act"), as amended by the Information Technology (Amendment) Act, 2008, and circulars, notifications and various rules made thereunder, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and the Information Technology (Intermediaries Guidelines) Rules, 2011 ("Privacy Rules"), are the main laws and regulations governing data protection and information technology in India.

The following additional legislations, though not dealing directly with data protection and information technology, find application in addition to the aforementioned regulations:

1. The Indian Contract Act, 1872;
2. Indian Penal code, 1860;
3. Right to Information Act, 2004;
4. Indian Copyright Act, 1957;
5. The Consumer Protection Act, 1986;
6. Specific Relief Act, 1963;
7. Reserve Bank of India Act, 1934; and
8. Tort Law.

Offenses under the above rules and regulations are enforced by the judiciary and the various cyber crime cells across the country. The provisions of the Indian Penal Code, 1860 have been applied to offenses under the law applicable to information technology as well. India does not have a “Regulator” in place presently, however, there are various organizations lobbying for more stringent data protection and privacy laws to be implemented. Presently, data protection is maintained by the judiciary and the cyber crime units of the police force.
4. Key Privacy Concepts

a. Personal Data

The Privacy Rules define “Personal Information” as “any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person”.

Apart from Personal Information, the Privacy Rules also define the term “Sensitive Personal Data or Information”. Even though both the terms have been defined in the Privacy Rules, the concepts tend to overlap. Different provisions are applicable to “Personal Information” and “Sensitive Personal Data or Information”, while some provisions are applicable to both. Pursuant to a clarificatory press note issued by the Ministry of Communications and Information Technology, Government of India (“Press Note”), the present stance of the industry is that, while all the provisions of the Privacy Rules apply to Sensitive Personal Data or Information, only some provisions apply to Personal Information.

b. Data Processing

Persons located in India

Privacy Rules are applicable to a person located in India. However, there is lack of clarity on whether the term “person” refers to “natural individuals” who are the providers of information, or body corporates collecting data.

If it is assumed that “person” refers to “natural individuals”, then a body corporate located overseas, which handles data of individuals located in India through a computer resource located in India, will have to comply with the Privacy Rules.

Body corporates located in India, computer resources located in India or overseas

Irrespective of the location of the computer resource (either in India or abroad) and the place of residence of the Data Subject, the Privacy Rules are applicable to all body corporates located in India.

Body corporate located overseas, computer resource located in India

Section 43-A of the IT Act, read with Section 75, provides that the IT Act will be applicable to a body corporate located overseas, whose computer resource is located in India. As per the interpretation that has been adopted, the Privacy Rules apply to all Indian body corporates and to those foreign body corporates which collect Personal Information or Sensitive Personal Data or Information from Indian persons.
c. **Processing by Data Controllers**
There are no specific provisions under applicable Indian laws.

d. **Jurisdiction/Territoriality**
A body corporate or any person on its behalf may transfer Sensitive Personal Data or Information or any other information, to any other body corporate or a person in India, or in any other country, only after it ensures, in the case of another country, that such jurisdiction provides the same level of data protection as is required to be in compliance with the Privacy Rules. Further, such transfer may be done only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and Data Subject. Alternatively, such data may be transferred with prior consent of the Data Subject.

e. **Sensitive Personal Data**
The Privacy Rules define sensitive personal information to include information relating to:

1. passwords;
2. financial information (e.g., bank account/credit or debit card or other payment instrument details);
3. physical, physiological and mental health condition;
4. sexual orientation;
5. medical records and history;
6. biometric information (biometrics means the technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes);
7. any detail relating to the above clauses as provided to a body corporate for providing services; and
8. any of the information received under the above clauses for storing or processing under a lawful contract or otherwise.

However, any information available in the public domain or any information to be furnished to any government agency or which should be made available to the public under the Right to Information Act, 2005 has been expressly exempt from the scope of this definition.

f. **Employee Personal Data**
There are no additional requirements/definitions for Employee Personal Information. If Sensitive Personal Data or Information of employees is being collected, then prior consent of such employees will be required.
There is no specific legislation pertaining to monitoring of employees. While it may be a practice of employers to monitor email and computer use of employees, employers must ensure compliance with the right to privacy of employees and with the regulations pertaining to collection, use, storage and transfer of Sensitive Personal Data or Information and personally identifiable information. Further, the IT Act also regulates images being captured via such monitoring and employers would have to adhere to the same.

An additional point to be noted is that the courts may construe the right to access information in a computer or computer resource in light of the ownership of computer or computer resource being transferred.

5. Consent

a. General

In India, consent of the Data Subject is required for the collection, processing, and disclosure of Sensitive Personal Data or Information. Consent is also contemplated as a justification or legal grounds for the collection, processing and/or use of Personal Information.

For consent to be considered valid, it must be voluntary, informed, explicit and unambiguous. It can be express or implied but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Information. Consent must be obtained prior to or at the time of collection of data. Consent given by a Data Subject can be withdrawn at any time. It does not need to be in the local language, but the Data Subject must understand the language in which consent is given.

b. Sensitive Data

An organization that processes Sensitive Personal Data or Information has an obligation to obtain consent in writing through letter or fax, or email or other electronic means from the Data Subject.

Based on this, the privacy policy of each body corporate may contain an “I Agree” tab at the end of the text. A click on the tab by the reader of the privacy policy (i.e., the Data Subject) would be deemed to be valid consent under the Privacy Rules.

Additionally, the Privacy Rules require that, while collecting Sensitive Personal Data or Information directly from the Data Subject, the body corporate must, inter alia, inform the Data Subject of the purpose for which his or her information is being collected, that the information so collected may be transferred/disclosed and names/addresses of the agency collecting and retaining this information.

358 | Baker McKenzie
Further, a body corporate or any person on its behalf may collect any Sensitive Personal Data or Information only if the information is collected for a lawful purpose connected with an integral activity of the body corporate.

c. Minors
There are no specific guidelines with regard to data privacy under the IT Act or Privacy Rules regarding minors.

However, the IT Act punishes the publication or transmission of material depicting children in sexually explicit acts, in electronic form.

d. Employee Consent
Employee consent is required if his or her Sensitive Personal Data or Information is being collected, used, handled, stored and/or transferred by the employer (i.e., the body corporate). The requirements for such consent are the same as the general consent requirements.

Employee consent is also required when an employer decides to implement a BYOD program. There is no specific legislation pertaining to BYOD, however various laws pertaining to the right to individual privacy and collection and storage of Sensitive Personal Data and Information and personally identifiable information would apply. The general practice prevalent is for companies to implement in-house corporate policies that cover various scenarios regarding confidentiality, integrity and access of data.

e. Online/Electronic Consent
Online/Electronic consent is permissible and can be effective if properly structured and evidenced. Hence, electronic consent is enforceable in India.

The related contract must comply with the requirements of the Indian Contract Act, 1872 to qualify as a valid binding contract.

The IT Act prescribes regulations pertaining to electronic signatures, the procedure for the issuance and the manner of obtaining a digital signature, and regulations pertaining to certifying authorities. Under the IT Act, any subscriber may authenticate an electronic record by affixing his/her digital signature to such electronic record.

Further under the Indian Evidence Act, 1872, electronic records may be submitted as primary evidence if compliant with the conditions provided thereunder. However, the prevalent practice presently is to affix a “wet signature” to a document, scan and email the same as an electronic record. This does not, however, satisfy the conditions provided under the Evidence Act, 1872 for electronically signed documents and primary evidence and is thereby considered secondary evidence by the courts.
6. Notice Requirements
An organization that collects Personal Information must provide Data Subjects with information about: the organization’s identity; the purposes for collecting Personal Information; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Information; the consequences of not providing consent; the rights of the Data Subject; how the Personal Information is to be retained; where the Personal Information is to be transferred and stored; how to contact the privacy officer or other individual who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access/and or correct the Data Subject’s Personal Information; the duration of the proposed processing; and the means of transmission of the Personal Information.

7. Processing Rules
An organization that processes Personal Information must limit the use of the Personal Information to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Information was collected, and delete/anonymize Personal Information once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization about the Personal Information the organization holds on the Data Subject and how the Data Subject’s Personal Information is being processed; access the Data Subject’s Personal Information, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Information; and request the deletion and/or destruction of the Data Subject’s Personal Information.

9. Registration/Notification Requirements
There are no formal registration requirements in India imposed on organizations that collect and process Personal Information.

10. Data Protection Officers
Every body corporate collecting/using/retaining or transferring Sensitive Personal Data or Information is obligated to designate a Grievance Officer in order to address any discrepancies and/or grievances that any Data Subject may have. The names and contact details of such Grievance Officer must be published on the website of the body corporate. The Grievance Officer is required to redress the grievances of the Data Subject within one month from the date of receipt of grievance.
11. International Data Transfers
Organizations in India may transfer Personal Information outside of the jurisdiction provided that the receiving jurisdiction provides a similar level of protection for Personal Information; impacted Data Subjects have been informed or have been provided consent; and that reasonable steps have been taken to safeguard the Personal Information to be transferred.

12. Security Requirements
Organizations are required to take steps to: ensure that Personal Information in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Information; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Information involved.

Foreign entities may have to comply with Indian security standards when dealing with Indian companies. Presently, Indian legislation prescribes data security standards of ISO/IEC 27001:2005 as the norm when handling sensitive personal information and personally identifiable information.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Information to third parties are required to use contractual or other means to protect Personal Information. These organizations may also be required to comply with sector-specific requirements. Furthermore, organizations that outsource data processing shall be liable with the third-party provider in case of breach by the latter.

There is no specific regulation pertaining to cloud computing. However any entity collecting Sensitive Personal Data or Information or personally identifiable information must comply with ISO/IEC 27001:2005 security standards.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, civil actions, and/or private rights of action. As per the IT Act, any body corporate which breaches Section 43-A is liable to pay damages by way of compensation to the Data Subject so affected. There is no limit on the amounts recoverable.

15. Data Security Breach
As per the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the “CERT-In Rules”) service providers, intermediaries, data centers and corporate entities are obligated to notify CERT-In upon the occurrence of
certain cyber security incidents, including data security breaches. While no fixed time limit has been prescribed in this regard, the CERT-In Rules require such notifications to be made within such reasonable time as would allow authorities to take necessary remedial measures.

16. Accountability
Organizations are currently not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Information.

17. Whistle-Blower Hotline
There is no filing requirement for the introduction of a whistle-blower hotline in India. Whistle-blower hotlines may be established as long as they are in compliance with local laws.

18. E-Discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Sensitive Personal Data or Information is involved, and advise employees of its implementation, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering
Generally, the introduction of a spam filtering solution in an organization does not raise privacy issues provided that the employees have been informed of the monitoring policies being implemented in the workplace.

20. Cookies
There are no specific laws/rules that regulate the deployment of cookies in India; and hence, the use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted. Consent of Data Subjects must be obtained before cookies can be used.

Under the IT Act, any person who, without permission of the owner or any other person who is in charge of a computer, computer system or computer network or computer resource introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network shall be liable to pay damages by way of compensation to the person so affected.

Cookies fall under the definition of “computer virus” as provided under the IT Act which means any computer data that attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource.
Based on the above, if a person were to include cookies on their websites without obtaining the permission of and informing such user of the use of cookies and any damage were to result from the placement of such cookies, the owner of the website would be liable to pay compensation to the person so effected.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.

There is no specific legislation in India that governs online direct marketing; however, the general practice is to permit an intended recipient to opt in/opt out of receiving any marketing material.

Similarly, there is no existing legislation that governs spam; however, the general practice of providing an opt-in/unsubscribe option is followed by email marketers.

The Telecom Commercial Communications Customer Preference Regulations (“TRAI Regulations”) regulate unsolicited marketing calls. The TRAI Regulations establish a “National Do Not Call Register”, and a “Private Do Not Call List”. The TRAI Regulations provide customers with the option to register with the Telecom Regulatory Authority of India (“TRAI”) or their service providers under the “fully blocked” or “partially blocked” categories. The TRAI Regulations also require telemarketers to register themselves with TRAI, which maintains a National Telemarketers Register.
Indonesia

Mark Innis
Jakarta
Tel: +62 21 2960 8618
Mark.innis@bakernet.com

Adhika P.S. Wiyoso
Jakarta
Tel: +62 21 2960 8507
adhika.wiyoso@bakernet.com

Denny Ngadimin
Jakarta
Tel: +62 21 2960 8641
denny.ngadimin@bakernet.com
1. New Implementing Regulation on Personal Data Protection

Recent developments

The Minister of Communication and Informatics has issued Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (“Data Protection Regulation”)\(^2\). This regulation is an implementing regulation of the Electronic Information and Transactions Law (i.e., Law No. 11 of 2008) (“EIT Law”) and Government Regulation No. 82 of 2012 (“Regulation 82”) (which address the use of Personal Data through electronic media/systems).

The Data Protection Regulation emphasizes the current Personal Data protection provisions in Indonesia by providing new measures to protect the use of Personal Data in electronic systems.

While the data protection regime in Indonesia is not as sophisticated as other developed countries (such as European countries or Singapore), the Data Protection Regulation introduces new measures; although there is a two-year period for compliance with the Data Protection Regulation.

The Ministry of Communication and Informatics (“MOCI”) will use the two-year transitional period to prepare for the implementation of the new regulation, as many provisions require further clarification and processes.

Implications for Electronic System Operators

The Data Protection Regulation provides more detailed provisions than the EIT Law and Regulation 82 on how to use Personal Data in electronic systems in every stage of the process, namely acquiring and collecting, processing and analyzing, storing, displaying, announcing, transmitting, disseminating and/or providing access to, and/or deleting Personal Data.

Failure to comply with the provision under the Data Protection Regulation could lead to administrative sanctions, including verbal warnings, warning letters, temporary suspension of business activities, and announcement on online website.

In terms of coverage, the Data Protection Regulation does not specifically state that it has extraterritorial coverage like the EIT Law. However, as an implementing regulation of the EIT Law, there should be an assumption that it does have extraterritorial coverage. It remains to be seen whether the MOCI will enforce the Data Protection Regulation against offshore electronic system operators.

---

\(^1\) As of the time of publication of this 2017 Global Privacy & Information management Handbook.

\(^2\) The Data Protection Regulation became effective on 1 December 2016 (but was only made publicly available on 9 December 2016)
**What the Data Protection Regulation says**

**a. Definition of Personal Data**

The Data Protection Regulation defines:

- "Personal Data" as "*certain individual data* which is stored, maintained and kept accurate and the confidentiality of which is protected".

- "Certain individual data" is defined as "true and actual information that is attached to and identifiable towards, directly or indirectly, an individual".

The definition above is very broad and basically could cover any information of an individual. At the time of publication it is unclear what would not be considered as Personal Data and whether anonymized data or publicly available data (or data which is otherwise not confidential) is covered under the definitions.

**b. Requirements for Personal Data Usage**

The Data Protection Regulation classifies the requirements in “using” Personal Data based on the relevant processes, i.e.:

<table>
<thead>
<tr>
<th>Process</th>
<th>Main Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquiring and collecting</strong></td>
<td>1. The acquisition and collection of Personal Data is limited for the specific purposes set out in the collection form.</td>
</tr>
<tr>
<td></td>
<td>2. Data Subjects must be given options to (a) specify whether the collected Personal Data is confidential, and (b) change, add to or update their Personal Data.</td>
</tr>
<tr>
<td></td>
<td>3. Collected Personal Data must be verified to ensure its accuracy.</td>
</tr>
<tr>
<td></td>
<td>4. Electronic system operators must have interoperability and compatibility, and must utilize legal (read as non-pirated) software.</td>
</tr>
<tr>
<td><strong>Processing and analyzing</strong></td>
<td>1. The processing and analyzing of Personal Data is limited to the extent it is disclosed to and given consent by the Data Subjects.</td>
</tr>
<tr>
<td></td>
<td>2. The processed and analyzed Personal Data must be verified to ensure its accuracy.</td>
</tr>
<tr>
<td>Process</td>
<td>Main Requirements</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Storing                                              | 1. Stored Personal Data must be verified to ensure its accuracy.  
2. Stored Personal Data must be encrypted data (the minimum requirement for the encryption is unclear).  
3. The minimum retention for stored Personal Data is five years (unless stated otherwise in other laws and regulations).  
4. Electronic system operators must have onshore data centers and disaster recovery centers if they are engaged in “public service” activities (the Data Protection Regulation does not define “public service”; so this issue, which has arisen under other regulations, remains unclear at the time of publication). |
| Displaying, announcing, transmitting, disseminating and/or providing access | 1. The display, announcement, transmission, dissemination and/or accessibility of Personal Data are limited to the extent it is disclosed to and given consent by the Data Subjects.  
2. The Personal Data that is used in these processes must be verified to ensure its accuracy.  
3. Offshore data transfers may only be conducted after a coordination with the MOCI (which involves reporting the plan and results of the transfer and seeking advocacy (the latter is unclear)). This process will need to be further clarified by the MOCI.  
4. Providing access to Personal Data can be done for law enforcement purposes based on a valid request from the law enforcement agency. |
| Deleting                                              | 1. Deletion of Personal Data can only be done (a) if the retention period has expired, or (b) based on a request from the Data Subject (and supported by a court order (see below)).  
2. Deletion of Personal Data covers both electronic and non-electronic deletions to the point where |
Process | Main Requirements
--- | ---
 | such Personal Data cannot be re-displayed in an electronic system unless the Data Subject gives the Personal Data/consent again.

**Other Provisions**

There following are some general requirements that are not specific to the processes above and which are relevant.

**a. Consent**

Any use of Personal Data through an electronic system may only be done with proper prior consent from the Data Subject. The consent must be in writing (meaning an express consent), whether manually or electronically, and in the Indonesian language (although there is no prohibition of a dual language format, so that format can still be used, if preferred). Further, the consent is only effective after a complete explanation from the electronic system operators on the intended use, broadly defined as noted above, of the Personal Data.

There is no further elaboration on the nature of the consent form and consequently, at the time of publication, it is unclear whether this means that a separate form must be prepared.

How the MOCI will regulate the concept of consent and the consent form and how market practice will develop remains to be seen.

**b. System Certification**

Electronic system operators must use a certified electronic system. There is no further elaboration on this requirement. The only regulations that govern the electronic system certification process are Regulation 82 and MOCI Regulation No. 4 of 2016 on Information Security Management Systems. Clearly further clarification on the certification process is needed from the MOCI.

**c. Data Breach**

Electronic system operators are required to promptly notify in writing the Data Subjects when there is a data breach. The notification:

i. must include the reasons or the causes of the data breach;

ii. can be done electronically to the Data Subjects if the approach has been approved by the Data Subjects during the data collection;
iii. must be received by the Data Subjects if the breach has a potential to cause loss to the relevant Data Subjects (that is, a positive obligation on electronic system providers to ensure that the Data Subject is fully aware of the breach); and

iv. must be sent within 14 days after the data breach is known by the electronic system operator.

d. Right to be Forgotten
The Data Protection Regulation provides that the Data Subject has the right to request his/her Personal Data to be removed at any time. However, the deletion request must be made in accordance with the prevailing laws and regulations (which under the EIT Law is only for irrelevant data and must be based on a court order).

Further, the Data Protection Regulation now stipulates that the deletion of Personal Data covers both electronic and non-electronic deletions to the point where such Personal Data cannot be re-displayed in an Electronic System, unless the Data Subject gives the Personal Data/consent again.

e. Dispute Resolution
Every Data Subject and electronic system operator can submit a complaint to the MOCI in relation to a failure to protect Personal Data. The intent is that the complaint will be dealt with outside the court process (through a discussion or mediation). The MOCI will delegate the dispute resolution authority to its Director General, who may form a panel for the dispute resolution.

The processes and procedures for this alternative dispute resolution mechanism are not yet in place.

If the complaint cannot be resolved through the alternative dispute resolution mechanism, a claim can be submitted to the court (but this is limited to civil claims).

Electronic system operators should consider the following (noting the need for further clarifications from the MOCI and the two-year transitional period):

1. Ensure that all consents are express and written consents.

2. Ensure that there is a data collection form containing the required consent, and the data collection form specifies (i) that the data provided is accurate, (ii) that the data is not confidential (if there will be extensive use of that Personal Data) and (iii) the purposes and use, as broadly defined (above), of the Personal Data.

3. Establish internal standard operating procedures on Personal Data protection:
   a. to comply with the above "usage" requirements;
b. to prevent data breaches; and

c. to stipulate the necessary actions should there be a breach of data.

4. Establish internal standard operating procedures on the deletion of Personal Data given the new provisions on the right to be forgotten.

5. Amend the privacy policy and any other electronic contracts to be in line generally with the provisions of the Data Protection Regulation.


7. Lobby the MOCI for favorable processes and procedures that the MOCI will need to set for implementation of the Data Protection Regulation.

2. Emerging Privacy Issues and Trends

a. Right to be Forgotten
With the issuance of an amendment to the EIT Law in October 2016 and the Data Protection Regulation in December 2016, Indonesia now has a concept of the right to be forgotten. While the provisions are still rudimentary and not as sophisticated as other countries (e.g., EU countries), this gives a right for Data Subjects to request deletion of their Personal Data from electronic systems provided that the Personal Data is irrelevant to the electronic system providers and that the request is based on a court decision. Further, for offshore internet companies, the issue will be the Government’s capacity to enforce offshore – with the only real enforcement being the blocking of internet sites.

b. Access to Electronic System in Criminal Investigations
The EIT Law, after being amended, now gives additional authority to civil servant investigators to request information in or made by electronic systems and can receive reports about, investigate and arrest internet users suspected of violating the law generally.

In addition, investigators are also authorized to restrict access to electronic documents or electronic systems that are engaged in criminal conduct such as cybercrime, and are authorized to carry out raids.

c. Government’s Right to Terminate Access
The EIT Law, after being amended, now gives the Government a right to terminate access and/or order electronic system operators to terminate access to electronic information and/or documents with contents that violate the law.

There is a current Negative Content Regulation issued by the Minister of Communications and Informatics, which authorizes the MOCI to block internet
websites with negative content based on reports from the public, government institutions or law enforcement authorities.

The EIT Law, as amended, includes a similar right (although without the need for reports to be made to the MOCI) and now the Negative Content Regulation has a firmer legal basis on which the MOCI can act. The EIT Law provides that there will be a Government Regulation implementing these provisions, however in the absence of the implementing regulation, it is likely the MOCI will continue to use the Negative Content Regulation issued by the Minister of Communications and Informatics.

d. **New Measures of Data Protection**

Clearly the issuance of the Data Protection Regulations introduces new measures to protect the use of Personal Data and new requirements for electronic system providers to comply with. While there is a two-year transitional period to comply with the regulation, electronic system operators should start considering changing their data privacy policies and systems to deal with these new requirements.

3. **Law Applicable**

The main law and regulations that address data protection/privacy matters are:

a. **The EIT Law**

b. **Regulation 82**

c. **The Data Protection Regulation**

Other than the above, there are also a number of other Indonesian laws and sectorial regulations that relate to the issue of data privacy and local data center requirements (such as (i) Minister of Energy and Mineral Resources Regulation No. 27 of 2006 on Management and Utilization of Oil and Gas General Survey, Exploration and Exploitation Data and SKK Migas Decision No. 8 of 2013 on Guidelines on Management of Information Technology and Communication for Contractors of Cooperation Contracts, for the oil and gas sector; (ii) Bank Indonesia Regulation No. 9 of 2007 on the Implementation of Risk Management in the Utilization of Information Technology by Commercial Banks, for the banking sector; (iii) Minister of Health Regulation No. 269 of 2008 on Medical Records and Minister of Health Regulation No. 1171 of 2011 on Hospital Information System, for the healthcare sector and (iv) Regulation No. 69 of 2016 on Implementation of Insurance, Syariah Insurance, Reinsurance and Syariah Reinsurance Businesses, for the insurance sector (“Sectorial Regulation”).
4. Key Privacy Concepts

a. Personal Data
Regulation 82 and the Data Protection Regulation define “Personal Data” as data of individuals which must be stored and maintained without error and the secrecy of which is protected (this is a literal translation of the regulation and it remains unclear at this time).

The above definition only covers data of individuals and does not cover data on businesses (e.g., company’s name, address, phone number, etc.). However, the definition is very general and may be interpreted broadly. It is advisable that a conservative approach be taken in assessing whether certain data contains Personal Data and to assess whether or not an element of information can lead to a specific person (e.g., name, email, IP address, phone number, ID, location, etc.).

b. Data Processing
Effectively, data processing is the use of Personal Data, which must be based on consent from the Data Subject and in accordance with the purpose conveyed to the relevant Data Subject when collecting the data.

c. Processing by Data Controllers
There are no specific laws or regulations on the processing of Personal Data by Data Controllers (as both Regulation 82 and the Data Protection Regulation do not differentiate between “Data Controller” and “Data Processor”). Effectively, any use of Personal Data must be based on consent from the Data Subject and in accordance with the purpose conveyed to the relevant Data Subject when collecting the data.

d. Jurisdiction/Territoriality
The EIT Law applies to local or foreign legal subjects and to all electronic transactions conducted inside or outside Indonesia, having a legal impact in Indonesia, or having a legal impact outside of Indonesia but produces detrimental effects to the interests of Indonesia.

Consequently, entities without a presence in Indonesia but undertaking activities that may affect Indonesia or Indonesian entities/individuals, may also be subject to the EIT Law. Although, in practice the EIT Law has not been strictly enforced against an offshore entity given the impracticality of doing so, the government could ultimately require sites/services to be blocked (as it does with pornography sites).

Regulation 82 and the Data Protection Regulation do not specifically state that they have extraterritorial coverage like the EIT Law. However, as implementing regulations of the EIT Law, there should be an assumption that they do have extraterritorial coverage.
e. **Sensitive Personal Data**
There is no law or regulation which classifies certain Personal Data as Sensitive Personal Data. In practice, however, the consent form, employment agreement, company regulation or collective labor agreement may include a provision which classifies certain Personal Data of an employee as “Sensitive Personal Data of an employee”.

f. **Employee Personal Data**
There is no law or regulation which classifies certain data of an employee as Personal Data. In practice, however, the consent form, employment agreement, company regulation or collective labor agreement may include a provision which classifies certain data of an employee as Employee Personal Data.

5. **Consent**

a. **General**
The EIT Law, Regulation 82 and the Data Protection Regulation require consent of the relevant individuals with respect to any use of their Personal Data through electronic media and/or electronic systems, unless the law stipulates otherwise. In addition, there is ambiguity among the various Indonesian laws to suggest that the prudent course would be to always secure prior consent of the Data Subject of such data to use, process, transfer and disclose their Personal Data, regardless of whether electronic media are used.

The Data Protection Regulation requires the consent to be in writing (meaning an express and opt-in consent), whether manually or electronically, and in the Indonesian language (although there is no prohibition of a dual language format, so that format can still be used, if preferred). Further, the consent is only effective after a complete explanation from the electronic system operators on the intended use, broadly defined as noted above, of the Personal Data.

There is also a requirement under the Data Protection Regulation to use a consent form in order to obtain consent. However, there is no further elaboration on the nature of the consent form and consequently, it is unclear whether this means that a separate form must be prepared.

b. **Sensitive Data**
There is no provision in the EIT Law, Regulation 82, the Data Protection Regulation or other laws and regulations on “Sensitive Data”. As the EIT Law, Regulation 82 and the Data Protection Regulation generally require consent for any use of Personal Data in electronic media and/or electronic systems from the relevant Data Subjects, any use of Sensitive Personal Data must also be based on the prior consent of the owner of such Sensitive Data.
c. Minors
Under the Data Protection Regulation, if the Data Subject is a person who is classified as a minor under Indonesian laws and regulations, consent must be given by the parent or guardian of the minor.

The term “parent” means the biological father or mother, while the term “guardian” means the person who is responsible to raise the minor.

Please note that in Indonesia, there are several laws that regulate the legal age of a person (e.g., Indonesian Civil Code, Marriage Law and Manpower Law), and the legal age varies – from one to another (generally between 18 and 21). Basically the general limitation to determine the legal age to perform legal action (namely to have the capacity to enter into a contract) is based on Article 330 of the Indonesian Civil Code which is 21 or already married.

d. Employee Consent
There is no exception for the use of Employee Personal Data. Any use of Employee Personal Data is subject to the general consent requirement mentioned above. Consequently, proper consent from the employees must be obtained for any use of their Personal Data.

In practice, the employment agreement, company regulation or collective labor agreement may also include a provision which reflects the employees consenting to the employer’s possible use, access, process, transfer and disclosure of their Personal Data. Nevertheless, in reviewing a number of related laws, the prudent course of action is to secure the prior consent of the employees concerned regardless of whether electronic media are used.

e. Online/Electronic Consent
The Data Protection Regulation clearly states that consent can be obtained electronically and must be in writing (which means express and opt-in consent).

Under the EIT Law, Regulation 82 and the Data Protection Regulation, electronic information and electronic documents, including their print-outs, are considered valid legal evidence, except where the law requires such documents to be made in writing (e.g., employment agreements) or in the form of a deed (e.g., land title documents). Electronic information and electronic documents are valid to the extent that the information can be accessed, presented or guaranteed of its completeness, and can be relied on to explain certain situations.

In practice, Indonesian courts (particularly, the Industrial Relations Courts, in the event of an employment dispute) may request for a print-out of the relevant electronic document.
In light of the above, we suggest that even though consent can be obtained electronically, mechanisms are put in place to:

1. allow the printing of such consent whenever necessary (e.g., in the event that the consent will be used as evidence in court); and

2. verify the authenticity of the consent (which is electronically generated).

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; the handling of the Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to make an inquiry or file a complaint, how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected and which have been informed to and consented by the Data Subject.

8. Rights of Individuals

Data Subjects have the general right to be informed by the data collector on what Personal Data is being collected and how the Personal Data is being used.

Further, the Data Protection Regulations stipulates that Data Subjects are entitled:

a. to have their Personal Data remains confidential;

b. to submit a complaint to the Minister of Communication and Informatics in order to resolve a Personal Data dispute on the grounds of failure by an electronic system operator to protect the confidentiality of their Personal Data;

c. to be given access or to revise or update the Data Subject’s Personal Data without affecting the Personal Data management system, unless stated otherwise by other laws and regulations;

d. to be given access to the historic information of the collected Personal Data; and
e. to request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

Under the Data Protection Regulation, electronic system operators must use a certified electronic system in order to use Personal Data. There is no further elaboration on this requirement.

Further, the Data Protection Regulation also requires coordination and reporting to be done in order to do offshore data transfers (please see below).

10. Data Protection Officers

There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Subject to the Data Protection Regulation and the Sectorial Regulations, organizations may transfer Personal Data outside of Indonesia, provided that impacted Data Subjects have been informed or have provided consent; and that reasonable steps have been taken to safeguard the Personal Data to be transferred.

Further the Data Protection Regulation provides that in order to do offshore data transfers, electronic system operators must:

a. coordinate with the MOCI or authorized officials/institutions; and

b. comply with the regulation on offshore Personal Data transfer (which is not yet available, at the time of publication).

The coordination is conducted by way of:

a. reporting the plan to implement the Personal Data transfer;

b. asking for advocacy (if necessary); and

c. reporting the result of the transfer implementation.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.
13. Special Rules for Outsourcing of Data Processing to Third Parties

The general requirements of an outsourcing arrangement under the Indonesian labor laws and regulations will apply.

In addition, for Indonesian banks, the Financial Services Authority (Otoritas Jasa Keuangan, “OJK”) has Regulation No. 38/POJK.03/2016 on the Application of Risk Management in the Use of Information Technology by Banks. This regulation is the legal basis for banks in Indonesia in applying its information technology system, particularly for data processing.

Indonesian banks are allowed to engage a third party that provides Information Technology service. The Information Technology service provider may be a local provider (Indonesian company) or a foreign provider (non-Indonesian company). If the bank intends to engage a foreign Information Technology service provider, the bank must first secure approval from the OJK.

That approval can only be given by OJK if the Indonesian bank meets certain requirements.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, administrative fines, penalties or sanctions, civil actions, class actions, criminal proceedings, and private rights of action.

15. Data Security Breach

The Data Protection Regulation requires a written notification to the relevant Data Subject in case of a data breach. The notification:

a. must include the reasons or the causes of the data breach;

b. can be given electronically to the Data Subject if the approach has been approved by the Data Subjects during the data collection;

c. must be received by the Data Subjects if the breach has the potential to cause loss to the relevant Data Subjects (that is, a positive obligation on electronic system providers to ensure that the Data Subject is fully aware of the breach); and

d. must be sent within 14 days after the data breach is known by the electronic system operator.

An organization that is involved in a data breach situation may be subject to a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions, and a criminal prosecution.
16. Accountability
Subject to regulatory guidance, organizations may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline
There are no laws/rules that regulate the implementation of whistle-blower hotlines in Indonesia.

18. E-Discovery
A provision in the Human Rights Law provides that secrecy of correspondence (including those in electronic form) may not be violated except by a court order in accordance with the prevailing laws. In addition, under the EIT Law, the basic principle is that the confidentiality of private or personal information of an individual must be preserved. Conceivably, if Personal Data of employees are deemed to have been gathered from various correspondence between the company and its employees, the provisions under the Human Rights Law and the EIT Law may be applied. However, there has been no case reported on this.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace; and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies
There are no specific laws/rules in Indonesia that regulate the use and deployment of cookies.

21. Direct Marketing
An organization that plans to use any Personal Data for direct marketing activities is required to obtain the Data Subject’s prior consent.
Ireland

John Cahir
Dublin
Tel: +353 1 649 2000
jcahir@algoodbody.com

Alison Quinn
Dublin
Tel: +353 1 649 2461
alquinn@algoodbody.com
1. Recent Privacy Developments

*The Irish Data Protection Commissioner seeks a reference to the CJEU for a preliminary ruling on the validity of Standard Contractual Clauses*

- Following the CJEU ruling in *Schrems v. Data Protection Commissioner C362/14* that the Safe Harbour framework was invalid, Schrems was allowed to amend and resubmit his complaint to the Irish Data Protection Commissioner (the “DPC”). He submitted a new complaint questioning the legality of transfers made under the Standard Contractual Clauses (“SCCs”), an alternative method used by companies to transfer data to the US.

- The DPC is of the opinion that the objections to SCCs are well-founded and sought a reference to the CJEU for a preliminary ruling on their validity. Representatives of the tech industry and the US government were joined in the case as *amicus curiae* (friends of the court).

- On 4 October 2017, the High Court decided it would ask the CJEU to rule on the validity of the SCCs. In its 152 page judgment the High Court agreed with the DPC’s concern that the SCCs alone cannot ensure an adequate level of protection in third countries for data protection rights.

- The High Court will frame the questions for referring to the CJEU and the Statement of Facts. It is expected that the hearing before the CJEU will take place within 12-18 months.

*The Supreme Court clarified the law in relation to the right of appeal against a decision of the Data Protection Commissioner*

- Section 26 of the Data Protection Acts 1988 and 2003 (the “DP Acts”) provides a right of appeal before the courts against decisions of the DPC in relation to complaints under Section 10(1)(a) (enforcement of data protection) of the DP Acts. The scope of this right was examined in the recent case of *Nowak v. The Data Protection Commissioner*.

- Nowak was a trainee accountant who submitted a request to Chartered Accountants in Ireland (“CAI”) to view one of his examination scripts. The CAI refused to release the script on the grounds that it was not Personal Data. Nowak complained to the DPC, which agreed that the material did not constitute Personal Data within the meaning of the Acts. It held that the complaint was both frivolous and vexatious and that it was therefore not required to investigate it.

- The Circuit Court held that there was no right of appeal against a decision by the DPC not to investigate a complaint. This was upheld in the High Court and the Court of Appeal.
In April 2016, the matter came before the Supreme Court. The Supreme Court overturned the finding of the previous courts, and held that the applicant did have a right to appeal the decision of the DPC. The question of whether an examination paper could be classified as Personal Data was deemed to be a matter of EU law and the Supreme Court therefore referred it to the CJEU.

In July 2017 Advocate General Kokott delivered an Opinion, stating that an exam script was capable of constituting Personal Data. The Opinion is not a ruling and the CJEU is not obliged to follow an Advocate General’s line of argument. A ruling by the CJEU is expected in the autumn of 2017, after which the case will be referred back to the Irish Supreme Court.

General Scheme of the Data Protection Bill 2017

The Department of Justice published the General Scheme of the Data Protection Bill 2017 in May 2017. The Bill is designed to give effect to, and provide for derogations from, the GDPR. It also transposes the Law Enforcement Directive (2016/680) which concerns the processing of Personal Data for the purposes of the prevention, investigation, detection or prosecution of criminal offenses, and the free flow of such data.

The Bill is still at a preliminary stage and may change considerably before it is enacted. There is no indication when exactly the Bill is expected to be published but it is listed as “priority legislation for publication” by the Department of Justice.

The most notable features of the Bill are the new powers and enforcement procedures. Greater investigative powers have been proposed for authorised officers of the DPC and it is proposed that the DPC will have the power to apply on an ex parte basis to the High Court to suspend or restrict the processing of Personal Data where there is an urgent need to protect the rights and freedoms of Data Subjects.

2. Emerging Privacy Issues and Trends

Digital Age of Consent

In July 2017, the Irish Government, following public consultation, set the digital age of consent for children at 13 years of age, which is at the lower end of the scale permitted by the GDPR. This is the age of consent for children to sign up to information society services without parental approval and the Bill contains an enabling provision with respect to this age.

The Data Protection Commissioner issued new guidance on Location Data

The DPC published detailed guidance on location data aimed both at individuals and organisations. Location data is any information which links
an individual to a particular place. Recent developments in technology have made it increasingly easier for services and devices to collect an individual’s location data.

- The guidance notes that location data relating to individuals is very likely to constitute Personal Data and could constitute Sensitive Personal Data. The DPC stressed that Data Controllers have a responsibility to minimize the amount of data collected, processed and retained because of risks posed by linked location data and that informed consent is the most appropriate basis for processing personal location data in most cases.

Data Protection Commissioner Annual Report for 2016

- In April 2017, the DPC published her Annual Report for 2016. It highlighted key developments and activities of her Office last year, as well as priorities for 2017, which were noted as being “all about GDPR readiness”.

- The report noted an increased number of queries, complaints and data breach notifications. The DPC has continued her engaged approach to regulation, engaging extensively with multinational companies on proposed new policies, products and services. The DPC also engaged with a number of entities in the public, health and private/financial sectors and as many as 50 audits and inspections were carried out during the year on a wide range of public bodies and private entities.

3. Law Applicable


- The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, implemented the ePrivacy Directive 2002/58/EC.

- The EU Regulation 2016/679 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (“GDPR”). The GDPR will come into force on 25 May 2018.

- The Data Protection Bill 2017 (to date only a General Scheme of the Bill has been published. It is expected that the full Bill will be published in late 2017.).
4. Key Privacy Concepts

a. Personal Data

The DP Acts apply to the processing of any data (“Personal Data”) relating to an identified or identifiable living individual (“Data Subject”). Personal Data is defined under the DP Acts as data relating to a living individual who is or can be identified either from the data or, most notably, from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller. Where the disclosure or receipt of data does not include Personal Data as defined, then such processing falls outside the scope of the legislation.

The ODPC has issued guidance stating that in order for the processing of Personal Data to be considered fair for the purposes of the DP Acts, certain information must be provided to an individual. It covers any information that relates to an identifiable, living individual. There are different ways in which an individual can be considered “identifiable”. A person’s full name is an obvious likely identifier but a person can also be identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms, occupation, or an address.

The GDPR broadens the definition of Personal Data explicitly providing that “an identification number”, “location data” and “an online identifier” constitute Personal Data. For online identification to constitute Personal Data, a company must have additional information enabling the identification of an individual.

b. Data Processing

“Processing” is widely defined to mean performing any operation or set of operations on information or data, whether or not by automatic means. To ensure that processing is in accordance with the DP Acts, a Data Controller should obtain consent from a Data Subject to process his/her Personal Data and should give notification to the Data Subject of certain specified information. This would include information on the right of access to the Personal Data and the purposes for which the data is processed.

The definition of processing remains the same in the GDPR.

c. Processing by Data Controllers

The DP Acts apply to a person who, either alone or with others, controls the contents and use of Personal Data (a “Data Controller”).

This remains the position in the GDPR.
d. **Jurisdiction/Territoriality**
The DP Acts apply to Data Controllers in respect of the processing of Personal Data only if:

- the Data Controller is established in Ireland and the data is processed in the context of that establishment; or
- the Data Controller is established neither in Ireland nor in any other state that is a contracting party to the EEA Agreement but makes use of equipment in Ireland for processing the data otherwise than for the purpose of transit through the territory of Ireland.

The following shall be treated as “established in Ireland”:

- an individual who is normally a resident in Ireland;
- a body incorporated under the law of Ireland;
- a partnership or other unincorporated association formed under the law of Ireland; and
- a person who does not fall within any of the above, but maintains in Ireland an office, branch or agency through which he or she carries on any activity, or a regular practice.

The GDPR applies to Data Controllers and Processors who have an EU establishment and process Personal Data in the context of the activities of such an establishment.

The GDPR also applies to non-EU Data Controllers and Processors who process Personal Data of Data Subjects in the EU where the processing relates to the offering of goods or services or the monitoring of their behavior.

e. **Sensitive Personal Data**

“Sensitive Personal Data” means Personal Data relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offense, or criminal proceedings. The DP Acts set out additional requirements for the processing of Sensitive Personal Data.

The processing of Sensitive Personal Data is prohibited unless at least one of a number of stated conditions is met:

- the Data Controller obtains the explicit consent of the Data Subject;
- the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the Data Controller in connection with employment;
• the processing is necessary to prevent injury or other damage to the health of the Data Subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the Data Subject or of another person in a case where consent cannot be given by or on behalf of the Data Subject or where the Data Controller cannot reasonably be expected to obtain such consent, or the processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of, or damage to the property of another person, in a case where such consent has been unreasonably withheld;

• the processing is carried out in the course of its legitimate activities by any body corporate, or any unincorporated body of persons, that is not established, and whose activities are not carried on, for profit, and exists for political, philosophical, religious or trade union purposes, it is carried out with the appropriate safeguards for the fundamental rights and freedoms of Data Subjects, it relates only to individuals who are either members of the body or have regular contact with it in connection with its purposes and it does not involve disclosure of the data to a third party without the consent of the Data Subject;

• the information contained in the data has been made public as a result of steps deliberately taken by the Data Subject;

• the processing is necessary for the administration of justice, for the performance of a function conferred on a person by or under an enactment, or for the performance of a function of the government or a minister of the government;

• the processing is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;

• the processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality to the Data Subject that is equivalent to that which would exist if that person were a health professional;

• the processing is necessary in order to obtain information for use, subject to and accordance with the Statistics Act, 1993, only for statistical, compilation and analysis purposes;

• the processing is carried out by political parties, or candidates for election to, or holders of, elective political office, in the course of electoral activities for the purpose of compiling data on people’s political opinions and complies with such requirements (if any) as may be prescribed for
the purpose of safeguarding the fundamental rights and freedoms of Data Subjects;

• the processing is authorized by regulations that are made by the Minister for Justice, Equality and Law Reform and are made for reasons of substantial public interest;

• the processing is necessary for the purpose of the assessment, collection or payment of any tax, duty, levy, or other moneys owed or payable to the state and the data has been provided by the Data Subject solely for that purpose; and

• the processing is necessary for the purposes of determining entitlement to or control of, or any other purpose connected with the administration of any benefit, pension, assistance, allowance, supplement or payment under the Social Welfare (Consolidation) Act 1993, or any non-statutory scheme administered by the Minister for Social Protection.

The GDPR broadens the definition of Sensitive Personal Data. It will include genetic data and biometric data. Data concerning criminal convictions will no longer be classified as Sensitive Personal Data, but will continue to benefit from special protection. Sensitive Personal Data will still be afforded more protection and require more stringent conditions to be satisfied in order to legitimize its processing.

f. Employee Personal Data

The DPC has published guidance notes in relation to employment issues and while they are not legally enforceable they would be taken into account by the courts when enforcing the DP Acts. These notes are a practical guide as to how the ODPC considers employers can comply with the DP Acts in relation to employee data and cover areas such as access requests and HR, staff monitoring, considerations when vetting prospective employees, biometrics, whistle-blowing and transfer of ownership of a business.

While the ODPC accepts that organizations have a legitimate interest to protect their business, reputation, resources and equipment, the monitoring of employees must comply with the transparency requirements of the DP Acts. Any monitoring must be a proportionate response by an employer to the risk he or she faces, taking into account the legitimate privacy and other interests of workers. The DPC recommends that at a very minimum, staff should be aware of what the employer is collecting on them (directly or from other sources). Staff have a right of access to their data under the DP Acts.

The employer is generally able to justify processing non-sensitive Employee Personal Data without the need to obtain the employees’ consent. It can do so, for example, if:

• it is necessary to perform the employment contract;
• it is necessary to comply with a legal obligation;
• it is necessary to prevent injury or damage to the health of the Data Subject or to prevent serious loss or damage to the property of the Data Subject; or
• it is in the employer’s legitimate interests and does not unduly prejudice the employee’s right to privacy or other rights.

However, these legitimate interests cannot take precedence over the principles of data protection, including the requirement for transparency, fair and lawful processing of data and the need to ensure that any encroachment on an employee’s privacy is fair and proportionate. A worker can always object to processing on the grounds that it is causing or likely to cause substantial damage or distress to an individual.

If the information being processed is sensitive, explicit consent must be obtained, unless certain limited exceptions apply such as:
• the processing is necessary to perform or exercise any right or obligation imposed by law in connection with their employment;
• the processing is necessary for the purpose of or in connection with legal proceedings or to obtain legal advice; or
• the processing is necessary to establish exercise or defend legal rights.

Due to the more stringent requirements for obtaining valid consent under the GDPR (see Section 5 below), it will be preferable for employers to rely on legitimate interests as their basis for legally processing Personal Data.

5. Consent

a. General

Consent is not defined in the DP Acts. In practice, while consent of the Data Subject to process Personal Data is not mandatory, it is contemplated as a justification for its processing and is often one of the more straightforward ways to justify processing. Written consent is not required and in certain circumstances it may be implied. In addition, the Data Subject also has the right to withdraw consent at any time.

In July 2011, the Article 29 Working Party issued an opinion paper on the definition of “consent” as used in the Data Protection Directive (95/46/EC) and the ePrivacy Directive.

The GDPR provides more stringent conditions for relying on consent. The GDPR defines consent as “any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which he or she, by a
statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

b. Sensitive Data

If the information being processed is sensitive (relating to race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life or commission or alleged commission of or a prosecution for an offense) and consent is relied upon to justify the processing of Sensitive Personal Data, it must be explicit and must be obtained prior to processing, unless certain limited exceptions apply. The ODPC has clarified that explicit consent means clear, unambiguous and freely given.

The GDPR continues to require “explicit consent” for the processing of sensitive data however the distinction between “explicit consent” and standard consent is less clear, given the increased requirements for valid standard consent.

c. Minors

The DP Acts do not specify a minimum age at which a child can provide valid consent to having their Personal Data processed. Where a person is under the age of majority (18), the DP Acts require the Data Controller to make a judgment on whether the young person can appreciate the implications of giving consent. The ODPC has issued useful guidance on the issues concerning the age of consent.

Specifically in relation to the right of access to health data, the guidance recommends that the general practitioner use professional judgment when deciding whether the entitlement to access should be exercisable by (i) the individual alone, (ii) a parent or guardian alone, or (iii) both. In making a decision, there is a suggestion that particular regard should be had to the maturity of the young person concerned and his or her best interests.

According to the ODPC, where marketing to young people is involved, a person under 18 could be expected to understand the implications of giving consent in suitable cases. It should be considered whether someone under 18 could be expected to understand the implications of giving consent to processing of their Personal Data in order to avail of a particular product or service. Otherwise, the consent of a parent or guardian should be obtained and suitable authentication measures adopted to make sure that such consent is genuine.

The GDPR includes more stringent conditions for information society services (e.g., online businesses) to rely on consent to process children’s Personal Data. It requires such service providers to obtain, and make reasonable efforts to verify parental consent to the processing of a child’s data, where the child is below the age of 16 years old. In July 2017, following public
consultation, the Irish Government set the digital age of consent for children at 13 years of age.

d. Employee Consent
Traditionally Irish employers have relied on consent for processing Personal Data and Sensitive Personal Data. However, the guidance of the Article 29 Working Party sets out the view that consent is not particularly easy to achieve and that the other justifications (see Section 4(f)) should always be considered in preference to consent. The ODPC issued some guidance in respect of consent and the obtaining of medical data in the employment context. An employer would not normally have a legitimate interest in knowing the precise nature of an illness and would therefore be at risk of breaching the DP Acts if they sought such information. The consent of the employee may not allow the disclosure of such information to an employer as there is a doubt as to whether such consent could be considered to be freely given in such circumstances.

Given new requirements under the GDPR it will be preferable for employers to effectively communicate their justifications for processing Personal Data to employees through either a privacy notice or accompanying privacy policies rather than basing their data processing on consent.

e. Online/Electronic Consent
Electronic consent will suffice if appropriate safeguards are taken to ensure a Data Subject is aware of the Data Controller's data processing notice and has granted consent on that basis (e.g., inclusion of a hyperlink directly above a consent button) and to prevent consent by mistake (e.g., a double-click acceptance process). The Data Controller should be able to evidence that such safeguards have been put in place (e.g., the Data Controller should be able to demonstrate that the user was provided with sufficient notice and that consent was informed and voluntary).

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to contact the privacy officer or person accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; and the means of transmission of the Personal Data.

The GDPR provides a list of specific, additional, information that must be provided to Data Subjects to ensure all processing activities are transparent.
This list includes, in particular, the legal basis for the processing and the data retention period or criteria used to determine same.

7. Processing Rules

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

In a significant change from the DP Acts, the GDPR imposes direct statutory obligations on Data Processors. This means processors are subject to direct enforcement by supervisory authorities, serious fines, and direct liability to Data Subjects for any damage caused by breaching the GDPR. The statutory obligations imposed by the GDPR on processors include among others:

- Not to engage a sub-processor without the prior written authorization of the controller;
- Only process data in accordance with the instructions of the controller;
- Maintain records of data processing activities and make same available to the supervisory authority on request;
- Take appropriate security measures and inform controllers of any data breaches;
- In specified circumstances, designate a data protection officer

The GDPR also imposes more prescriptive obligations in regard to the terms of a data processing contract, requiring certain mandatory terms be included.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject's Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject's Personal Data; and request the deletion and/or destruction of the Data Subject's Personal Data.

In the GDPR these rights are reflected however there is a requirement that specific, additional, information be provided to Data Subjects when responding to access requests including informing the Data Subject of their right to rectification, erasure, restriction or objection to the processing of their data and informing the Data Subject of their right to complain to the relevant supervisory authority.
9. Registration/Notification Requirements

An organization that collects and processes Personal Data is required to register with the local data authority.

Due to the new concept of accountability in the GDPR, Data Controllers will no longer have to register or notify supervisory authorities of their processing activities. Instead, Data Controllers will have to implement appropriate technical and organisational measures to demonstrate that their data processing is performed in accordance with the GDPR.

10. Data Protection Officers

In Ireland, there is currently no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

The GDPR provides that Data Protection Officers (DPOs) must be appointed if you are a public body; your primary activities involve large-scale processing of sensitive data, data relating to criminal convictions, or systematic monitoring of Data Subjects. A DPO can be an employee or a contractor, but should have expert knowledge of data protection law.

11. International Data Transfers

The transfer of Personal Data out of Ireland is particularly topical in light of recent developments. The transfer of Personal Data from Ireland to the EEA is uncontroversial; Member States are generally permitted without the need for further approval. Transfers are also permitted to Canada (for certain types of Personal Data), Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Andorra, Israel, Switzerland, New Zealand and Uruguay, which are the subject of the European Commission’s findings of adequacy (subject to the fulfilment of certain preconditions) in relation to their data protection laws.

Until October 2015, transfer to the US was permitted where the recipient had signed up to the US Department of Commerce’s Safe Harbor Privacy Principles. Any US organization that was subject to the jurisdiction of the Federal Trade Commission could participate in Safe Harbor. However in October 2015 Safe Harbor was struck down as inadequate by the European CJEU following an Article 267 preliminary reference from the Irish Courts. Following the decision, the EU and the US were given a three-month timeline to agree a new regime to replace Safe Harbor. The EU/US Privacy Shield was announced in February 2016 and adopted by the European Commission on 12 July 2016.

The adoption of Standard Contractual Clauses approved by the European Commission will also provide an adequate level of protection to justify the transfer. (Note that the Data Controller must in any event justify all of its data
processing under the DP Acts; justification of any transfers is an additional compliance requirement.) Unlike many other EU Member States, if a transfer contract is used it will not need to be filed or approved by the DPC, whether before or after any transfers take place. However, following the Schrems decision detailed above, the validity of the Standard Contractual Clauses has been called into question. Maximillian Schrems submitted a complaint to the ODPC questioning the legality of Standard Contractual Clauses. This complaint has resulted in the ODPC seeking a reference from the Irish High Court to the CJEU regarding their validity. This case was heard in February 2017 and in October 2017 the High Court ruled in favor of referring the matter to the CJEU.

Subject to the specific authorizations mentioned above, Personal Data may not be transferred to countries outside the EEA unless the destination country provides adequate protection of the Personal Data. Exceptions to this general prohibition are, however, expressly contemplated under the DP Acts, including where:

- the transfer of Personal Data is required or authorized by law;
- the Data Subject has consented to the transfer;
- the transfer is necessary to perform a contract with the Data Subject, or to take steps at his request with a view to entering into a contract with him;
- the transfer is necessary for the conclusion or performance of a contract entered into between the Data Controller and third parties in the interests of, or at the request of, the Data Subject;
- the transfer is necessary for reasons of substantial public interest;
- the transfer is necessary for obtaining legal advice or in connection with legal proceedings;
- the transfer is necessary to prevent injury or other damage to the Data Subject’s health, or to prevent serious damage to his or her property, or to protect his or her vital interest in some other way, provided that it is not possible to inform the Data Subject, or to obtain his or her consent, without harming his or her vital interests;
- the Personal Data to be transferred are an extract from a statutory public register; or
- the transfer has been specifically authorized by the ODPC where the Data Controller can point to adequate data protection safeguards, such as approved contractual provisions.
Where multinational organizations are transferring personal information outside the EEA, but within their group of companies, they may also adopt Binding Corporate Rules ("BCRs") as a means of justifying such intra-group transfers. BCRs provide adequate safeguards for the protection of privacy with regard to all transfers of Personal Data protected under European law. Acceptable BCRs may include intra-group agreements, policies or procedures, and special arrangements among the group of companies that afford the requisite protection.

The ODPC and 20 other DPAs across the EEA have agreed to mutually recognize BCRs approved by one of these 21 DPAs. For BCRs to enable the transfer of personal information freely within a corporate group, they must be approved by at least one DPA that has agreed to mutually recognize BCR applications, and by any remaining DPAs in EEA countries from which the organization transfers Personal Data and which have not agreed to mutual recognition of BCR applications. The Article 29 Working Party has adopted a model checklist and table setting out the required contents of an application to a data protection authority for approval of proposed BCRs.

In January 2012, the ODPC approved Intel Corporation’s BCRs in conjunction with other EU DPAs. The ODPC highlighted how BCRs are a valuable tool for entities to embed privacy principles into their business practices and to comply with EU data protection requirements.

The GDPR largely leaves the position regarding international transfers of data unchanged. The GDPR prohibits the transfer of data to a third country (i.e., a country outside the EEA) unless that country ensures an adequate level of protection. The ODPC will retain the ability to decide that a third country or a specified sector within that country or international organization ensures an adequate level of protection.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

This remains the same under the GDPR.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case
of the occurrence of a data breach, the outsourcing organization may be held liable together with the third-party provider.

As outlined above, the GDPR imposes direct statutory obligations on outsourced service providers and imposes prescriptive obligations in regard to the terms of a data processing contract.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

This remains the same under the GDPR. The GDPR also allows for processors to be subject to direct enforcement by supervisory authorities, fines and compensation claims by Data Subjects.

15. Data Security Breach
Under the Privacy Regulations, “publicly available communications services” providers (such as telecommunications companies and ISPs) are required to report all incidents in which Personal Data has been put at risk as soon as the Data Controller becomes aware of the incident, except when the full extent and consequences of the incident have been reported without delay directly to the affected Data Subject(s), it affects no more than 100 Data Subjects and it does not include Sensitive Personal Data or Personal Data of a financial nature. The ODPC has the ability to audit relevant organizations to assess their compliance with these guidelines and instructions.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions, class actions, and/or a criminal prosecution.

The GDPR introduces a new mandatory obligation requiring controllers to notify data breaches to the relevant supervisory authority “without undue delay, and where feasible, not later than 72 hours after having become aware of it”. If notification is not made after 72 hours, a reasoned justification for the delay must be provided. However, it is not necessary to notify the supervisory authority where “the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons”.

The GDPR also requires Data Controllers to notify Data Subjects of data breaches, without undue delay, where the breach is likely to result in a high risk to the rights and freedoms of natural persons.

A processor is will be obliged to inform the controller of a data breach without undue delay, but has no other notification obligation.
16. Accountability

There is no existing law in Ireland that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

The GDPR introduces a new principle of accountability. Data controllers will be required to demonstrate how they comply with the data protection principles. It will be mandatory for controllers and processors to maintain records of processing activities and to make them available to the supervisory authority on request. Only organisations with less than 250 employees are exempt from this obligation (unless the processing carried out is likely to result in a risk to the rights of Data Subjects, the processing is not occasional, or the processing includes sensitive data or data relating to criminal convictions).

17. Whistle-Blower Hotline

The general filing requirement under the DP Acts still currently applies, and any whistle-blower hotline will constitute one of the Data Controller’s data processing activities in Ireland. That must be covered in its filing (i.e., registration) with the ODPC. The employees should also be informed (in a written policy typically) as to how the data will be processed as part of the hotline procedure.

The ODPC has issued specific guidance in respect of whistle-blowing and how to ensure compliance when Personal Data is involved. A best practice approach for an organization introducing a whistle-blowing scheme is to arrange, where possible, that the data produced from such a scheme refers to issues as opposed to individuals.

18. E-Discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of said system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace.
20. Cookies

Organizations may not simply provide website users with the opportunity to “opt out” of the use of cookies, but are now required to obtain the consent of the user to the organization’s storage of cookies on their device.

The Privacy Regulations prohibit the use of an electronic communications network to store information or gain access to information already stored in the terminal equipment of a subscriber or user unless the individual (i) has been given clear and comprehensive information about why this is being done and (ii) has given consent. Information that is necessary to facilitate the transmission of a communication, or information that is strictly necessary to provide an information society service explicitly requested by the user, is not subject to this requirement.

The ODPC issued guidance setting out that in order to meet the legal requirements such settings would require, as a minimum, clear communication to the user as to what they are being asked to consent to in terms of cookies usage and a means of giving or refusing consent to any information being stored or retrieved. It is particularly important that the requirements are met where third party or tracking cookies are involved.

Unlike other jurisdictions, there was no formal compliance grace period in Ireland. In December 2012, the ODPC issued correspondence to 80 Irish companies requesting information on how they are complying with the revised rules for cookies, providing 21 days to outline the steps that have been taken to ensure compliance. The ODPC made specific reference to its powers of enforcement in the event of non-compliance.

In December 2013, the ODPC issued updated guidance on the use of cookies. In respect of cookie usage, the ODPC indicated that it would be satisfied with a prominent notice on the homepage of a website informing users about the website’s use of cookies with a link to a cookie statement containing information sufficient to allow users to make informed choices, together with an option to manage and disable the cookies. From a practical perspective they set out certain minimum requirements for website operators to adhere to as follows;

1. Consent – consent of the user must be captured and may be obtained explicitly through the use of an opt-in check box or may be obtained by implication.

2. Notification – consent should be sought as part of a prominent notification displayed on entry to a website containing a link to a cookie statement which should outline in further detail how the website makes use of cookies.
3. **Cookies Statement** – this statement should contain clear and comprehensive information on the types of cookies, how cookies are used and details on how to remove them.

4. **Third Party Cookies** – it is not sufficient to simply refer a user to third-party websites. The cookie statement should ideally contain information as to the type of cookies, their name, a description of their purpose, their expiry dates and a link to advertising networks’ opt-out mechanisms for third-party cookies.

21. **Direct Marketing**

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.

Please note that the current laws applicable to direct marketing will be subject to change on the introduction of the proposed regulation relating to e-privacy issues which, when adopted, will replace the existing ePrivacy Directive 2002/58/EC.
Israel

Nurit Dagan
Tel Aviv
Tel: +972 3 692 7424
dagan@hfn.co.il

Ohad Elkeslassy
Tel Aviv
Tel: +972 3 692 7424
elkeslassy@hfn.co.il
1. Recent Privacy Developments

The Protection of Privacy Law, 1981 (the “Privacy Law”) regulates the issue of protection of privacy in general, and the matter of protection of privacy in computer databases in particular. The Registrar of Databases (the “Registrar”), which is part of the Israeli Law Information and Technology Authority (“ILITA”), is responsible for the enforcement of the Privacy Law. In accordance with the Registrar’s role, the Registrar has issued from time to time various guidelines which set out ILITA’s interpretation of the Privacy Law and operative instructions and also various recommendations for the general public.

In this regard, below is a brief outline of some of the principles contained in recent guidelines and draft guidelines issued by ILITA:

- In August 2017, ILITA published a draft directive regarding the handling of Personal Data that is being transferred during the course of M&A transactions (e.g., acquisition or merger of companies). The draft directive prescribes cases in which consent of Data Subjects (opt-out or opt-in) will be required for the transfer and determines the manner and form in which the transfer of Personal Data should be disclosed to the Registrar. It should be noted that the draft directive has only been published for the public’s comments and accordingly, the final contents of the directive as well as the date in which it will come into force, if at all, are unclear at this stage in time.

- On 9 August 2017, the Privacy Protection Regulations (Fees) (Cancellation), 2017 were officially published. These regulations cancel the Privacy Protection Regulations (Fees), 2000 and accordingly, as of the date of such publication, annual fees and registration fees for databases no longer apply.

- In June 2017, ILITA published a directive regarding the interpretation and implementation of the Privacy Law provisions relating to Direct Marketing and Direct Marketing Services¹. With respect to consent, the directive states that, in general, consent for direct marketing and direct marketing services should be on an opt-out basis, unless the inclusion of the data pertaining to a Data Subject in the database was by way of breach of the Privacy Law. However, the directive further states that the use of information relating to a Data Subject, which has been obtained during a relationship between a client and a service provider to which a standard

---

¹ “Direct Marketing” is defined as “approaching a specific person based on his/her belonging to a group of the population that is determined by one or more characteristics of persons whose names are included in a database.” “Direct Marketing Services” is defined as “providing Direct Mailing services to others by way of transferring lists, labels, or data by any means.”
contract (a contract which has been pre-determined by one party in order for it to be used in several agreements between that party and an undetermined and unspecified number of other parties) applies, for the purpose of Direct Marketing Services which has no linkage to the transaction requires an opt-in consent of the Data Subject. The directive further determines the ways to implement the right of the Data Subject to know the sources of the information regarding him/her contained in the database, the manner in which the Data Subject can delete information regarding him/her from the database, etc.

- In February 2017, a non-governmental draft bill initiated by a few members of the Israeli parliament (the Knesset) was issued, titled “The Draft Bill Protection of Privacy Law (Amendment – Protection of Privacy of Minors), 2017”. The bill aims to determine stricter rules regarding the collection and use of personal information pertaining to minors. It should be noted that, currently, this draft bill is at the very early stages of its enactment process and accordingly it is unclear whether and when it will be enacted, and what will be its final version.

- In January 2017, ILITA published a directive titled “The Application of the Provisions of the Protection of Privacy Law on the Right to Inspect Voice Calls, Video Footage and Other Types of Digital Information”. The aim of the directive is to clarify the right of Data Subjects to inspect voice calls, chat correspondences, filmed video calls etc., that have been digitally stored by businesses and other entities that provide service to the public (“Digital Information”) and how the Registrar interprets the Privacy Law in order to apply its authority to implement the right to inspect Digital Information. The directive states that Digital Information held by magnetic or optical means and intended for computer processing is considered a database and all the provisions of the Privacy Law regarding databases apply to it. The directive further states that the provisions of the Privacy Law, and particularly the provision which grants the right to inspect data, apply to all types of data which are stored in a digital form, including voice recordings of telephone conversations and video footage. The directive also states that the right of a Data Subject to review Digital Information should be carried out by delivering the digital files in a form which can be read, listened to or viewed (as the case may be), through publicly available software.

- In October 2016, ILITA published guidelines addressing the issue of acquisition of databases for the purposes of marketing, sales promotions, market research, etc. in these guidelines, ILITA prescribes “rules of thumb” for all those considering acquiring databases, in order to ascertain the validity of the database and the consents granted by those whom information is included in the database.
In August 2016, ILITA published a draft directive titled “The Use of Surveillance Cameras in the Workplace and within the Framework of Labor Relations”. This directive is offered as a supplemental chapter to ILITA’s general guidelines regarding the use of surveillance cameras (as further detailed below). The draft directive clarifies the Registrar’s position regarding the use of surveillance cameras in the workplace and determines, for example, that installation of surveillance cameras should be made only for legitimate purposes of the employer; the employer should obtain the employees’ explicit consent for the use of the surveillance cameras (as opposed to the general guidelines pertaining to the use of surveillance cameras which require a notification sign only); the employer should establish a clear and detailed policy regarding the use of surveillance cameras after consulting with the employees or their representatives; and the use of footages for purposes which are different from the purpose which has been pre-determined is prohibited. It should be noted that the draft directive has only been published for public comment and, accordingly, the final contents of the directive as well as the date in which it will come into force, if at all, are unclear at this stage in time.

In June 2016, a non-governmental draft bill initiated by a few members of the Knesset was issued, titled “The Draft Bill Protection of Privacy Law (Amendment – Right to be Forgotten), 2016”. The bill, which follows the ruling of the Court of Justice of the European Union, aims to provide Israeli courts with the authority to instruct a website (or in some cases – ISPs) to remove publications and links containing content which infringes an individual’s privacy, from the internet (or from any other electronic communication network). It should be noted that, currently, this draft bill is at the very early stages of its enactment process and accordingly it is unclear whether and when it will be enacted, and what will be its final version.

In May 2015, a non-governmental draft bill initiated by a few members of Parliament was issued, titled “The Draft Bill Protection of Privacy Law (Amendment – Report on Security Breach in a Database), 2015”. The purpose of this draft bill is to require the owner or holder of a database to report cases of breaches of their databases to Data Subjects and to the Registrar, and in addition, to authorize the Registrar to impose fines in this regard. It should be noted that, currently, this draft bill is at the very early stages of its enactment process and accordingly it is unclear whether and when it will be enacted, and what its final version will be (similar non-governmental draft bills were issued in February 2012 and October 2013). However, we note that on May 2017 the Protection of Privacy Regulations (Information Security), 2017 were enacted. These Regulations which will come into force on 8 May 2018 include
requirements with respect to data breach notifications and therefore may cause the above draft bill to be redundant.

- In April 2015, ILITA published a Privacy Impact Survey – a tool designed to be used by an organization in order to identify and reduce the risk of privacy violation in establishing and managing new projects that have an impact on privacy. The survey should be performed in the early stages of the privacy by design process conducted by an organization. The survey analyzes the processes for collecting and processing Personal Data and risk management in connection with such data.

- On 6 October 2015, the European Court of Justice ruled (in the case of Schrems v. Data Protection Commissioner) that the EU Commission decision approving the “Safe Harbor Framework” – which governs the sharing of Personal Data from the EU to US-based companies which have engaged in the self-certifying “Safe Harbor” scheme – is invalid (the “Ruling”). In view of the Ruling, on 15 October 2015, ILITA announced that it revoked its prior permission of the transfer of Personal Data from Israel to organizations in the United States that have been self-certified under the Safe Harbor Arrangement. On 4 January 2016, ILITA announced that in light of the continuous negotiations between the representatives of the US and the EU to conclude an agreement to replace the Safe Harbor arrangement, for the time being, ILITA does not initiate enforcement actions in connection with data transfers under Section 2(8)(2) of the Transfer Regulations (as detailed under Section 3(11) below). As of 20 September 2017, ILITA has not issued any further instructions with respect to the Privacy Shield.

2. Emerging Privacy Issues and Trends

Protection of privacy is a developing area in Israel, and it has become more and more predominant, both due to the technological developments, which create new risks to privacy (such as social networks, e-commerce, etc.), and the active role taken by ILITA and the Registrar including by increasing the enforcement of the Privacy Law and by raising the public’s awareness to privacy matters.

Some examples of enforcement actions that were taken by the Registrar are published on ILITA’s website, and they include:

i. imposing administrative fines on companies that used or transferred information from their databases for purposes other than those for which the databases were established;

ii. imposing an administrative fine for engaging in direct marketing activities in contravention of the requirements of the Privacy Law; and
iii. determining a breach of the Privacy Law in cases where owners of
databases failed to comply with the requirement to employ adequate data
security measures.

In addition, the Registrar has issued many guidelines in which the Registrar
sets out the authority’s interpretation of the Privacy Law with respect to
various privacy-related fields. Set out below is a brief reference to all of these
guidelines.

Furthermore, there are also draft laws and guidelines which to date have still
not been enacted or approved. These legal developments demonstrate a
focus on strengthening the powers of the Registrar, ensuring the security of
databases, and developing privacy awareness in various fields. Section 1
above and the points below set out, in brief, some of the principles outlined in
such draft legislation and guidelines. It should be noted that currently, the draft
legislation and guidelines indicated below are at the early stages of the
enactment or approval process, as applicable, and accordingly it is unclear
whether or when they will be enacted or approved, and what their final
versions look like.

i. On 18 December 2012, ILITA published a statement of opinion with
respect to the use of biometric attendance control systems in the
workplace. Under such statement, an employer must: (a) first justify the
selection of a means which infringes privacy, in light of other alternatives
which may cause less harm to the privacy and, if such justification exists,
use such means in a proportional manner; (b) refrain as much as possible
from storing biometric information in a database (the storage of such
information in “smart keys” is advisable); and (c) in the event where there
is no other alternative but to store biometric information in a database –
employ strict data security measures. The legal status of the above-
mentioned statement is not clear but it indicates how the Registrar
interprets the use of biometric attendance systems in the workplace, in
light of the Privacy Law.

In March 2017, with respect to the use of the biometric attendance
systems in the workplace, the Israeli National Labour Court has ruled (in
the Qalansawe case) that a person’s fingerprint constitutes private
information and that the use of a biometric attendance system harms the
employees’ right to privacy and their right to autonomy, and
consequently, an employer’s right will only triumph above its employees’
right to privacy in the following two cases: (a) by law (currently there is
none); or (b) by consent.

The National Labour Court determined that a balance must be achieved,
between the right to privacy in the workplace, and the employer’s
managerial privilege in the workplace, which includes the right to set clear
policies; the principle of transparency; the involvement of the employees
in the setting of policies and the anchoring of such in employment agreements; and, maintaining the principle of proportionality and the principle of legitimacy.

The National Labour Court further ruled that consent of the employees must be informed and free willed, such that it will not negate “public policy” (the fundamental values underlying Israeli society and the Israeli judicial system), and should be examined separately with respect to each individual employee. Any direct or indirect coercion on the employees to agree to the use of their fingerprint, including by way of imposing sanctions due to their refusal, will taint the free will required in this respect.

In addition, the Court stated that employers that would like to obtain their employees’ consent for the use of their fingerprint, must present the employees with comprehensive information on the matter, including a detailed explanation of what exactly will be “taken” from them; who will take the fingerprint, and what is their training; will the fingerprint be kept in a database; who is in charge of the database and who has access thereto; is the information held in the database in proximity to other identification details; do external factors have access to the database; can the fingerprint be copied; how does the employer ensure that the information in the database is properly safeguarded; how and when is the data deleted from the database, etc.

ii. Protection of privacy on the internet: ILITA has published recommendations addressed to the general public with respect to using the internet. Such recommendations are intended to raise awareness and provide general tools for coping with the disclosure of personal information on social networks, security risks relating to one’s personal computer, the use of smart phones and downloading applications, tracking activities on the internet, and internet scams.

iii. Guideline No. 4-2012, dated 21 October 2012, titled “The Use of Security and Surveillance Cameras and the Use of Databases Containing Pictures Taken by Those Surveillance Cameras”. Under this guideline, the Registrar addresses the application of the Privacy Law with respect to the use of Surveillance Cameras in public areas.

The guideline provides guidance with respect to using Surveillance Cameras and choosing the specific location of such Cameras, the coverage they provide and their specific functionalities. The guideline also states that the public must be informed as to the use of the Surveillance Camera, including by way of placing clear and readable signs and the contents of such warning signs (including, for example, the name and contact details of the organization that installed the Camera, the purpose for which it was installed, etc.). The guideline also sets out instructions
with respect to the period of retention of the pictures and their deletion, the rights of inspection of the pictures by those who have been captured on the cameras, various security requirements with respect to the database of pictures, and limitations on the uses of the database.

iv. Guideline No. 3-2012, dated 29 July 2012, titled “The Application of the Privacy Law on Databases Owned by Private Agencies for Placing of Foreign Employees in the Nursing Field”. The purpose of this guideline is to protect the privacy of people who require the services of foreign workers in the nursing field, as these people are usually among the weaker and more vulnerable persons in the general population. The guideline sets out the requirements of the applicable private agencies with respect to: registering databases, receiving applicable consents, the uses and transfer of the Personal Data, use of data for direct marketing, data security, and conditions of retaining data upon the termination of the services.

v. Guideline No. 2-2011, dated 10 June 2012, titled “Use of Outsourcing Services for Processing of Personal Data”. This guideline refers to any outsourcing to third parties for the processing of Personal Data from an Israeli database.

vi. Guideline No. 2-2012, dated 28 February 2012, titled “The Application of the Provisions of the Protection of Privacy Laws on Processes for Screening Applicants for Employment Purposes and the Activities of Employee Screening Centers”. This guideline sets out various requirements. For instance, it establishes the requirement to register a database with respect to the information collected during the employee screening process, access rights with respect to such a database, limitations on the uses of the database, the requirement to receive the applicant’s consent to any use of the information, the requirement that the use be subject to general criteria determined by labor law and relevant case law, the requirement that use of the personal information be proportionate and reasonable, the requirement that access rights with respect to the screening information (including test results) be granted, and the obligation to delete the information or render it anonymous when it is no longer necessary for its applicable purpose.

This guideline has been scrutinized by many screening centers and by the Organization of Psychologists. These organizations have filed petitions with courts against the Registrar and this guideline. During 2013, such petitions were settled and ILITA published an update to the guideline. This update provides, among other things, that access rights granted to the applicant will not include access to certain types of data, including: (a) details relating to the potential employer; (b) specific characterizations of the job; and (c) analysis of the suitability of the
applicant and his/her qualities and personality to the job specifications based on the details set out in (a) and (b) above.

vii. Guideline No. 1-2012, dated 27 February 2012, titled “The Application of the Provisions of the Protection of Privacy Law on Databases of Public Transportation Operators using “Smart Cards””. Smart Cards are electronic tickets used for most means of public transportation. They are issued in accordance with certain applicable transportation legislation. This guideline refers to the information collected by public transportation operators for the purpose of issuing Smart Cards and through the use of Smart Cards by passengers. The guideline refers to matters such as: the registration of applicable databases and data security, receipt of informed consent from the passengers to the collection, processing and transfer of the information, and permitted uses of the information.

viii. Guideline No. 1-2011, dated 20 September 2011, titled “Prohibition on the Use of Information Regarding Attachments Imposed on a Third Party”. This Guideline clarifies that a third party (such as a bank, insurance company, etc.) is not permitted to use information regarding the imposition of an attachment on the assets of a debtor that have come to such third party’s knowledge due to an attachment order that was submitted to the third party other than for the purpose stated in the order, without the prior informed consent of the debtor.

ix. Guideline No. 1-2010, dated 20 May 2010, titled “Minimum Requirements of Processes for Identity Verification of a Data Subject for the Purpose of Providing Access to Information About Him in a Database”. This directive imposes requirements for identity verification methods to be used when enabling “remote access by a Data Subject to the Data Subject’s Personal Data stored in a database”. The directive requires that the verification process solicit from the Data Subject at least one item of data which should only be known to the Data Subject (and which is not included in the list of particulars contained in an illegal copy of the population registry (which was illegally distributed), as detailed under the guideline). The number of verification items required should rise in accordance with the sensitivity of the data, or alternately, other measures could be employed, such as identity verification by means of a SIM card, cellular phone or biometric characteristic. Failure to correctly assess the sensitivity of the data and adjust the requirements accordingly constitutes a breach of data security obligations.

x. Guideline No. 1-2009, dated 18 November 2009, titled “The Application of the Duties under the Law in Medical Databases used by Sick Funds and Medical Service Providers”. This directive determines that in the event that medical information is being stored by a service provider, in accordance with a contractual engagement vis-à-vis a certain Sick Fund
(which are the Israeli equivalent of HMOs), the owner of the database in which the medical information is being stored should be the Sick Fund itself and not the service provider.

xi. In 2013, ILITA updated its forms for registration of databases which are required to be registered under the Privacy Law and for updating registration details. The new and amended application forms are more comprehensive and require the applicant (i.e., the owner of the database) to provide more detailed information than was previously required, such as the sources of the data, information concerning third parties to whom information is transferred, the database’s infrastructure, etc.

xii. On 9 December 2014, 26 Data Protection Authorities worldwide (Israel among them) issued an open letter to operators of app marketplaces (including Apple), urging them to require each app to provide specific and direct links to privacy policies applicable for apps that collect personal information.

xiii. In November 2011, the government published a draft bill titled “Draft Bill Protection of Privacy Law (Amendment No. 12) (Enforcement Powers), 2011” (the “Draft Enforcement Powers Bill”), as part of its efforts to improve the supervisory and enforcement powers of the Registrar. The Draft Enforcement Powers Bill would enable the Registrar to, among other things: issue security orders with respect to security breaches, penetrating computers, requesting the court to issue various orders, performing investigations, seizing relevant documents and other materials, conducting searches, and imposing various monetary fines. The Draft Enforcement Powers Bill proposes establishing an alternative administrative enforcement mechanism that could be used in parallel with the current enforcement mechanism under the Penal Law, 1977.

xiv. In August 2012, an initial draft of an amendment to the Protection of Privacy Law was issued for the public’s comments, titled “Reducing Registration Requirements and Determining Obligations to Maintain Management and Work Procedures and their Documentation, 2012”. The purpose of this draft bill is to loosen the requirement to register databases and to place more emphasis on improving compliance with the provisions of the Privacy Law by establishing internal procedures and enforcement of the supervisory authorities of the Registrar.

xv. In July 2013, ILITA published a draft directive titled “The Responsibility of Database Owner for Implementing Security Measures when Providing Inspection of Personal Data through a Website or by Distributing it via Email”. This draft directive sets out the obligations of the owner and holder of a database who are providing Data Subjects with the right to inspect Personal Data pertaining to the Data Subjects through a website or distributing the Personal Data through email (e.g., security measures
that should be implemented, the form of consent that should be obtained from the Data Subject, etc.).

xvi. In May 2013, ILITA published a draft guideline titled “Prohibition on Use by Banks of Information on Restricted Accounts after the Termination of the Restriction Period”. This draft guideline would, if implemented, limit the bank’s ability to use information regarding a restricted account in the event that the owner of the account was not the bank’s client during the restriction period. The draft guideline also outlines certain circumstances in which the banks should delete all information regarding restrictions on accounts.

In March 2012, ILITA published a draft directive titled “Conditions for Collection and use of ID Numbers in Databases”. Under the directive, the collection and storage of ID numbers is prohibited, unless: (a) the owner of the database has first examined (and documented the examination process) the necessity of the collection of ID numbers; (b) the Data Subject has granted his/her knowledgeable consent after being given the proper notice under the Privacy Law, including, inter alia, with respect to the intention to collect ID numbers and the purposes of such collection; (c) use of such information shall be made only for the purpose for which the information was granted; (d) the owner of the database employed strict data security measures, in a level which is no less than the one set out under the applicable regulations (as detailed in Section 3(ii) below); and (e) the information will be retained only for the necessary period of time in order to fulfill the applicable purpose for which such data was collected.

xvii. In April 2012, ILITA issued a draft guide titled “Handbook for Employers and Employees on the Protection of Personal Information at the Workplace”, for the public’s comments. The draft handbook covers various issues including employee consent limitations and requirements, uses of information, confidentiality and data security, processing of employees’ personal information during the entire period of the relationship between the parties (including with respect to applicants, employees and former employees), and monitoring of employees’ use of various technological means at the workplace.

xviii. In February 2011, the Israeli National Labor Court set a precedent as to what is or is not permitted with respect to an employer’s infiltration of its employees’ email correspondence – the Isakov case. According to such case law, monitoring employees’ email correspondence must meet several conditions: (a) principles of legitimacy – the monitoring and the use of the derived information must be limited to essential business purposes; (b) proportionality – the employer should examine and select the means which is the least harmful to the employees’ privacy; (c)
proximity of purpose – the collection of information is limited only to what is necessary in order to achieve the initial purpose for which the information was initially collected; and (d) transparency – the employer must set a clear policy regarding the technologies it intends to use in order to monitor the employees’ activity and to bring this policy to its employees’ attention.

In addition, the case law determined that the infiltration of the employee’s personal correspondence through his or her inbox should only occur as a last resort and in exceptional circumstances, where protecting the employer’s legitimate interests would justify the employee’s privacy violation. The employee’s explicit and informed consent with respect to accessing specific personal email correspondence is required.

The employer is forbidden from monitoring an employee’s use of a private mailbox (e.g., webmail like Gmail) and accessing it, both with respect to any inbox and the contents of such correspondence. If the employer believes that the monitoring of the employee’s external personal mailbox is required due to extraordinary circumstances, then it must apply to the Labor Court for an “Anton Pillar” order.

The principles of the Isakov case have been applied to additional communication means and electronic systems other than emails.

3. Law Applicable

In general, the Israeli legislation with respect to privacy issues is governed by The Basic Law: Human Dignity and Liberty (the “Basic Law”) (as Israel does not have a written Constitution, the Supreme Court of Israel has conferred constitutional status on such Basic Laws), and the Privacy Law.

While the Basic Law sets out in general terms the fundamental rights of any person to privacy and to intimacy and further protects in general the privacy and secrecy of a person’s communications, the Privacy Law and subsequent regulations set out detailed provisions for the protection of personal information (note that the Privacy Law refers to protection of privacy and of personal information of individuals only and not of entities). These include a number of substantive issues concerning, inter alia, the processing, collecting, transferring and maintaining of such information.

Below is a list of the regulations and orders which have been enacted under or in connection with the Privacy Law:

i. **Protection of Privacy Regulations (Conditions for Viewing Information and Procedural Rules for Appealing Against A Refusal to Allow Viewing)** 1981. These regulations establish the procedure for submitting an application for viewing information and the viewing process. In addition, these regulations set out the reasons according to which an owner of a
database may reject the application and how to appeal against such rejection.

ii. *Protection of Privacy Regulations (Conditions for Holding and Maintaining Information and Procedures for Transfer of Information Between Public Bodies) 1986.* These regulations include general provisions with respect to the management of databases; procedures for the transfer of information between public bodies; and rules for the management and use of databases that include restricted information. Most of the provisions of these regulations will be annulled once the Protection of Privacy Regulations (Information Security), 2017 (the “Security Regulations”) come into effect (see Section 3(ix) below).

iii. *Protection of Privacy Regulations (Designation of Databases That Include Information that May Not be Disclosed) 1987.* These regulations specify databases of particular bodies that may not be disclosed due to national security issues.

iv. *Protection of Privacy Regulations (Transfer of Information to Databases Outside the Borders of Israel) 2001.* These regulations establish restrictions and conditions for the transfer of information from an Israeli database to a recipient outside of Israel.

v. *Administrative Offenses Regulations (Administrative Fine Protection of Privacy) 2004.* These regulations determine the amount of the administrative fines which can be imposed in the event of any violation of specific provisions of the Privacy Law.

vi. *Protection of Privacy Order (Designation of Public Bodies) 1986.* These regulations set out a list of bodies to be considered as public bodies under the Privacy Law (in addition to the public bodies listed in the Privacy Law).

vii. *Protection of Privacy Order (Designation of Investigation Authority) 1998.* These regulations set out specific authorities that have investigatory powers and the databases of which are therefore not subject to viewing rights of Data Subjects.

viii. *Protection of Privacy Order (Establishment of Supervision Unit) 1999.* These Regulations establish a supervisory unit for supervision of databases, their registration and data security.

ix. *Protection of Privacy Regulations (Information Security), 2017.* These Regulations impose data security obligations on owners, holders and managers of databases, based on the level of security assigned to the database in accordance with the criteria set out under the Security Regulations (high level/medium level/basic level). These Regulations will
come into effect on 8 May 2018. See Section 12 below (Security Requirements).

4. Key Privacy Concepts

a. Personal Data

The Privacy Law handles both general matters of privacy as well as the protection of privacy in computerized databases.

The first chapter of the Privacy Law regulates the infringement of privacy in general and establishes 12 occurrences which constitute an infringement of privacy, if done without the consent of the Data Subject:

i. spying on or trailing a person in a manner likely to harass him/her, or any other harassment;

ii. listening (wiretapping) in a manner prohibited under any law;

iii. photographing a person while he/she is in a private domain;

iv. publicizing a person’s photograph under circumstances in which the publication is likely to humiliate the person (under certain circumstances publicizing a picture of a deceased in a manner which could identify him/her will also be deemed to a breach of privacy);

v. publication of a victim’s photograph, shot during the time of injury or immediately thereafter, in a manner where he/she is identifiable and under circumstances by which the publication thereof is likely to embarrass him/her, except for the immediate publication of a photograph, without delays between the moment of photographing and the moment of actual transmission of broadcast, which is reasonable under the circumstances; for this purpose, “victim” is a person who suffered physical or mental injury due to a sudden event and the injury thereof is noticeable;

vi. copying or using, without permission from the addressee or the writer, the contents of a letter or of any other writing not intended for publication, unless the writing is of historical value or 15 years have passed since the time when it was written (this provision refers also to electronic messages);

vii. using a person’s name, appellation, picture or voice for profit;

viii. infringing an obligation of secrecy laid down by law in respect of a person’s private affairs;

ix. infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person’s private affairs;
x. using, or passing on to another, information on a person’s private affairs, other than for the purpose for which it was given;

xi. publicizing or passing on anything that was obtained by way of an infringement of privacy under paragraphs (i) to (viii) or (x) above; or

xii. publicizing any matter that relates to a person’s intimate life, state of health or conduct in the private domain.

The second chapter of the Privacy Law regulates the protection of privacy in databases. According to the Privacy Law, the definition of “Database” is “a collection of information, maintained by magnetic or optical means and intended for computer processing”, subject to the following exclusions: a collection of information that includes only names, addresses and means of communicating, which by themselves do not create any characteristics that infringe the privacy of individuals whose names are included on it, on the condition that neither the owner of the collection, nor a body corporate under its control, owns an additional collection.

Furthermore, “Information” is defined as “information about an individual’s personality, personal status, intimate affairs, health condition, financial condition, professional qualifications, opinions and beliefs”.

The Privacy Law further defines “Sensitive Information” as “information about an individual’s personality, intimate affairs, health condition, financial condition, opinions and beliefs”.

When a database includes Sensitive Information, this is one of the conditions under the Privacy Law for the registration of such database.

It should be noted that according to Israeli case law, the definitions mentioned above of “Information” and “Sensitive Information” should be interpreted broadly. Accordingly, for example, a person’s identity number and date of birth might be considered Sensitive Information which requires the registration of a database. Whether information is sensitive depends on the specific circumstances including the aggregate scope of information maintained about the Data Subject.

b. Data Processing

Note that the Privacy Law does not define the term “Data Processing”. However, there is a definition of the term “Use” as including: “disclosure, transfer and delivery”.

Furthermore, according to the Privacy Law, no person shall use Information in a database that must be registered under the Privacy Law for purposes other than those for which the database was established.

In addition, under the Privacy Law, any request to a person for information, with the intention of maintaining and using it in a database, must be
accompanied by a notice that indicates, inter alia, whether such person is under a legal obligation to provide the information or whether this is subject to his/her free will and consent, the purpose for which the information is requested, to whom the information is to be provided, and for what purpose. The database may not be used in a different manner than what was indicated in the notice without requesting an additional consent of the Data Subject.

c.  **Processing by Data Controllers**
The Privacy Law applies to any person or entity that either owns or holds a database. In certain cases, specific provisions of the Law apply to their employees and to the manager of the database (such as with respect to confidentiality obligations).

d.  **Jurisdiction/Territoriality**
In general, the Privacy Law, as part of the Israeli civil legislation, has territorial application. Accordingly, the Privacy Law will apply to offenses which have been committed in Israel in respect of violations of the applicable provisions of the Privacy Law.

However, it should be noted that there is one decision rendered by the District Court relating to the area of gambling, according to which operating an online gaming website was regarded as a domestic offense, even if the owner of the website is a foreign company, in the event that the website specifically addresses Israelis (such as translation of the website into Hebrew, the marketing of activities in Israel, etc.). The Court determined that the offense itself will have been “completed” in Israel when an Israeli individual gambled through the website (by clicking the computer mouse) and, accordingly, participated in the proposed activity of the gambling organization. The principles of this case could be applied to the Privacy Law as well, mutatis mutandis.

e.  **Sensitive Personal Data**
According to the Privacy Law, “Sensitive Information” is defined as one of the following:

i. Information about an individual’s personality, intimate affairs, health condition, financial condition, opinions and beliefs.

ii. Information which the Minister of Justice, by order (with the approval of the Israeli Parliament’s Constitution, Law and Justice Committee) has referred to as sensitive information.

As noted above, according to the Privacy Law, when a database includes sensitive information, it must be registered. It should be noted that the term sensitive information is interpreted broadly according to Israeli case law.
f. Employee Personal Data
The Privacy Law also applies to Personal Data concerning employees. Inevitably, employers are required to process both personal information as well as sensitive information regarding their employees (and potential employees). With respect to employees, according to case law, due to the nature of the relationship between the employer and the employee (i.e., the employee being in a relative position of weakness vis-à-vis the employer, with the result that the employee may be overzealous in his or her willingness to grant the employer broad consents over a wide range of information), the court will also carry out a review as to whether the employer’s actions, including the collection of any employee personal information, obtaining employee consents and the uses of the information, were undertaken in good faith and if they were proportional and relevant to the employment relationship.

5. Consent Requirements

a. General
Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent must be informed, which means that the person should receive sufficient information with respect to the matter in order to be able to reach a decision whether or not to provide the Personal Data. In general, consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data.

b. Sensitive Data
The same general rules above apply with respect to Sensitive Data. However, in general, the scrutiny of the informed consent is likely to be more stringent when it comes to Sensitive Data.

c. Minors
In general, the Privacy Law does not include any specific reference to minors and minors’ consent and accordingly the consent requirements detailed above would apply to them as well, subject to the provisions of the Legal Capacity and Guardianship Law 1962 (the “Capacity Law”), which governs matters relating to minors.

Under the Capacity Law, the legal acts of a minor (i.e., a person under the age of 18) may be cancelled if performed without the consent of a parent/guardian. However, legal acts of a kind that minors of his/her age are accustomed to perform, or legal acts performed with a person who did not or could not reasonably be expected to know that the minor is a minor, may not be cancelled unless they involve material damage to the minor or his/her property. This general rule would be applicable to any consent provided by a minor for the purpose of compliance with the provisions of the Privacy Law.
It should be noted that in December 2010, ILITA issued certain draft general principles (which are, as of this date, non-official and non-binding) which refer to the collection of information from minors over the internet. According to the draft principles, the collection of information will require, under certain circumstances, the consent of a parent/guardian, regardless of the qualifications set out under the Capacity Law, as the consent of a minor in this aspect should be dependent on the minor’s ability to understand the notice provided to the minor regarding the collection of information from such minor.

Accordingly, ILITA recommends, inter alia: (i) restricting the collection and publication of information from minors under the age of 14, without the consent of a parent/guardian and restricting the collection and publication of sensitive information from minors under the age of 18, without the consent of a parent/guardian; (ii) requiring bodies who collect information from minors to set out and publish a defined and clear privacy policy; (iii) restricting the transfer of or trade in minors’ data to or with third parties; (iv) requiring bodies who collect information from minors to comply with certain security measures; and (v) erasing the information of minors which is no longer needed or at the request of a minor’s parent or guardian.

d. Employee Consent

Under Israeli case law, an implicit consent is not sufficient with respect to employees and the employee is required to give his/her explicit consent (usually in writing) with respect to his/her waiver of his/her right to privacy.

In addition, the employee’s consent should be examined in light of the following conditions:

- condition of legitimacy – the violation of the privacy right must be limited to essential business purposes;
- condition of proportionality – the employer should examine and select the means which are the least harmful to the employees’ privacy;
- principle of proximity to the purpose – the collection of information is limited only to what is necessary in order to achieve the initial purpose for which the information was collected in the first place.

Moreover, the general policy which is applicable in the workplace, with respect to privacy matters, should be approved by the employee.

e. Online/Electronic Consent

Electronic consent is permissible and can be effective in Israel if it is properly structured and evidenced.
6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: whether the Data Subject is under a legal obligation to provide the information or whether this is subject to his/her free will and consent; the purposes for collecting Personal Data; third parties to which the organization will disclose the Personal Data and the purpose of the transfer.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

Organizations that collect and process Personal Data may be required to register a database with the local data authority.

10. Data Protection Officers

Organizations may be required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Specific regulations have been enacted with respect to the transfer of data from a database in Israel outside of Israel, titled “The Protection of Privacy Regulations (the Transfer of Information to a Database outside the State Borders), 2001” (the “Transfer Regulations”). The Transfer Regulations impose restrictions in addition to all other restrictions on transfer of information which appear in the Privacy Law, as follows:

i. The Transfer Regulations prohibit the transfer of information from a database in Israel to a database located abroad, unless the receiving country ensures a level of protection of Information that equals or exceeds the level of protection provided for under Israeli law.
ii. Nevertheless, the Transfer Regulations lay down several conditions which enable the transfer of information from a database in Israel to a database abroad, even when the laws of the country in which the data will be received provide a level of protection which falls below that which is provided under Israeli law, subject to compliance with any one of the following conditions:

- receipt of consent to the transfer of the information from the person who is the subject of the information;
- it is not possible to obtain the consent of the person who is the subject of the information, but its transfer is absolutely necessary in order to protect his/her health or the integrity of his/her physical body;
- the information is being transferred to a corporation under the control (i.e., the ability to direct the activities of an entity) of the owner of the Israeli database and it has ensured the protection of privacy following the transfer;
- the information is being transferred to someone who has undertaken in an agreement, with the owner of the Israeli database, to fulfill the conditions laid down in Israel for the maintenance and use of the information, mutatis mutandis;
- the information was made public by the lawful authority, or it was made available for inspection by the public under lawful authority;
- transferring the information is essential for the protection of public welfare and security;
- transferring the information is required by Israeli law; or
- the information is being transferred to a database in a country in which any one of the following conditions exist: (a) it is a party to the European Convention for the Protection of Individuals in connection with automatic processing of Sensitive Information; (b) it receives information from member states in the European Union, under the same conditions of receipt; (c) the Registrar has notified with respect to the destination country, in a notification which has been published in the Official Gazette, that there exists in such country a designated authority to protect privacy, after it has reached an arrangement for cooperation with such authority (to date the Registrar has not issued any such notification).

In addition to the completion of the above conditions (either under subsection i) or ii)), the Transfer Regulations state that the owner of the database must ensure (by way of a written obligation from the recipient of the information) that the recipient shall take action to ensure the privacy of the person to whom
the information relates, and that the recipient undertakes that the information shall not be transferred to any person other than the recipient, whether or not such person/entity resides in the same country.

12. Security Requirements

Organizations are required to take steps to: ensure that Personal Data in its possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

According to the Security Regulations, owners of databases, holders of databases and managers of databases are required to comply with certain data security obligations. These include, inter alia, the formulation of a database definition document, drafting of a security procedure, mapping the systems and conducting risk surveys, implementing physical and environmental security measures, access permissions management, security event documentation, data breach notifications, mobile devices management, security of communication, rules pertaining outsourcing of Personal Data, backup and recovery, conducting periodic audits, etc.

13. Special Rules for Outsourcing of Data Processing to Third Parties

ILITA has issued guidelines titled “Use of Outsourcing Services for Processing of Personal Data”, which refer to any outsourcing to a third party of the processing of Personal Data from an Israeli database. These guidelines require that an agreement be entered into with the service provider which should cover various matters. In addition, prior to entering into any agreement for the processing of Personal Data, such outsourcing should be reviewed carefully in order to ascertain its necessity and compliance with data protection laws. Under these guidelines, the following matters, inter alia, should be covered by the agreement with respect to outsourcing services:

- The agreement should establish the purpose of the transfer of information and limitations on its uses and transfer.
- Upon the termination of the agreement, the service provider should sign an affidavit confirming that the service provider has either returned the personal information or destroyed it.
- The service provider should store the information separately from the information of its other clients or its other commercial activities.
- Access and correction rights of Data Subjects are to be determined in the agreement (including with respect to timing and costs).
• The service provider should hold regular guidance sessions to its employees and they should also sign NDAs.

• The parties should each appoint a contact person with respect to the agreement.

• The service provider should provide ongoing reports with respect to the performance of the agreement and there should be extensive supervisory rights of the service provider’s activities (including audit and inspection rights).

• The agreement should define a complete binding security document which should include reference to specific matters, such as, physical security, applicable security measures according to the sensitivity of the data, separation of the database from the service provider’s other databases, policies with respect to: storage means, management of the database, access rights, etc. As an alternative to the above security document, the service provider could undertake as part of the agreement to comply with the provisions of ISO/IEC 27001.

• It is recommended that the service provider should appoint a security officer (this is mandatory in case the service provider maintains databases of more than five clients for such data processing services).

In addition to the above, the Security Regulations sets certain requirements to be complied with whenever personal information is being transferred to an external party, including certain provisions which should be included in an agreement between the owner of the database and such third-party transferee, e.g., the nature of the information being transferred, types of processing operations that transferee is permitted to perform and systems to which he/she will gain access, the term of the agreement and requirements to delete or destroy personal information upon termination, duty to provide annual reports and notify in case of data breach events, etc.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach
According to the Security Regulations, notification of breach to the Israeli data protection regulator (ILITA) is required in the following cases: (i) with respect to databases subject to the medium level of data security – prompt notification shall be provided regarding any severe data breach in which a material part of the database was accessed or used without authorization, or while exceeding
authorized access, or where the database’s integrity was compromised, with respect to a material portion of the database; (ii) with respect to databases subject to a high level of data security – the breach notification requirement applies to any severe data breach in which any portion of the database was breached (not just a material part).

In addition, the Security Regulations determine that ILITA is authorized to instruct the database owner (after consulting with the Head of the National Cyber Security Authority) to notify all affected Data Subjects regarding the data breach.

It should be noted that even when there is no specific instruction by the regulator to notify Data Subjects, notification to the affected individuals is something that should be considered in order to reduce any possible damages and exposure under tort and contract law, if in the applicable circumstances, such damages or exposure might exist.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.

Note that notification requirements with respect to data security breaches may be applicable in certain specific fields under legislation and/or guidelines issued with respect to such specific field.

16. Accountability

According to the Security Regulations in a database which is subject to the high level of data security the owner of the database is required to perform privacy impact assessments and penetration tests at least once every 18 months.

Organizations may be required in certain circumstances to furnish the results of privacy impact assessments and to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline

There are no specific laws/rules regarding whistle-blower hotlines in Israel. In general, whistle-blower hotlines may be established in Israel as long as they are in compliance with local laws, e.g., registration might be required in connection with the hotline under general privacy laws, depending on the specific circumstances of the matter.
18. E-Discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved. Organizations may be required to advise employees of the implementation of said system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to obtain the consent of employees for monitoring policies being implemented in the workplace.

20. Cookies
There are no specific laws/rules in Israel that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws, to the extent the cookies collect personal information or information which can be cross referenced with personal information. As such, the consent of Data Subjects may have to be obtained before cookies can be used.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which can in certain circumstances be on an opt-out basis.

For further information regarding direct marketing, please see Clause 1 above.
Francesca Gaudino
Milan
Tel: +39 02 76231 452
francesca.gaudino@bakermckenzie.com
1. Recent Privacy Developments

In the following, we provide an overview of the Privacy Authority’s activities during 2017.

**Agreement with the Information Security Department**

On 6 October 2017, the Authority signed a protocol of agreement with the Information Security Department (Dipartimento delle informazioni per la sicurezza – DIS) that confirms and re-vamps the guidelines agreed in 2013. The document takes into consideration recent governmental developments in the area of national cybersecurity and information security and is aimed at rendering more effective the Authority’s monitoring of activities performed by the DIS.

**Auditing activities**

The Authority has recently provided information on its auditing activities planned for the period July – December 2017. Main areas of focus are the following:

- telemarketing;
- beauty contests, promotions and similar initiatives;
- the recruitment sector;
- call centers, especially located in Albania (following the 2015 cooperation agreement between Italy and Albania on this matter);
- compliance with the requirements of providing adequate information notices, of collecting a valid consent (when necessary), of having data retention policies and of using only data necessary for the relevant purposes (necessity and proportionality principles);
- compliance with data security obligations;
- processing of data for digital identity purposes by public authorities;
- data sharing among health assistance entities and pharma and health companies;
- data processing for credit claim purposes;
- data processing for statistical purposes.

The results of the auditing activities performed over the first six months of 2017 reveal sanctions of more than EUR 1,700,000; 300 sanctioning decisions issued; and 20 reports to criminal courts, mainly for lack of mandatory data security measures and unlawful monitoring of workers. The monitoring activities of the Authority have been focused mainly on credit and
financial companies, marketing, door-to-door sales, sharing services, telemarketing.

**Guidelines and materials**

The Privacy Authority has been fairly active over the last year in issuing orders and guidelines, especially relating to the digital dimension (e.g., for search engines and social networks). In this respect, it has issued a number of guidelines and informative material, for example in relation to the use of Apps, cyberbullying, privacy issues in school, the risks of phishing attacks, data processing for credit claim purposes, the use of smartphone and social media platforms (for example when making pictures and selfies, when purchasing, when using chats, etc.). Specific new rules have been issued for call centers, with particular attention to call centers located outside the European Union.

**GDPR**

In relation to GDPR (Regulation EU 2016/679) the Privacy Authority has issued the following documents: a general guide on the application of the GDPR, supplemented by information on the legislative path of the GDPR, and a one-page leaflet summarizing main themes, including DPO, lead supervisory authority and the right to data portability.

In addition, the Privacy Authority has rolled out a series of meetings with public authorities in order to provide guidance on implementation of GDPR in the public sector.

In Italy we are still waiting for an implementation/adoptions law of the GDPR.

**The Internet of Things**

With regard to the Internet of Things, the Privacy Authority has launched a public consultation in order to gather information and comments from stakeholders and organizations on how to adapt new technologies to the regulatory framework. Among others, importance has been given on the manner of complying with the requirements to provide Data Subjects with the mandatory information on data processing and of the manner of securing valid consent, when requested by the Privacy Code. Individuals’ opinions are also considered. In addition, the Privacy Authority has teamed up with other international organizations in relation to multi-jurisdictional investigations, with specific focus on domotics or home automation.

**Online Profiling**

The Privacy Authority has issued Guidelines for online profiling activities (i.e., the building of personal/cluster profiles of individuals based on Personal Data such as preferences, habits, purchases, activities performed online, etc.). The relevant provisions are addressed especially (but not only) to websites and
other online initiatives, with the aim of providing solid guarantees to the privacy of Data Subjects in the digital ecosystem. Organizations must carefully consider the requirements set forth for online profiling and combine them with the applicable rules on cookies and profiling activities performed offline.

**Other matters**

The Privacy Authority has also defined guidelines and criteria to address and manage Data Subjects’ requests relating to the “right to be forgotten” and the de-indexing of URLs.

In the e-health sector, the Privacy Authority has adopted specific Guidelines for electronic health records, in order to provide tighter guarantees to the Data Subjects.

Lastly, the Privacy Authority has formally invalidated the application in Italy of the Safe Harbor mechanism, and positively welcomes the approval of the Privacy Shield Scheme as well as of the General Data Protection Regulation (“GDPR”) (see paragraph 2 below).

**2. Emerging Privacy Issues and Trends**

**Inspection activities**

For the year 2016, the annual report of the Authority states that fines have been issued for a total amount of almost EUR 5 million, almost 400 inspections have been carried out and the Authority has received almost 5,000 replies to claims.

In the annual report for 2016, the Authority provided a glimpse on their initiatives for the next year, especially in light of the application of the GDPR as of May 2018. One of the main goals is to guarantee real protection of individuals’ Personal Data in the digital ecosystem, in light of new economic business models and the strong call for protection of individuals.

In terms of data breaches reported to the Authority (currently the reporting obligation in Italy in the private sector applies to Telecoms companies), the Authority received 43 reports.

The number of administrative breaches rose by 38% in respect to 2015, reaching 2,339. Out of these, 1,817 relate to lack of notification to Data Subjects of data breaches by Telecom operators. The remaining breaches mostly relate to the following:

i. failure to obtain consent of Data Subjects;

ii. providing inadequate or no information on data processing to Data Subjects;

iii. breach of data security requirements;
iv. breaches of orders and provisions of the Authority;

v. failure to disclose data breaches;

vi. failure to provide documentation to the Authority; and

vii. failure to comply with data retention limitations for telephone and traffic data.

The administrative sanctions reached the threshold of EUR 3 million and 300,000, while 282 audits have been carried out.

The business sectors on the Authority’s radar are car sharing, web and telephone marketing, online gaming, financial services and money transfers. In relation to money transfers, the Authority aims to combat money laundering and has issued sanctions totaling EUR 11 million.

In addition, it is worth noting that the Authority is fairly active in participating in international activities and joint initiatives with other European data protection authorities and also non-European authorities.

The annual report of the Authority is available in Italian on the Authority’s website, at: www.garanteprivacy.it

**National and international cooperation – the case of cookies**

The Privacy Authority has been fairly active within the Article 29 Working Party, since the President of the Privacy Authority is acting as Vice President of the same. Main areas of interest have been: drones, cloud computing, e-health, cookies, profiling in the financial sector, binding corporate rules and passengers’ Personal Data (i.e., Passenger Name Records).

The Privacy Authority has been deeply involved in the analysis of the Schrems case that has led to the invalidation of the Safe Harbor scheme for the transfer of Personal Data to the US.

The Privacy Authority has actively joined the process for issuance of the GDPR (the new European Regulation on data protection), also taking part as technical expert to the meetings of the competent working group of the Counsel of the European Union (DAPIX).

The Privacy Authority has also collaborated with the European Counsel in relation to the Convention of 1981 on the protection of data and on the recommendations on the processing of Personal Data in the employment sector.

Lastly, collaboration with international based organizations, such as the Global Privacy Enforcement Network, is actively pursued by the Privacy Authority.
3. Law Applicable

The Data Protection Directive (Directive 95/46/EC), the Directive on Privacy and Electronic Communications (Directive 2000/58/EC), the Directive on Data Retention (Directive 2006/24/EC) and the Cookies Directive (Directive 2009/136/EC) have been implemented by Legislative Decree no. 196 of 30 June 2003, which enacted a code on the protection of Personal Data (the “Code”). The Code is primarily intended to consolidate all pre-existing Italian data protection rules, which were replaced by the Code. Furthermore, the Code provides for additional protections for Data Subjects (defined below) and simplifies the applicable rules. The Code attempts to ensure consistency between privacy rules and other legal provisions applicable to various sectors. The Code combines the provisions of the former basic privacy law and subsequent amendments, regulations, and codes of ethics, as well as the case law precedents of the Italian Data Protection Authority.

The Code is organized into three parts:

- the first contains general data protection provisions;
- the second contains provisions applicable to specific sectors (e.g., judicial sector; public sector; health care sector; educational sector; processing for historic, scientific and statistical purposes; work and social security issues; banking, financial and insurance sectors; electronic communications; professionals and private detectives; journalism, literary and artistic sectors; and direct marketing); and
- the third contains remedies and sanctions for breach of the Code.

The Code applies to the processing of information relating to “Data Subjects” as outlined below.

4. Key Privacy Concepts

a. Personal Data

The Code applies to the processing of information relating to natural persons (“Data Subject”); legal entities and bodies or associations are within the scope of the Code only for limited purposes. Data is considered “personal” where a person can be identified from that data directly or indirectly by reference to any other information (e.g., through cross-referencing via a personal identification number) (“Personal Data”). The information necessary for the identification can be held by the Data Controller (defined below) processing data or by any other third party. Thus, the definition of Personal Data is significantly broad. In practice, only anonymous data (e.g., data that does not allow identification of the Data Subject, whether directly or indirectly) is not subject to the Code.
b. Data Processing
As in the applicable Directive, the term “processing” is extremely broadly defined to mean any operation or set of operations carried out on Personal Data, including the collection, recording, organization, keeping, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure, and destruction of Personal Data. Even mere reading is considered processing of Personal Data. The Code applies to electronic, automated and non-electronic (manual and paper) data processing.

c. Processing by Data Controllers
The Code applies to those who determine the purposes for which and the manner in which any Personal Data is collected and processed (“Data Controllers”).

d. Jurisdiction/Territoriality
The Code applies to data processing activities performed by a Data Controller established within Italy, and to data processing activities performed by Data Controllers that are established outside the EEA but that use equipment based in Italy to carry out data processing activities (other than merely for the purpose of transit).

e. Sensitive Personal Data
The Code imposes additional requirements for the processing of Sensitive Personal Data – that is, Personal Data relating to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, and data concerning health or sexual life. Specifically, the processing of Sensitive Personal Data is prohibited unless the following conditions are met: (i) the Data Controller provides an information notice drafted pursuant to the Code and obtains the explicit written consent of the Data Subject; (ii) limited exceptions apply (see Sections 4(f) and 5(b) below); (iii) and the Data Controller has the prior authorization of the Authority. The Authority has issued general authorizations that cover usual business activities. A specific authorization is required when the Data Controller intends to perform a data processing activity that does not fall within the general authorizations issued by the Authority under conditions that follow outside the same.

f. Employee Personal Data
Employee Personal Data is likely to include Sensitive Personal Data (e.g., health- and trade union-related information) and non-Sensitive Personal Data. Sensitive Personal Data relating to an employee may be processed provided that the requirements mentioned in Section 4(e) above are met. The employee’s consent is not requested when the processing of Sensitive Personal Data is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or community legislation in the employment
context, also when they relate to occupational and population hygiene and safety, and to social security and assistance purposes. In addition, recent legal reform has introduced a further exemption from the written consent requirement. Written consent is not required for the processing of sensitive data of candidates, when such data is contained in the curriculum vitae that is sent by candidates. One of the general authorizations issued by the Authority applies to employee Sensitive Personal Data. This allows Data Controllers to process an employee’s Sensitive Personal Data in certain circumstances and for certain purposes specified in the authorization. Non-Sensitive Personal Data relating to an employee may be processed by a Data Controller in certain circumstances, including where the processing is necessary for the performance of the employment agreement or where the processing is necessary for compliance with a labor law or tax obligation of the employer or other applicable laws. A fallback justification for processing both Sensitive and non-Sensitive Personal Data in the employment context may be available if consent (written, in the case of Sensitive Personal Data) is provided by the Data Subject (see Section 5(d), below).

The Authority issued two regulations on the processing of employees’ Personal Data and Sensitive Personal Data in November 2006 and March 2007. The regulations impose an obligation on the employer to comply with the principles of transparency and proportionality, so that only data that is strictly necessary for a specified purpose may be processed. Further, the consent of the employee must be obtained when there is no other legitimate ground for the processing. Moreover, if the employer provides its employees with personal computers, access to the Internet and email accounts, the employer must fulfill certain requirements. For example, the employer should clearly specify to the employees the conditions and limits of the use of the company’s information system and relevant resources, and it should also clarify, among other matters, whether personal use is allowed, the relevant conditions (e.g., time and duration), and whether and how the employer intends to perform monitoring activities (including the specific circumstances and purposes of said monitoring). The employer should also seek approval from trade unions or the competent labor office.

5. Consent

a. General

Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be explicit, freely given, specific, voluntary, informed and unambiguous, though it is not required in certain prescribed circumstances.

Consent must always be express and cannot be implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives
consent, it is understood that such consent only covers the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

Consent must be in the local language. The Data Subject also has the right to withdraw consent at any time.

b. Sensitive Data
Sensitive Personal Data is recognized as a special category of Personal Data and is subject to additional or special consent requirements. Sensitive Personal Data may only be collected and processed with the express consent of the Data Subject and on the basis of a general or specific authorization of the Authority.

For the processing of Sensitive Personal Data, written consent must be provided – that is, in the form of a handwritten or digital signature of the Data Subject. Limited exceptions apply (see Section 4(f) above).

c. Minors
A person under the age of 18 cannot give valid consent. A parent or legal guardian must give consent on behalf of the minor. When the minor becomes of age it is necessary to obtain confirmation of the consent previously provided by parents or guardians.

d. Employee Consent
Consent given by an employee to the processing of his or her Personal Data is generally considered valid. The usual business practice and advisable procedure is to have a specific privacy document containing the information notice and consent form, usually attached as an Annex to or incorporated by reference in the employment agreement. If Personal Data is also to be processed for purposes not necessary to fulfill legal obligations or unrelated to the employment agreement (for example, if Personal Data is disclosed to business partners or other companies that may offer products or services to the employees, or if employees’ Personal Data such as pictures or professional information are published on the company’s intranet), the Authority recommends that these additional purposes be specifically approved by the employees through separate consent.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in Italy provided that it is properly structured and evidenced. For Sensitive Personal Data, however, electronic consent may only be permissible in very limited circumstances specifically identified by the Authority.
6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) the conditions of the data processing; (v) third parties to which the organization will disclose the Personal Data; (v) the mandatory or voluntary nature of providing Personal Data and the consequences in case of denial to provide Personal Data; (vi) the rights of the Data Subject; (vii) how the Personal Data is to be retained; (viii) where the Personal Data is to be transferred; (ix) where the Personal Data is to be stored; (x) how to contact the privacy officer or other person accountable for the organization’s policies and practices; and (xi) the name and contact details of the Controller and the Data Processor mainly responsible for the data processing considered, as applicable.

7. Processing Rules

An organization that processes Personal Data must, among others: (i) limit the use of the Personal Data to those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; (ii) collect and use only the number and kind of Personal Data strictly necessary to fulfill the intended purpose; (iii) make use of key-coded or anonymous data whenever possible; and (iv) delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects, among others, have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; (iv) request the deletion and/or destruction of the Data Subject’s Personal Data; (v) and exercise the writ of habeas data as well as the right to know the source of data.

9. Registration/Notification Requirements

Organizations that collect and process Personal Data may be required to register, file or notify the local data authority in case specific data processing operations are carried out.

10. Data Protection Officers

There is no such privacy role under the Code. It is possible to appoint an internal Data Processor (Responsabile del trattamento) for managing privacy issues within an organization on behalf of the Data Controller. In case of third-party service providers processing Personal Data in delivery of relevant
services, they must be appointed by the Data Controller as external Data Processors.

11. International Data Transfers

Transfer of Personal Data between EEA Member States is generally permitted without the need for formal approval by the Authority. Furthermore, no restrictions apply to the transfer of Personal Data to recipients in countries that have been recognized by the European Commission as granting an adequate level of protection to Data Subjects. This is the case for transfers to Switzerland, the Isle of Man, Guernsey, Argentina, Canada, and others. In the above-referenced cases, the transfer of Personal Data is regulated as a communication of Personal Data, thus relevant requirements for Personal Data sharing apply. Transfers outside the EEA are prohibited where the third country does not ensure an adequate level of protection of Personal Data. Exceptions are as follows:

- the Data Subject has given his or her express consent to the transfer (written consent is required for Sensitive Personal Data);
- the transfer is necessary for the performance of obligations resulting from a contract to which the Data Subject is a party, or for gathering information at the Data Subject’s request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the Data Subject;
- the transfer is necessary for safeguarding an important public interest;
- the transfer is necessary for carrying out criminal investigations;
- the transfer is necessary to safeguard the life or bodily integrity either of the Data Subject or of a third party, and the Data Subject cannot give his or her consent because of physical or legal incapacity or mental disorder;
- the transfer is carried out in response to a request for access to administrative documents or for information included in a public register, list, act, or document which is publicly available, in compliance with the provisions applying to such subject matter; and
- the transfer is authorized by the Authority on the basis of adequate guarantees for the Data Subject’s rights, as resulting from contractual clauses in a data transfer agreement.

The following specific requirements relate to the use of a data transfer agreement: (i) incorporation (or incorporation by reference) of the European Commission’s model clauses for transfer of data between Data Controllers or towards Data Processors into the data transfer agreement by the data exporter and the importer, so that they are available, upon request, to the Data Subjects to whom the Personal Data relates; (ii) a copy of the data
transfer agreement must be provided to the Authority upon request of the Authority; (iii) the choice made in case of a dispute that is not settled amicably and is submitted to an entity other than either the Authority or a judicial authority must be communicated to the Authority; (iv) the Data Subjects must be informed of the transfer and the fact that the data transfer agreement is in place. When the aforementioned conditions are met, no formal approval of the data transfer agreements by the Authority is required. In case of transfer to Data Processors, the name and details of sub-processors shall be provided to the Authority.

12. Security Requirements

An organization is required to take steps to: (i) ensure that Personal Data in its possession and control is protected from unauthorized access and use, alteration, destruction and loss, even accidental, and against any form of unlawful data processing; (ii) implement appropriate physical, technical and organization security safeguards to protect Personal Data; (iii) and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved, as well as the technological progress. Minimum data security measures are detailed by the law, while adequate security measures shall be determined by the Data Controller according to its specific processing conditions and features. Lastly, specific measures for specific processing activities may be set forth by the Authority.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties acting as service providers are required to appoint the third party as external Data Processor through a data processing agreement in order to keep control and protect Personal Data. Sector-specific requirements should also be taken into consideration. Organizations may be held liable in the event of breach by the third-party service provider.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

The Code provides for an obligation of disclosure to Data Subjects and/or the Authority or other authorities in the event of a security breach limited to specific sectors (e.g., telecoms operators, banks, public authorities and institutions, data breaches involving material impact on biometric data and electronic patient dossiers). In any case, the Data Controller is liable to
compensate not only for monetary but also for moral damages caused by the data processing. Thus, also for companies not subject to a disclosure obligation under the Code, in the event of security breaches, organizations that are involved in a data breach situation should: (i) gather information about the breach; (ii) assess the potential risk of harm to the Data Subject(s); (iii) take steps to mitigate the harm to the impacted Data Subject(s); (iv) take steps to contain the breach and to prevent future similar breaches; (v) assist authorities with any investigation relating to the breach; (vi) and comply with data authority orders and court orders.

An organization that is involved in a data breach situation may be subject to a suspension of business operations; closure or cancellation of the file, register or database; an administrative fine, penalty or sanction; civil actions and/or class actions; or a criminal prosecution.

16. Accountability

Organizations are required to file a prior checking procedure with the Authority in case the processing operations may represent a risk for the Data Subject’s rights, fundamental freedoms and dignity, in relation to the nature of the data processed, to the conditions of the data processing or to the consequences that may derive from the processing.

In general terms, Controllers should conduct a privacy impact assessment prior to the implementation of new information systems and/or technologies for the processing of Personal Data in order to verify privacy risks and relevant counter-measures to be applied. In case of an audit, request or investigation, organizations should furnish the results of the privacy impact assessments (as applicable) to privacy regulators and competent authorities; and also furnish evidence relating to the effectiveness of the organization’s privacy management program and status of compliance to privacy regulators and competent authorities.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Italy as long as they are in compliance with local laws.

18. E-Discovery

Employers should advise employees of the implementation of an e-discovery system, the features and purposes of the said system, and (if applicable) that the use of work tools (e.g., email, Internet) is being monitored and that information such as emails is stored. Employers should also specify the features of the monitoring activities and the consequences of failure by employees to comply with the employer’s guidelines on the correct use of the employer’s electronic equipment and system. An employer should also specifically inform employees whether and to what extent electronic devices
and equipment provided by the employer for business purposes may also be used for personal purposes. The above information should be contained in a specific IT policy that the employer provides to its employees.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to: (i) inform employees of monitoring policies being implemented in the workplace; (ii) give employees the opportunity to opt out from the spam-filtering solution; and (iii) give employees the opportunity to review the isolated emails designated as spam.

20. Cookies
The use of cookies must comply with data privacy laws. As such, consent of Data Subjects must be obtained before cookies can be used and deployed in case of cookies that are not necessary from a technical perspective or in order to provide the product/service requested by the Data Subject. Consent is thus necessary, for example, for marketing and profiling cookies.

Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent and if obtained online or through apps, pre-checked boxes cannot be used.
**Japan**

**Daisuke Tatsuno**  
Tokyo  
Tel: +813 6271 9479  
daisuke.tatsuno@bakermckenzie.com

**Kensaku Takase**  
Tokyo  
Tel: +813 6271 9752  
kensaku.takase@bakermckenzie.com
1. Recent Privacy Developments

On 3 September 2015, extensive amendments were introduced to the law in Japan which deals with the protection of personal information, “The Act on the Protection of Personal Information” (“APPI”). The amended APPI took effect on 30 May 2017 and the following are some of the noteworthy amendments to the law.

a. Amended Definition of “Personal Information”

The amended APPI and relevant implementation regulations set out a new definition of “personal information”. The definition has expanded to include letters, numbers, marks or other codes for use with computers converted from a person’s bodily information, such as fingerprint data, face and voice recognition data, and base sequence of DNA.

b. Establishment of the Personal Information Protection Commission

The “Personal Information Protection Commission” (the “Commission”) is now in its second year since its establishment and has produced various guidelines including new general guidelines (“APPI Guidelines”) which have replaced the Ministry of Economy, Trade and Industry guidelines and other ministerial guidelines. The only exceptions being the specific ministerial guidelines for the financial, medical and telecommunications industries.

c. Handling of Anonymized Information

The amended APPI sets out the following obligations on business operators when anonymizing Personal Data to be transferred to third parties.

- a business operator must create the anonymized data pursuant to the regulations of the Commission;
- the business operator must ensure that the original pre-anonymized data may not be recreated; and
- the business operator must publicly disclose certain information concerning the anonymization of the data.

d. Sensitive Data

Under the previous APPI, there were no specific definitions concerning sensitive data such as race, religion or medical history. Under the amended APPI, business operators are prohibited from obtaining such sensitive data without the Data Subject’s consent.

e. Transfer of Personal Data to Third Parties

Under the amended APPI, a business operator that receives Personal Data must confirm how the Personal Data was obtained and retained, and keep a record concerning the receipt of information for a certain period of time. A
business operator that transfers Personal Data to a third party must also keep a record concerning the transfer of information for a certain period of time.

**f. Criminal Sanction for the Misuse of Personal Data**

Under the amended APPI, individuals who are involved in the handling of Personal Data which has been subject to misuse or which has been stolen for unjust profit are subject to a criminal penalty.

**g. Opt-Out for Transfers of Personal Data**

The previous APPI permitted business operators to transfer Personal Data to a third party without the Data Subject's consent unless the Data Subject later opted out from doing so. Under the amended APPI, a prior notification to the Commission is necessary in order to use this opt-out arrangement.

**h. Cross-Border Transfer of Personal Data**

Under the previous APPI, there were no restrictions on international transfers of Personal Data. However, the amended APPI provides that Personal Data may be transferred to a foreign country only when:

- specific consent of the Data Subject is obtained;
- the country has a legal system that is deemed equivalent to the Japanese Personal Data protection system; or
- it is transferred to a third party which undertakes adequate precautionary measures for the protection of Personal Data, as specified by the Commission.

**i. Extra-Territorial Application**

The amended APPI provides that some of its main provisions apply extra-territorially. Such provisions include the requirement to specify the purpose of use, notification of purpose of use, and the requirement for consent when transferring Personal Data to third parties. Such provisions apply to entities that collect personal information in order to provide goods or services in Japan, but process the personal information overseas. Therefore, a foreign entity needs to comply with the amended APPI if it provides goods or services to Japanese consumers, and collects and processes their personal information outside of Japan.

2. **Emerging Privacy Issues and Trends**

There is an increasing amount of awareness on the importance of privacy in Japanese companies. Now that most of the guidelines have been drafted, the Commission has been active in raising awareness of the amended APPI to the public.

On 4 July 2017, Japan’s Commission and the European Commission published a joint statement that the recent reforms of their respective privacy
legislation have further increased the convergence between the EU and Japan privacy law systems. They were looking towards a “simultaneous finding of an adequate level of protection by both sides” by early 2018.

3. Law Applicable

Extensive amendments were introduced on 3 September 2015 to the law dealing with the protection of personal information, and took effect on 30 May 2017.

In addition to the APPI, the Commission has issued various guidelines. The guidelines serve to ensure that companies comply with the APPI, and to provide an interpretation of the APPI as it relates to specific industries, and to particular issues, such as security measures. These guidelines include the following:

- **Guidelines on the Act on Protection of Personal Information: General Rules**
- **Guidelines on the Act on Protection of Personal Information: Transfer to Overseas Third Party**
- **Guidelines on the Act on Protection of Personal Information: Confirmation and Record-keeping Obligations for Third Party Transfer**
- **Guidelines on the Act on Protection of Personal Information: Anonymized Information**
- **Guidelines on the Act on Protection of Personal Information: Actions to Take in case of Leakage**

While the guidelines do not have any direct financial penalties for breach, non-compliance for applicable companies may have other consequences such as warnings from the agencies or loss of regulatory licenses.

In many instances, companies may find that more than one set of guidelines are applicable to them.

There are also laws that relate separately to the protection of personal information held by Japanese government agencies. These laws are not discussed in this handbook.
4. Key Privacy Concepts

a. Personal Data

The APPI applies to “Personal Information”.

As mentioned in Section 1, the amended APPI added a new definition and now the term “Personal Information” is defined to mean the following two categories of information:

- information about a living individual which can identify a specific individual by the description contained in the information, such as name, date of birth or other description (including voice or behavior information), including information which can easily be combined with other information so as to enable the identification of that individual; and

- information that contains Personal Identifier Codes. “Personal Identifier Codes” means either (a) letters, numbers, marks or other codes for use with computers converted from a person’s bodily information which may identify the person, or (b) letters, numbers, marks or other codes on cards or other documents which are unique to the user or purchaser, and may identify the person.

The relevant implementation regulations, which were subject to public comment in August 2016, provide further details as to what information is covered by the “Personal Identifier Codes”. According to the regulations, a person’s bodily information, such as fingerprint data, face and voice recognition data, and base sequence of DNA, are included in the “Personal Identifier Codes”. Further, the regulation provides that passport numbers and driver’s license numbers are “Personal Identifier Codes”.

Consequently, when broadly interpreting the amended APPI, it provides that such bodily information is protected as personal information, even when converted into a code which is only machine readable and not recognizable by human beings.

The APPI only applies to information concerning individuals, and does not cover information concerning corporations or other types of corporate entities.

Apart from “Personal Information”, “Personal Data” is separately defined to cover information stored in a business operator’s database (see the comments in 4(c) below with regard to a “business operator”). Such databases are defined to include the following:

- an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; or

- an assembly of information arranged in accordance with certain rules that has a table of contents, index or other means to facilitate the retrieval.
In other words, once Personal Information is stored in a database, it will be treated as “Personal Data” under the APPI. Certain provisions of the APPI deal with the broader concept of “Personal Information”, while other provisions deal with the more specific concept of “Personal Data”.

The APPI Guidelines give various examples of what constitutes a “database”, such as:

- email address book (where combined information of names and email addresses are inputted);
- electronic files in which user IDs and log-information on transactions by users are stored;
- business card information stored in electronic spreadsheets for business use and which can be retrieved by individuals such as workers;
- alphabetically (Japanese) arranged registration cards of temporary staff.

The APPI does not distinguish between public information and privately held information.

b. Data Processing

The APPI has a very broad and open concept of data processing. “A business operator handling personal information” is interpreted to mean a business operator using a personal information database for its business.

c. Processing by Data Controllers

There is no concept of a “Data Processor” under Japanese law. As such, handling of Personal Data under the APPI should pertain to how a “business operator” treats and manages the Personal Information or Personal Data in its possession.

i. Definition of a “Business Operator”

The APPI uses the term “business operator”, which is defined as an individual/entity that uses for its business a database of personal information containing Personal Data. A “business operator” essentially refers to the entity responsible for the proper handling of all “Personal Information”. This is similar to the concept of a “Data Controller” under EU law. It is worth noting again that there is no “Data Processor” concept under the APPI. The previous APPI did not apply to a business operator that used a database of personal information containing Personal Data of less than 5,000 living individuals. However, this exemption has been abolished by the amendments. As a result, the amended APPI applies to all business operators, regardless of the number of individuals whose personal information they retain.
ii. Use of Personal Information by the Business Operator

Once a business operator has acquired Personal Information, it must promptly notify the Data Subject, or publicly announce the “Purpose of Use” of such Personal Information. If the business operator acquires Personal Information in the course of executing an agreement or otherwise through obtaining a document on which the Data Subject’s Personal Information is indicated, the Purpose of Use must be notified to the Data Subject in advance (i.e., a public announcement is not sufficient). “Purpose of Use” refers to the business operators’ intended methods of use of the Personal Information. Any such use of Personal Information by the business operator must be made within the scope of the “Purpose of Use”.

Such “Purpose of Use” must be promptly disclosed to Data Subjects where the business operator gathers their Personal Information. The “Purpose of Use” must be described in specific detail. Alternatively, the business operator must make a public announcement of the “Purpose of Use”.

The APPI Guidelines give various examples of what is meant by the term “publicly announce”. The APPI Guidelines state that the announcement must be done in a reasonable and appropriate manner depending on the nature of the business and the status of the Personal Information. The APPI Guidelines state that this can include notices in stores, brochures and on websites that can be easily accessible with a few clicks.

The Data Controller must not use the Personal Information beyond the scope necessary to achieve the “Purpose of Use” unless:

- it can obtain the prior consent of the Data Subject; or
- such use is expressly permitted under the APPI or other applicable laws.

The APPI encourages business operators to maintain accurate and up-to-date Personal Data within the scope necessary to achieve the “Purpose of Use”.

Any subsequent changes to a “Purpose of Use” must be reasonable.

d. Jurisdiction/Territoriality

As mentioned in Section 1, the amended APPI provides that some of its main provisions apply extra-territorially to entities that collect personal information in order to provide goods or services in Japan, but process the personal information overseas.

e. Sensitive Personal Data

Under the previous APPI, there were no specific definitions concerning sensitive data. The amended APPI has created a new definition for “Personal Information that needs special care” (“Sensitive Data”), which is defined to
include race, religion, social status, medical history, criminal history and the fact that the person suffered damages by a crime.

The regulations further provide information concerning the following which are also classified as “Sensitive Data”:

- mental and physical disabilities;
- results of medical checks;
- medical advice, diagnoses or dispensing of pharmaceuticals by doctors based on medical checks;
- criminal procedures conducted against an individual; and
- juvenile delinquency procedures against minors.

Under the amended APPI, business operators are prohibited from obtaining such Sensitive Data without the Data Subject’s consent. Further, the opt-out exception (described in Section 5(a) below) does not apply to Sensitive Data under the amended APPI.

f. Employee Personal Data

The APPI does not treat Employee Personal Information or Personal Data any differently than any other form of Personal Information or Personal Data.

5. Consent

a. General

The general rule under the APPI is that a Data Subject’s prior consent is required for the transfer of their Personal Data (i.e., not for the collection of the Personal Information). Also, both the transferor and the transferee must keep a record concerning such transfer or receipt of information. However, there are exceptions to the general rule:

Subcontractor

Where a business operator entrusts the handling of Personal Data under its control, in whole or in part, to another party, such party is considered a “subcontractor” under the APPI. For transfer of Personal Data to a subcontractor as such, a Data Subject’s consent is not required. However, the business operator must exercise necessary and appropriate supervision over the subcontractor to ensure proper security management of the Personal Data.
Joint User

If the Personal Data will be jointly used by a “joint user” for the purpose of the APPI, the Data Subject’s consent is not required. However, the business operator must notify the Data Subject of the following information in advance:

- the fact that Personal Data is used jointly with other individuals or entities;
- the items of Personal Data to be used jointly;
- the scope of the joint users (i.e., the names of joint users or other information by which the Data Subject may understand who will jointly use the Personal Data);
- the purpose for which the Personal Data is used by them; and
- the name of the individual or entity responsible for the management of the Personal Data.

Opt-Out

Under the previous APPI, a business operator may transfer Personal Data to third parties without the Data Subject’s consent if the Data Subject can opt out from doing so. Under the amended APPI, a prior notification to the Commission is necessary in order to use this opt-out arrangement. The amended APPI does not allow business operators to transfer Sensitive Data to third parties based on this opt-out arrangement.

Disclosure due to corporate merger

Where information is disclosed to a surviving or newly established company following a merger or sale of a business, the surviving or newly established company receiving any Personal Data is not considered a “third party”.

Others

Transfer of Personal Data to a third party is also allowed in the following circumstances:

- when the disclosure is made in accordance with the law;
- when the disclosure is necessary to protect life, body or property (e.g., sudden illness);
- when the disclosure is necessary to protect public health (e.g., epidemiology investigation); or
- when the disclosure is necessary for governmental purposes (e.g., tax investigations).
b. **Sensitive Data**
As explained above, under the amended APPI, business operators are prohibited from obtaining such Sensitive Data without the Data Subject's consent.

c. **Minors**
The APPI Guidelines state that where a child has no ability to understand the results that may arise from his or her consent to the handling of his or her Personal Information, then it is necessary for the business operator to obtain consent from the “attorney-in-fact”, which essentially means the child's parent or guardian.

d. **Employee Consent**
As there is no special treatment in the APPI for employees, the issue of employee consent is not addressed.

e. **Online/Electronic Consent**
Catch-all and preliminary consent is not allowed under the APPI. Although the APPI has no restrictions on the manner of how consent is obtained, the guidelines issued by Financial Services Agency generally require written consent. Electronic consent is also recognized by the Financial Services Agency guidelines as being an acceptable form of written consent.

6. **Notice Requirements**
Business operators are obligated under the APPI to provide Data Subjects with:
- the business operator's name;
- the "Purpose of Use";
- the procedures used by the business operator to access, modify and terminate the use of the Personal Data it possesses; and
- contact information for the purposes of handling complaints.

7. **Processing Rules**
See our comments under Section 4(c)(ii) with regard to Purpose of Use. Generally, a business operator must ensure that its use of Personal Information does not extend beyond the Purpose of Use (which the Data Subject has agreed to in advance).

8. **Rights of Individuals**
Personal Data processed by business operators must be disclosed to the Data Subjects upon their request in writing or by other means acceptable to the Data Subjects. If retained Personal Data is found to be incorrect, such
Personal Data must be corrected while remaining in compliance with the Purpose of Use.

If a Purpose of Use is found to have been violated, the Data Controller may have to discontinue using its retained Personal Data to the extent necessary to redress the violation.

If a Data Subject requests disclosure of his/her information or requests modifications to his/her information, the business operator must, in principle, comply with such requests unless:

- the disclosure is likely to harm the life, body, property or other rights or interests of the Data Subject or a third party;
- the disclosure is likely to seriously impede the proper execution of the business of the business operator; or
- the disclosure violates other laws and regulations.

9. Registration/Notification Requirements

Business operators that collect and process Personal Data are not required to register, file and notify the Commission other than where they transfer the Personal Data to third parties based on this opt-out arrangement.

10. Data Protection Officers

Some guidelines, such as the APPI Guidelines, recommend the implementation of a chief privacy officer as an organizational security measure. The Ministry of Health, Labor and Welfare’s guidelines state that organizations under their ambit should have an administrator or, preferably, a group of administrators who have sufficient knowledge of Personal Information issues to ensure proper management of the Personal Information they deal with.

11. International Data Transfers

The amended APPI provides that Personal Data may not be transferred to a foreign country unless:

i. the Data Subject has given specific advance consent to the transfer of the Data Subject’s Personal Data to the entity in a foreign country;

ii. the country in which the recipient is located has a legal system that is deemed equivalent to the Japanese Personal Data protection system, designated by the Commission; or

iii. the recipient undertakes adequate precautionary measures for the protection of Personal Data, as specified by the Commission.
The Commission has not yet published the list of countries that have "a legal system deemed equivalent to the Japanese Personal Data protection system" mentioned in item (ii) above.

With regard to item (iii), the regulations provide that in order to apply this exception, the recipient (a) has to agree with the transferring party to implement measures that comply with the obligations concerning the handling of Personal Data under the amended APPI in an appropriate and reasonable manner, or (b) must be certified under the international scheme concerning handling of personal information.

“International scheme” refers to the certification under the Asia-Pacific Economic Cooperation’s Cross-Border Privacy Rules. Other schemes, such as the certification of Binding Corporate Rules under the EU regulations, are not recognized as an “international scheme” under the APPI yet.

12. Security Requirements

The APPI states that business operators must take necessary and appropriate measures to prevent leakage, loss or damage of Personal Data and ensure proper security management thereof. This requirement is further built into industry-specific guidelines.

In particular, under the APPI Guidelines, business operators are recommended to establish and manage a system to report any data security breach to:

- the Data Subject(s) who may be affected by the breach; and
- administrative authorities.

In certain industrial sectors such as banking or financial business, the reporting of such breaches is mandatory and business operators are required to make public announcements about the factual background as well as measures they intend to implement to prevent similar data security breaches in the future.

13. Special Rules for Outsourcing of Data Processing to Third Parties

See comments under Section 5.

14. Enforcement and Sanctions

The APPI imposes sentences of imprisonment (with labor) for up to six months, or a fine of up to JPY 300,000 for certain breaches. Under the amended APPI, current or past executive members, officers, or employees of business operators who disclose personal information retained by the business operators to a third party in order to gain unjust benefit can be
punished by imprisonment (with labor) for up to one year, or a fine of up to JPY 500,000.

However, such sentences or fines may only be imposed in cases where there has been a breach of a Commission’s order made under the APPI. So far, no such orders have been made. As such, no sentences or fines have yet been made.

15. Data Security Breach

There are no legal requirements to notify a breach of the APPI to a government organization. However, the Guidelines on the Act on Protection of Personal Information: Actions to Take in case of Leakage (“Security Breach Guidelines”) recommend that business operators:

- report any data leakage to an internal responsible person;
- investigate the factual background and cause of leakage;
- identify the scope of influence caused by data leakage;
- consider and take preventive measures;
- report the Data Subject(s) who may be affected by the data leakage; and
- publicly announce the factual background and the preventive measures.

The Security Breach Guidelines also recommend that business operators report any data leakage incidents to the Commission in principle. However, there are special organizations set up to specifically handle complaints relating to Personal Information on an industry level. These organizations are referred to as “authorized personal information protection organizations”. The Security Breach Guidelines provide that if a business operator engages in a business subject to supervision by a certain authorized personal information protection organization, the business operator needs to report the data leakage incident to the organization, not to the Commission.

Business operators are not required to report the data leakage incidents to the Commission where (i) the Personal Data or anonymizing methods are not substantially leaked or (ii) minor data leakage incidents (erroneous facsimile or mail transmissions and miscarriage) occurs.

To date, all data security breaches have been handled by companies taking the initiative and paying Data Subjects small amounts of compensation where breaches have occurred. There have been no instances of government agencies taking action against companies for data security breaches.
16. Accountability
Japan does not recognize the concept of a Data Processor. Accountability lies with the business operator, which is similar to a Data Controller under EU law.

17. Whistle-Blower hotline
There are no laws or regulations governing whistle-blower hotlines in Japan.

18. E-Discovery
There are no laws or regulations governing the implementation of an e-discovery system in Japan.

19. Anti-Spam Filtering
There are no laws or regulations governing the implementation of an anti-spam filtering system in Japan.

20. Cookies
There are no specific provisions in either the APPI or the various guidelines on the use of electronic cookies.

21. Direct Marketing
Other than the general provisions dealing with transferring Personal Information to third parties, there are no specific provisions dealing with direct marketing. Please note, however, that the sending of advertisement emails is regulated by a separate law named “The Act on Regulation of Transmission of Specified Electronic Mail”. Under this act, advertisement emails may not be sent unless prior consent of the recipient is obtained.
1. Recent Privacy Developments

The adoption of the European General Data Protection Regulation ("GDPR") and the necessity highlighted by the CNPD to recast the Luxembourg data protection legislation

a. status and scope of local legislation supplementing GDPR

The GDPR will start to apply directly in the Member States on 25 May 2018, following a two-year transition period to allow the public and private sectors to get ready for the new rules. Several sections of the GDPR, however, allow or require national laws to provide specific rules.

In light of this, in its activity report for the year 2016 published on 14 September 2017, the Luxembourg National Commission for the Protection of the Data ("CNPD") has highlighted the necessity to recast the Luxembourg data protection legislation currently applicable in Luxembourg. Such recasting would have the effect of preventing the current national legislation from inhibiting the effectiveness of the provisions of the GDPR and would make use of the opening clauses of the GDPR.

A first draft of the bill of law modifying the law of 2 August 2002, as amended, on the Protection of Persons with regard to the Processing of Personal Data has been presented and is aimed mainly at simplifying the administrative obligations applicable to certain types of processing, such as for the processing of Personal Data for monitoring purposes.

In addition, a second draft bill establishing the National Commission for Data Protection and implementing the GDPR has been filed on 12 September 2017 by the Ministry of Communication & Media in Luxembourg (Draft Bill – N°: 7184).

The draft bill confirms and extends the competences of the CNPD, which will notably be empowered to:

- monitor compliance with the GDPR by any Data Controller or processor (as well as with the draft bill n°7168 regarding data processing in criminal matters and matters of national security);
- have legal standing and initiate judicial proceedings in the interests of the GDPR;
- require from any Data Controller or processor all the necessary information to assess their compliance with the GDPR;
- order a Data Controller/processor to suspend or stop the processing of Personal Data;
- impose administrative penalties and sanctions on parties found to have infringed the GDPR (with periodic penalty payments when necessary).
The draft bill also provides for specific provisions that would “complement” the GDPR in matters that were left to the discretion of the Member States:

First, the draft bill grants some exemptions from the GDPR’s obligations in case of:

- data processing for the purposes of journalism, university research, art or literature (art. 56 of the draft bill); and in case of
- data processing for the purposes of statistics or scientific or historical research, provided that such “limitations” are proportional to the aim pursued and take into consideration the nature of the data and of the processing (art. 57 of the draft bill). The counterpart of the exemptions is a long list of additional safeguards that Data Controllers processing data for statistics or scientific or historical research must put in place, including, as the case may be, the designation of a Data Protection Officer and the conduct of a Data Protection Impact Assessment (art. 58 of the draft bill).

Second, regarding the processing of sensitive data, including health data, the draft bill confirms that such processing is allowed for the relevant medical bodies and healthcare professionals in the framework of their activities, as well as for research bodies (with appropriate safeguards), social security organisms, insurance companies, pension funds, the Medical and Surgical Mutual Fund and other approved organisms. The lawful transfer of sensitive data between these actors is also facilitated.

b. local regulator guidance and activities

The CNPD has collaborated on the current legal work and publishes guidance and recommendations on its website with respect to the upcoming new legislation.

In addition, to support the stakeholders in their task of incorporating the provisions of the general rules on data protection in their in-house policies, the CNPD decided to work with the LIST, with support from Digital Lëtzebuerg, on developing a Compliance Support Tool. A tool of this kind is a contribution to the Grand Duchy’s aim of digitizing and simplifying procedures, particularly those concerning compliance with the present and future framework of regulations.

The aim of the Compliance Support Tool is to draw up an innovative, intuitive solution enabling users to check the level of maturity of their organisations. The tool will allow users not only to manage a processing register, together with all the other documents necessary for demonstrating their responsibility, but also to monitor the evolution of the level of maturity of their organisations.
The invalidation of the “Safe Harbor” decision by the Court of Justice of the European Union: the steps taken in Luxembourg

On 6 October 2015, the Court of Justice of the European Union issued a decision in Maximilian Schrems v. Data Protection Commissioner by which it invalidated the “Safe Harbor” arrangement. From that date, companies are no longer able to transfer personal information of individuals to the United States using as a basis the “Safe Harbor” decision.

Following that decision, the CNPD sent, on 25 and 26 November 2015, a letter to all companies that were known by the authority for exporting Personal Data to the United States based on the “Safe Harbor” decision. Data exporters were expressly required to take, without delay, active steps in order to ensure that they were lawfully transferring data to the United States.

In Luxembourg, a transfer of Personal Data to countries not considered as ensuring an adequate level of protection of privacy, such as the United States, may be legitimised and thus considered as lawful, where they are based on a justification provided by the law. If not, they should be authorized by the CNPD which would analyze the steps taken by the data exporter to ensure an adequate level of protection of privacy, for example the adoption of binding corporate rules by a group of companies transferring data between the different entities. The Privacy Shield constitutes an alternative solution for lawfully transferring data to the United States.

Activity report for the year 2016 from the CNPD published on 14 September 2017 reveals a record number of complaints filed by individuals

On 14 September 2017, the CNPD published its activity report for 2016. The report reveals a record number of complaints or requests for verification filed from individuals and requests for information which have constantly increased since 2011. Most of the complaints have been filed by citizens of other EU Member States, which can be attributed to the fact that numerous international companies operate in Luxembourg.

Out of 185 complaints, 77 led to inspections and investigations regarding shortcomings such as illegal monitoring of employees, failure to adequately handle access, rectification or deletion requests, and illegal data communications to third parties.

2. Emerging Privacy Issues and Trends

Internet of Things: Following the development of an increasing number of devices connected to the Internet and the security issues arising from this new trend, the CNPD is paying close attention to the Internet of Things. The authority takes into consideration the risks to privacy, as well as the impact on
the protection of Personal Data of Data Subjects and has proposed tools that can be used and which will provide protection when using such devices.

**Privacy by design:** A current point of focus and discussion among stakeholders in privacy matters in Luxembourg is the question of privacy by design. This concept refers to a way of protecting privacy by embedding it into the design specifications of technologies, business practices, etc., and decreasing the risk of security as regards to the processing of Personal Data of users. Following this approach, data protection safeguards should be built into products and services from the earliest stage of development. The notion of privacy by design has, in addition, been expressly set out as a principle by the GDPR. In its activity report for the year 2016, published on 14 September 2017, the CNPD announced the development of its guidance mission in order to help public and private actors to notably implement this principle in their daily practice.

3. **Law Applicable**

The applicable law is the law of 2 August 2002, as amended, on the Protection of Persons with regard to the Processing of Personal Data (“Law of 2002”).

Further data protection provisions are contained in legislation regulating specific sectors, such as the law of 28 July 2011 amending the law of 30 May 2005, concerning the protection of privacy in the electronic communication sector.

As of 25 May 2018, the GDPR will be directly applicable in Luxembourg as supplemented by the incoming national legislation mentioned under 1. The below does not reflect the rules coming in under GDPR.

4. **Key Privacy Concepts**

a. **Personal Data**

The Law of 2002 applies to any information (“Personal Data”) of any type regardless of the type of medium, including sound and image, relating to an identified or identifiable natural person (“Data Subject”). Natural persons will be considered to be identifiable if they can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to their physical, physiological, genetic, mental, cultural, social, or economic identity.

b. **Data Processing**

“Processing” is widely defined and covers any operation or set of operations performed on Personal Data, whether or not by operated means, such as the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise
making available, alignment or combination, as well as blocking, erasure or destruction of Personal Data.

c. **Processing by Data Controllers**
The Law of 2002 applies to a natural or legal person, public authority, agency or any other body other than the Data Subject which, solely or jointly, determines the purposes and methods of processing Personal Data ("Data Controller").

d. **Jurisdiction/Territoriality**
The Law of 2002 only applies:

- if the Data Controller is established in the territory of the Grand Duchy of Luxembourg; or

- if the Data Controller is not established in Luxembourg or in another EU member State, but utilizes “equipment of processing” based in Luxembourg territory, apart from equipment that is used only for the purposes of transit through the said territory.

e. **Sensitive Personal Data**
As a principle, the processing of Sensitive Personal Data, that is, data relating to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, or health or sexual life, is prohibited.

However, the Law of 2002 provides a list of exceptions to this prohibition. Sensitive Personal Data may be processed if:

- the Data Subject has given his/her express (i.e., written) consent subject to certain restrictions;

- the processing is necessary for the purpose of carrying out the obligations and specific rights of the Data Controller in the field of employment law in so far as it is authorized by law;

- the processing is necessary to protect the vital interests of the Data Subject or another person, where the Data Subject is physically or legally incapable of giving consent;

- processing is carried out with the consent of the Data Subject by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade union aim in the course of its legitimate activities and on the condition that the processing relates to the necessary data solely of members of that body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to third parties without the consent of the Data Subject;
• the processing relates to data that has clearly been made public by the Data Subject;
• the processing is necessary to acknowledge, exercise or defend a right at law;
• the processing is necessary in the public interest for historical, statistical or scientific reasons;
• the processing is implemented via a specific Luxembourg regulation, such as the processing of operations relating to State security, defense and public safety; or
• the processing is implemented in the context of the processing of legal data, i.e., the processing of data for the purpose of criminal investigations and legal proceedings and data related to offenses, criminal convictions or security measures.

There are specific additional requirements in relation to the processing of genetic data and the processing of specific categories of data by health-related services.

f. Employee Personal Data
The Law of 2002 does not provide for specific rules regarding Employee Personal Data.

When such data is likely to include Sensitive Personal Data (e.g., health-related information), the data may be processed in the circumstances mentioned in Section 4(e) above and, in particular, for the purpose of carrying out the Data Controller’s obligations under employment law.

5. Consent
a. General
Consent of the Data Subject is not specifically required by Luxembourg law. It is, however, considered as a justification for the collection, processing and use of Personal Data. Written consent is not required, except for Sensitive Data.

When a Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to. In addition, a Data Subject has the right to withdraw consent at any time in given circumstances.

b. Sensitive Data
Where consent is relied upon to justify the processing of Sensitive Personal Data, it must be explicit and must be either written or obtained by a double-click, if consent is given over the Internet.
c. Minors
Minors under the age of 18 cannot give valid consent. The consent of a parent or guardian is required on their behalf. Further, the parent or guardian has the right to be informed of the collection of information and to access and rectify the Personal Data.

d. Employee Consent
While consent of employees is not specifically required by Luxembourg Law, the Article 29 Working Party has produced an opinion on the processing of Personal Data in the employment context which states that it is not appropriate for an employer to try to rely on an employee’s consent as it is unlikely to be freely given.

The CNPD has raised doubts as to whether consent given in the context of an employment relationship can be considered valid. There is a risk that the employee may feel forced to consent.

e. Online/Electronic Consent
In the case of non-Sensitive Personal Data, consent may be given electronically, and will be considered to have been properly demonstrated where it can be shown that the Data Subject had sufficient notice of the requisite information forming the basis of consent (e.g., inclusion of a notice or policy in a box directly above a consent button) and steps have been taken to prevent consent from being mistakenly given (e.g., a double-click acceptance process). Where written consent is required by law (e.g., regarding Sensitive Data), further requirements need to be met.

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) its privacy practices (which must be provided in a clear and transparent way); (v) third parties to which the organization will disclose the Personal Data; (vi) the consequences of not giving consent; (vii) the rights of the Data Subject; (viii) where the Personal Data is to be transferred; (ix) where the Personal Data is to be stored; (x) how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; (xi) how to make an inquiry or file a complaint; and (xii) how to access and/or correct the Data Subject’s Personal Data.

7. Processing Rules
An organization that processes Personal Data must: (i) limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; (ii) and
delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and of how the Data Subject’s Personal Data is being processed; (ii) access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements
Data Controllers must notify the CNPD prior to the processing of Personal Data. The Law of 2002 provides for a list of cases where the Data Controller is exempt from the notification requirement. The exemption mainly applies to the processing of data concerning employees’ wages and/or payroll, as well as clientele management, book-keeping, and the administration of shareholders.

10. Data Protection Officers
The appointment of a data protection officer is possible but is not mandatory. Should a data protection officer be designated by the Data Controller, specific formalities defined by the Law of 2002 will apply. There is no requirement for such officer to be located in Luxembourg.

11. International Data Transfers
Transfers of Personal Data from Luxembourg to EEA Member States are generally permitted without the need for further approval. The same applies to transfers to Andorra, Australia, Faroe Islands, Switzerland, Israel, Jersey, Guernsey, Argentina, the Isle of Man and Canada.

The Data Controller may transfer the Personal Data to a state not offering a sufficient level of protection of privacy in the following cases:

- the Data Subject has given consent to the proposed transfer;
- the transfer is necessary for the performance of a contract to which the Data Subject and the Data Controller are parties or which has been concluded in the interest of the Data Subject between the Data Controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of a legal claim;
- the transfer is necessary in order to protect the vital interests of the Data Subject; or
• the transfer occurs from a public register.

According to the Article 29 Working Party, the above-mentioned conditions must be interpreted strictly.

Without prejudice to the exceptions listed above, the transfer of Personal Data to a “non-safe” country is legal if it has been authorized beforehand by the CNPD. Such authorization is granted only if the following conditions are met:

• Initial processing of Personal Data complies with the Law of 2002: the initial processing of Personal Data has to comply with the requirements related to the quality and security of the Personal Data processed, the legitimacy of the processing, and the information of the Data Subject; and

• Contractual clauses: the CNPD’s authorization to transfer the Personal Data to a “non-safe” country may be granted if the Data Controller offers sufficient guarantees in respect of the protection of privacy, freedoms and fundamental rights of the Data Subjects, as well as the exercise of the corresponding rights, and that these guarantees may result from appropriate contractual clauses.

The CNPD will always accept data transfer agreements incorporating the model contractual clauses approved by the European Commission for transfers from Data Controller to Data Controller or from Data Controller to Data Processor.

Alternatively, another form of securing the transfer of Personal Data within the same corporate group consists of applying binding corporate rules (“BCR”) with which any organization of the group will need to comply.

The general rules concerning the legality of processing must always be fulfilled.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.
13. Special Rules for Outsourcing of Data Processing to Third Parties

According to the Law of 2002, any processing carried out on another’s behalf must be governed by a written contract (data processing agreement) or legal instrument binding the Data Processor to the Data Controller and providing in particular that:

- the Data Processor will act only on instructions from the Data Controller; and
- the Data Processor has the obligation to implement adequate appropriate technical and organizational measures.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

There is no legal obligation to notify data security breaches under the Law of 2002. The Data Controller could, however, always decide, depending on the importance of the breach, to inform the authority or the affected individual on a voluntary and purely informative basis, based on an internal management decision and not as a consequence of a legal requirement. The only existing obligations to provide notice of a breach of security is in the sector of electronic communications and networks. A specific form allowing a Data Controller to notify of data security breaches is available on the website of the National Commission for Data Protection.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions.

16. Accountability

There is currently no law/regulation/guidance materials in Luxembourg that mandate organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

The Law of 2002 is silent with respect to whistle-blower hotlines. On 11 May 2009, the CNPD published on its website, a “thematic file” on the issue and
indicated that their position is in line with the Opinion WP 117 issued by the Article 29 Working Party on 1 February 2006.

Nevertheless, a whistle-blowing system has to be notified to the CNPD beforehand.

Should the system imply the permanent monitoring of employees by technical instruments, the filing of a prior authorization is also needed.

18. E-Discovery

An organization implementing an e-discovery system is not required to obtain the consent of employees even if the collection of Personal Data is involved. The organization is also not mandated to advise employees of the implementation of an e-discovery system, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace. Spam-filtering solutions will need to comply with applicable data protection laws. A notification will need to be filed before the CNPD. Additionally, the storage and access to location and traffic data must be performed in compliance with the Law of 2011.

20. Cookies

There are specific laws/rules that regulate the deployment of cookies; and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. An organization must obtain consent for a specific activity. Bundled consent is not considered valid consent.
Malaysia

Brian Chia
Kuala Lumpur
Tel: +603 2298 7999
brian.chia@wongpartners.com

Shameen Mohd. Haaziq Pillay
Kuala Lumpur
Tel: +603 2298 7943
shameen.mohd.haaziqpillay@wongpartners.com
1. Recent Privacy Developments

A data user will now have to comply with the Security, Retention and Data Integrity Standards.

The Malaysian Personal Data Protection Act 2010 (“PDPA”) came into force on 15 November 2013 together with various regulations.

These are the Personal Data Protection Regulations 2013 (“Regulations”), Personal Data Protection (Class of Data Users) Order 2013, Personal Data Protection (Fees) Regulations 2013, and the Personal Data Protection (Registration of Data User) Regulations 2013. On 16 March 2016, the Personal Data Protection (Compounding of Offences) Regulations 2016 came into effect. The Personal Data Protection Commissioner (“Commissioner”) issued the Personal Data Protection Standards (“Standards”), effective from 23 December 2015. Data users need to comply with the Standards, which provide for matters relating to, among others, security measures in relation to conventional and electronic data management, the requirement to destroy data collection forms within a prescribed period and measures to ensure that Personal Data that is retained is accurate, complete and up-to-date.

Prior to the coming into force of the PDPA, information of a personal nature was protected only as confidential information through sectoral secrecy obligations, contractual obligations or common law.

The PDPA seeks to govern the previously unregulated area of Personal Data processing by data users in the context of commercial transactions, and to provide safeguards for Data Subjects such as consumers, employees and e-commerce users. “Commercial transactions” are defined broadly to encompass transactions of a commercial nature, whether contractual or not, and include matters relating to the supply or exchange of goods and services, agencies, investment, financing, banking and insurance. There was a three-month transitional period for compliance in respect of Personal Data collected prior to the PDPA coming into force. The PDPA is a Code of Practice (“Code”) based regime. To date, the Code for the Utilities, Insurance, and Banking sectors have been introduced.

On 3 May 2017, a local private college was the first data user to be charged in the Sessions Court for processing Personal Data of former employees of the college without a valid certificate of registration issued by the Commissioner, contrary to section 16(1) of the PDPA. Section 16(1) provides that certain classes of data users must be registered and issued with a valid certificate of registration by the Commissioner.

The charge, under section 16(4) of the PDPA, provides that in the event of conviction, the college would be liable to a fine of up to RMB 500,000, or imprisonment of its officer(s) for up to three years, or both. Enforcement is expected to be more rigorous moving forward.
2. Emerging Privacy Issues and Trends
   a. The Insurance, Utilities, and Banking Codes have been introduced in the past year.
   b. These Codes have generally clarified some of the following issues:
      i. instances and situations whereby consent of Data Subjects’ may be deemed;
      ii. instances whereby the retention of Personal Data is permissible following the withdrawal of consent; and
      iii. types of information that are not covered under the PDPA, which includes for instance, data relating to a deceased person and/or a company/society/partnership.
   c. The Commissioner has not made any substantive official announcements, but we would expect the following matters to be eventually dealt with through Codes or other official guidelines:
      i. retaining or otherwise processing the information stored within the Data Subject’s national identification card;
      ii. clarification on Personal Data contained in business cards. The PDPA has no business information-related exceptions’ and
      iii. data breach notification obligations.

3. Law Applicable

Apart from the PDPA, the various regulations are: the Regulations, Personal Data Protection (Class of Data Users) Order 2013, Personal Data Protection (Fees) Regulations 2013, the Personal Data Protection (Registration of Data User) Regulations 2013, and the Personal Data Protection (Compounding of Offences) Regulations 2016. On 23 December 2015, the Standards were issued.

The Commissioner has also approved and registered the following Codes:

a. Personal Data Protection Code of Practice for the Utilities Sector (Electricity), effective from 23 June 2016;

b. Personal Data Protection Code of Practice for the Insurance/Takaful Industry, effective from 23 December 2016; and

4. Key Privacy Concepts

The PDPA sets out a broad framework for the protection of Personal Data. The scope and application of the PDPA are/will be fleshed out through Codes.

a. Personal Data

Under the PDPA, “Personal Data” means any information in respect of commercial transactions which:

- is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- is being recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

and that relates directly or indirectly to a Data Subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any Sensitive Personal Data and expressions of opinion about the Data Subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

There are seven data protection principles which form the basis of protection of Personal Data under the PDPA. The principles are as follows:

- General Principle;
- Notice and Choice Principle;
- Disclosure Principle;
- Security Principle;
- Retention Principle;
- Data Integrity Principle; and
- Access Principle.

b. Data Processing

The scope of the PDPA extends to Personal Data that is recorded in a form which may practically be processed by any automatic means or otherwise, including both electronic and manual processing. If the information is not recorded (e.g., in oral form or manual unconsolidated data), it will be excluded from the scope of the PDPA. “Processing” is defined under the PDPA as
collecting, recording, holding or storing of Personal Data or carrying out any operation or set of operations on the Personal Data, including the:

- organization, adaptation or alteration of Personal Data;
- retrieval, consultation or use of Personal Data;
- disclosure of Personal Data by transmission, transfer, dissemination or otherwise making available; or
- alignment, combination, correction, erasure or destruction of Personal Data.

c. Processing by Data Processors

The PDPA defines a “data user” as a person who either alone or jointly or in common with other persons processes any Personal Data or has control over or authorizes the processing of any Personal Data, but does not include a Data Processor.

Note that a person who merely collects, holds, processes or uses Personal Data solely on behalf of another person, and not for any of his own purposes may be construed as “Data Processor” under the PDPA. There are different requirements applicable to ensure that the Personal Data processed by Data Processors is protected.

d. Jurisdiction/Territoriality

The scope of the PDPA only extends to Personal Data that is processed in Malaysia. The PDPA will not apply to any Personal Data processed outside Malaysia, unless the Personal Data is intended to be further processed in Malaysia.

While it is not expressly stated in the PDPA, the Personal Data Protection Department (“Regulator”) has verbally confirmed that the provisions of the PDPA apply only apply to living individuals. Personal Data processed only for the purpose of an individual’s personal, household affairs and for recreational purposes is exempted from the PDPA.

In addition, the federal and state governments are excluded from the PDPA. Credit reporting or referencing agencies are separately regulated by the Credit Reporting Agencies Act 2010.

e. Sensitive Personal Data

Under the PDPA, “Sensitive Personal Data” is defined broadly as any Personal Data consisting of information as to the physical or mental health or condition of a Data Subject, his/her political opinions, his/her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him/her of any offense or any other Personal Data as the Minister may determine by order published in the Gazette.
The PDPA prohibits any person from collecting, holding, processing or using any Sensitive Personal Data unless the Data Subject has given his or her explicit consent. Exceptions include where the processing of Sensitive Personal Data is required for the administration of justice or for medical purposes.

f. **Employee Personal Data**
The scope of the PDPA is only limited to commercial transactions. Notwithstanding that an employment relationship is not typically regarded as a “commercial transaction”, the Regulator has verbally confirmed that the provisions of the PDPA apply to employers who process Employee Personal Data.

5. **Consent**
a. **General**
The PDPA prohibits the processing of Personal Data without the consent of the Data Subject for any purpose other than the purpose for which the Personal Data was to be used at the time of its collection, unless such other purpose is directly related to the purpose for which the Personal Data was to be used at the time of its collection.

Consent of the Data Subject is not necessary if the use of the Personal Data falls under any of the following exceptions:

- performance of a contract to which the Data Subject is a party;
- for the taking of steps at the request of the Data Subject with a view to entering into a contract;
- compliance with any legal obligation to which the data user is subject, other than an obligation imposed by a contract;
- protection of the vital interests of the Data Subject;
- administration of justice; or
- exercise of any functions conferred on any person by or under any law.

The PDPA does not specify the form or nature of the consent and whether consent can be implied by conduct (but see discussion below regarding “explicit consent” for the processing of Sensitive Personal Data).

The Codes for the Utilities, Banking, and Insurance sectors do provide instances whereby consent can be deemed. These include, under the Insurance Code, where the processing is necessary to carry out Data Subjects’ instructions for insurance-related purposes, and under the Banking and Utilities Code, consent may be deemed where the Data Subject does not
object to the processing of his/her Personal Data, the Data Subject voluntarily discloses his/her Personal Data, and/or the Data Subject proceeds to use the services of the data user.

The Data Subject also has the right to withdraw consent at any time in any given circumstances.

b. **Sensitive Data**

“Sensitive Personal Data” requires “explicit” Data Subject consent. “Sensitive Personal Data” includes medical history, religious beliefs, political opinions and the commission or alleged commission of any offense. “Explicit consent” implies that such consent must be in writing and that relatively more detailed information from the data user will be required before the consent can be regarded to be sufficient. This also indicates that under the PDPA, consent with regard to (non-Sensitive) Personal Data need not always be in writing and can be implied.

Explicit consent is not required in certain circumstances – for example, the use or disclosure of data is necessary to protect the vital interests of the Data Subject or another person. Otherwise, the processing of the data is prohibited.

“Explicit consent” implies that such consent must be in writing, and that there must be an additional level of detail relating to the purpose of the processing. This also indicates that consent with respect to the processing of non-Sensitive Personal Data can be implied.

c. **Minors**

The Regulations provide that with respect to the processing of the Personal Data of a person who is under the age of 18, consent is to be obtained from the parent, guardian or persons with parental responsibility.

d. **Employee Consent**

Under the PDPA, the consent of employees (as Data Subjects) needs to be obtained for the processing of the employees’ Personal Data (which includes Sensitive Personal Data).

e. **Online/Electronic Consent**

In Malaysia, electronic consent is permissible and enforceable provided that it is properly structured and evidenced.

In relation to commercial contracts, the Malaysian Electronic Commerce Act 2006 (“MECA”) expressly provides that any information shall not be denied legal effect, validity or enforceability on the ground that it is wholly or partly in an electronic form. Note, however, that the MECA applies only to commercial contracts and not to Personal Data in particular.
While there is no provision in the PDPA that specifically addresses online/electronic consent, the Regulator has verbally confirmed that this is permissible for the purposes of the PDPA.

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the description of the Personal Data processed; (iii) the purposes for collecting and further processing the Personal Data; (iv) the source of the Personal Data; (v) third parties to which the organization will disclose the Personal Data; (vi) whether it is obligatory or voluntary for Data Subjects to supply the Personal Data and if obligatory the consequences of not providing consent; (vii) the rights of Data Subjects to request access to and correct of their Personal Data and how to contact the data user or a contact person within the organization in order to make an inquiry or file a complaint; and (viii) the Data Subjects’ right to limit the processing of their Personal Data.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access their Personal Data subject to some restrictions and/or qualifications; (iii) request the correction of their Personal Data; and (iv) request the deletion and/or destruction of their Personal Data.

9. Registration/Notification Requirements

Organizations that collect and process Personal Data may be required to register with the Regulator.

Certain classes of data users are required to register with the Regulator. These include, among others, licensed banks, insurers, private health care institutions, licensed tour operators, direct sales businesses, private higher education institutions and certain utilities and transportation service providers. These data users have a three-month period from enforcement to register. Data users who fail to do so may be liable for a fine of up to MYR 500,000 and/or a term of imprisonment of up to three years. Directors, managers and other responsible persons may be found to be jointly liable with the non-
complying data user. The Commissioner is not empowered to order compensation for damage suffered, and there is no express right to pursue a civil claim for non-compliance.

10. Data Protection Officers
The PDPA is silent as to whether organizations are required to designate a privacy officer or any other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
The PDPA prohibits data users (and by extension, their Data Processors) from transferring any Personal Data of a Data Subject to a place outside Malaysia, unless:

- it is to a place specified by the Minister and published in the Gazette;
- the Data Subject has given his or her consent; or
- any other general exemptions apply.

The factors that the Minister will take into consideration include: whether or not that place has in force any law which is substantially similar to the PDPA or serves the same purposes as the PDPA and whether that place ensures an adequate level of protection in relation to the processing of Personal Data which is at least equivalent to the level of protection afforded by the PDPA. No places have been officially published by the Minister thus far.

In April 2017, the Regulator issued a public consultation paper on the draft Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017 which specifies a “whitelist” of countries in which Personal Data from Malaysia can be transferred to. Under the PDPA, a data user has to satisfy certain conditions set out under section 129(3) of the PDPA prior to any cross-border transfer of Personal Data, unless the Personal Data is transferred to the “whitelist” jurisdictions. When the whitelist is finalized, data users will be able to transfer Personal Data to countries on the whitelist without relying on any particular exemption.

12. Security of Personal Data
Organizations are required to take steps to: (i) ensure that Personal Data in their possession and control is protected from unauthorized access and use; (ii) implement appropriate physical, technical and organization security safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved. The Regulations mandate that all data users must develop and implement a security policy which complies with the Security Standard as set out from time to time by the Commissioner. Some of the Security Standards
include: (a) registering employees who are involved in the processing of Personal Data; (b) discontinuing the access rights of employees pursuant to the termination of their employment; (c) ensuring employees who have access to Personal Data have individual user ID and passwords; (d) protecting computer systems from malware threats; and (e) implementing safety procedures such as the installation of close circuit television in the data storage location and/or 24-hour daily security.

13. Retention of Personal Data
The Standards require data users to take reasonable steps to ensure that all Personal Data is destroyed or deleted permanently. Some of the measures pursuant to the Standards include: (i) preparing and managing a Personal Data disposal record which shall be disclosed when requested by the Commissioner; (ii) disposing all Personal Data collection forms in respect of commercial transactions within a period not exceeding 14 days, unless the form has legal value relating to the commercial transaction; and (iii) implementing a Personal Data disposal schedule for Personal Data which is inactive for a period of 24 months.

14. Data Integrity of Personal Data
The Standards require data users to take reasonable steps to ensure that Personal Data is accurate, complete, not confusing and updated by taking into consideration the meaning, including any directly-related meaning, for which Personal Data is collected and further processed. Some of the measures include preparing Personal Data update forms to be filled by Data Subjects whether online or through conventional means and announcing the updating of Personal Data either through a portal or by displaying a notification on the premises or by any other suitable means.

15. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and are required to comply with applicable sector-specific requirements. Organizations may, depending on the particular circumstances, be liable together with third-party providers in cases of breaches by the latter.

Under the PDPA, where a Data Processor processes Personal Data on behalf of the data user, the data user shall, for the purpose of protecting the Personal Data from any loss or misuse, ensure that the Data Processor:

- provides sufficient guarantees in respect of the technical and organizational security measures governing the processing; and
- takes reasonable steps to ensure compliance with those measures.
The Security Standard requires that a contract be entered into between the data user and the Data Processor for the purposes of ensuring the security of the Personal Data.

16. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, and/or criminal proceedings, which could result in imprisonment of the directors, managers and other persons responsible if the data user is found guilty.

Pursuant to the Personal Data Protection (Compounding of Offences) Regulations 2016, certain data protection offenses may be “compounded” instead of being formally prosecuted. The Commissioner may, with the consent of the Public Prosecutor, make an offer to an alleged offender to compound a compoundable offense. The offer may be made any time after the offense has been committed and before any prosecution has been instituted in relation to it. The Commissioner may determine the amount to be paid by the offender which must not exceed 50% of the maximum fine for the relevant offense. Where an offense is compounded, no prosecution may be instituted against the offender in respect of that offense.

17. Data Security Breach

At present, there is no positive obligation to notify the Regulator or Data Subjects in the event of a security breach. Such notification may, however, be taken into account when assessing whether the data user has complied with the Security Principle.

A breach of any of the data protection principles is an offense under the PDPA and is punishable by a fine of up to MYR 300,000, and/or up to two years’ imprisonment.

18. Accountability

Organizations are not legally required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

19. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Malaysia as long as they are in compliance with local laws.

20. E-Discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of the employees if the processing of Personal Data is
involved, and to advise employees of the implementation of the system, workplace surveillance and on the storage of information.

21. Anti-Spam Filtering

Under the Communications and Multimedia Act 1998 (“1998 Act”), it is an offense for any person to intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept, any communications including communication via electronic means. It is possible that a spam-filtering solution installed by an employer may be tantamount to intercepting its employees’ communications. The issue of whether or not the employees had given consent is irrelevant under the 1998 Act. Nevertheless, it is not uncommon for large organizations to implement a spam-filtering system whereby suspected spam emails are isolated.

A general spam filter should not fall foul of the 1998 Act, when the system merely gives the receiver of suspected spam email the option to allow these spam emails to be forwarded to his or her inbox and to create rules that future emails from the same email account will not be filtered.

22. Cookies

There are no specific laws/rules in Malaysia that regulate the use and deployment of cookies. In general, the use of cookies is valid as long as it complies with data privacy laws.

23. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which may not be inferred from a Data Subject’s failure to respond.
Mexico

Sergio Legorreta-Gonzalez
Mexico City
Tel: +52 55 5279 2954
sergio.legorreta-gonzalez@bakermckenzie.com

Carlos Vela-Treviño
Mexico City
Tel: +52 55 5279 2911
carlos.vela-trevino@bakermckenzie.com
1. Recent Privacy Developments

**Mexican Safe Harbor Program: Finally ready**

Under the Federal Data Protection Law (“FDPL”), companies may develop and implement self-regulation schemes (“SREs”), such as BCRs. Corporations that register their SREs with the Mexican Data Protection Authority (“INAI”) are granted regulatory benefits, such as lesser fines in case of infringement. In order to obtain a registration, companies must file with the INAI, which is entitled to review and approve the SRE if it complies with minimum regulatory requirements. INAI has already started receiving applications.

Likewise, NYCE, a non-profit organization with substantial expertise on certification matters, has been authorized by the Mexican government to issue certificates of compliance in connection with the Mexican FDPL; NYCE will audit the self-regulation schemes developed by a company and, if they are compliant with the law, will issue the certificate of compliance. Companies that obtain NYCE certificates will be imposed lesser fines in case of non-compliance. Note that NYCE does not provide consultancy services or advice – it only carries out audits and identifies compliance gaps.

**Data Protection Authority issues guidelines on the safe deletion of Personal Data**

The INAI issued a new set of guidelines regarding the safe deletion of Personal Data. These guidelines cast light on the physical and logical means available to Data Controllers for the deletion of data once retention periods have expired and processing purposes are considered accomplished.

This guidance should allow companies to reduce the odds of third parties retrieving old or outdated information and using it for purposes other than those for which the information was originally collected and processed.

Considering that some legal retention periods in Mexico are quite long (10 years), the new guidelines should provide legal certainty to companies on how to most efficiently approach retention periods, handle documents and destroy Personal Data.

2. Emerging Privacy Issues and Trends

**Exorbitant fines for Personal Data Misuse.** INAI has continued its strong pace as an enforcement authority. Between January and June 2016, INAI imposed 22 fines on different companies, for an amount of up to USD 2.8 million, with banking, insurance and education services as the most penalized industries. Of particular relevance is the sanction imposed on a major Mexican financial institution, which was found to be processing Sensitive Personal Data of the wife of a credit applicant, without a legitimate reason and without
notice to either the applicant or his wife. This violation incurred a fine of over USD 1.5 million.

**Forgetting about the “right to be forgotten”?** In 2015, the INAI imposed a sanction on a major search engine provider because it rejected a petition filed by a Data Subject who requested certain information to be deleted from the indexed search results of the service in Mexico. The deletion request concerned a journalistic investigation report published by a magazine which associated the petitioner to possible fraud. INAI’s decision promptly fueled a debate around the so-called “Right to be Forgotten” and its potential repercussions on the freedom of speech. As part of this debate, the magazine, represented by a Mexican non-governmental organization, filed a claim before a court in order to evidence that INAI’s decision was illegal because it failed to involve the magazine in the proceeding. The magazine also argued that taking down such type of content jeopardized the fundamental right of freedom of speech and created a form of censorship. The court found that INAI’s decision breached the constitutional Right of Audience of the magazine and vacated the decision without effect. The process is set to start again, now with the magazine being part of the proceeding before the INAI.

**Data kept by telecom carriers for collaborating with justice authorities. Can it be accessed by the Data Subject as well?** Under the Mexican Federal Law of Telecommunications, telecom carriers must keep all records of written and/or oral communications of their users for a specific period, with the purpose of sharing such data with justice authorities to fight crimes; recently, the INAI issued a resolution obliging a major telecom carrier to deliver to a Data Subject all records held by the carrier under the telecom laws; the carrier is now facing legal proceedings and may be subject to fines.

### 3. Applicable law

**Legal Framework**

- Constitution of the United Mexican States (Articles 16 and 73).
- Federal Law on Protection of Personal Data Held by Private Parties.
- Regulations to the Federal Law on Protection of Personal Data Held by Private Parties.
- Recommendations on Security Measures.
- Parameters to design compliant self-regulation schemes.
- Mandatory Guidelines for Building Privacy Notices.
- Mandatory Guidelines for Video-Surveillance activities.
Relevant guidelines and recommendations

- Guidelines for Designing and Implementing a Privacy Office or Function.
- Guidelines for handling access, correction, cancelation and opposition rights request filed by Data Subjects.
- Guidelines for non-judicial, private collection services.
- Guidelines to prevent identity theft.
- Guidelines for appropriate deletion of Personal Data.

4. Key Privacy Concepts

a. Personal Data

Any information that refers to an identified or identifiable individual is considered to be personal data (“Personal Data”) under the Data Protection Law. The definition includes information of, among others, any of the following groups:

- customers and potential customers;
- suppliers/vendors/entity partners;
- employees; and
- other third parties/competitors.

b. Data Processing

The term “Data Processing” means the collection, use (i.e., access, handling, profiting, transferring and disposal), disclosure and storage of Personal Data and therefore comprises the whole life cycle of Personal Data processed within an organization. As a general rule, a Data Subject’s consent is required for any Data Processing activity. The Law applies to Personal Data held both in hard-copy and electronically, and to both manual and automated handling of data.

c. Processing by Data Controllers

A “Data Controller” is an individual or entity that takes decisions regarding the processing of Personal Data. Under the “Responsibility Principle” embraced by the Law, a Data Controller is responsible for complying with the obligations and data protection principles set forth by the Law, even if such data is transferred to a Data Processor, to an affiliate or to a third party, being such parties located in Mexico or abroad. A Data Processor (“Data Processor”) is an individual or an entity that solely or jointly with others, processes Personal Data on behalf of the Data Controller. The Data Processor, in order to be legally considered as such, should be a third party (i.e., it should not be an
entity related to the Data Controller or from the same corporate group) and
must operate under an agreement.

Since 6 July 2011, all Data Controllers have two notable obligations:

- all Data Controllers must deliver privacy notices to Data Subjects before
  the data is collected; and

- all Data Controllers must create within their organization a data protection
  function, either by appointing a Chief Privacy Officer or by creating a Data
  Protection Department.

Data Subjects are entitled to file, before the Data Controller’s Data Protection
Departments, requests related to ARCO (i.e., Access, Rectification,
Cancellation, Opposition) rights. Privacy Departments must receive and
process such requests, analyze if the petitions must proceed and resolve such
request within specific timeframes set forth by the Law.

Data Controllers are required to develop compliance programs and to allocate
resources in order to strengthen the privacy function.

d. Jurisdiction/Territoriality

The Data Protection Law is applicable to any individual or entity having a legal
domicile or local office or branch in Mexico, or where the managed databases
are located in Mexico. However, data protection rules apply also to Data
Controllers not based in the Mexican territory, if such entities use, for the
processing of Personal Data, means located within the Mexican territory. In
such a case, the Law provides that the Data Controller, even if located
abroad, shall incorporate the necessary mechanisms to comply with the Law.

e. Sensitive Personal Data

In Mexico, Sensitive Personal Data encompasses any data that may affect the
privacy and intimacy of the Data Subject. Certain data is considered, per se,
as Sensitive Personal Data: data that reveals racial or ethnic origin, present or
future health conditions, genetic information, religious, philosophic or moral
beliefs, union affiliation or sexual preference should at all times be considered
as sensitive data. However, other types of data could be considered as
sensitive in a specific context. In this regard, Personal Data that, if wrongly
used, may place the Data Subject in a dangerous situation or in a position of
being subject to discrimination should also be considered as sensitive data.

In general, the processing of Sensitive Personal Data is subject to more
stringent rules. Fines imposed if an entity fails to comply with applicable rules
are multiplied twofold when the breach relates to Sensitive Personal Data.

f. Employee Personal Data

There is no special regime applicable to employees, as Data Subjects, under
the Personal Data Law. Therefore, general rules apply to employees.
5. Consent

a. General
Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

Consent is generally contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is usually understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

Consent must be in the local language to be valid.

b. Sensitive Data
Mexican law recognizes Sensitive Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed with the express consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances.

c. Minors
While consent from minors is not specifically addressed in any law, the general rule is that minors are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor.

d. Employee Consent
The general rule is that employee consent is required to collect and process an employee’s Personal Data; however, there are instances when employee consent is not required, e.g., to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. Online/Electronic Consent
In Mexico, online or electronic consent is permissible and deemed effective if properly structured and evidenced.
6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the types of Personal Data being collected; the purposes for collecting Personal Data, its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the rights of the Data Subject; where the Personal Data is to be transferred; how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; and how to access and/or correct the Data Subject’s Personal Data.

7. Processing Rules

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; anonymize the Personal Data whenever possible; provide the Data Subject the option to use a pseudonym or remain anonymous whenever possible; and delete/ anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements

An organization that collects and processes Personal Data is not required to register, file and notify the appropriate data authority.

10. Data Protection Officers

In Mexico, organizations are required to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Organizations may transfer Personal Data outside of Mexico provided that impacted Data Subjects have been informed or have provided consent, and that reasonable steps have been taken to safeguard the Personal Data to be transferred.
Organizations may transfer Personal Data outside of Mexico provided that appropriate data transfer agreements (e.g., Model Contractual Clauses) or other prescribed measures are put in place; or binding corporate rules are implemented to secure international data transfers.

12. Security Requirements
Organizations are required to take steps to ensure that Personal Data in their possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of the occurrence of a data breach, the outsourcing organization may be held liable together with the third-party provider.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
Organizations that are involved in a data breach situation are required to comply with mandatory data breach notification requirements, notify impacted Data Subjects depending on the scope of the breach; gather information about the breach; assess the potential risk of harm to the Data Subjects; take steps to mitigate the harm to impacted Data Subjects; take steps to contain the breach and to prevent future similar breaches; and comply with data authority orders and court orders. Depending on the nature and scope of the breach, the organization is not required to notify the data authority.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions.

16. Accountability
In Mexico, organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. Subject to regulatory guidance,
organizations may be required to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Mexico, provided they are in compliance with local laws.

18. E-Discovery

When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved; and advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Opt-out consent is permissible.
Netherlands

Remke Scheepstra
Amsterdam
Tel: +31 20 5517 831
remke.scheepstra@bakermckenzie.com

Wouter Seinen
Amsterdam
Tel: +31 20 5517 161
wouter.seinen@bakermckenzie.com

Nathalja Doing
Amsterdam
Tel: +31 20 5517 128
nathalja.doing@bakermckenzie.com

Andre Walter
Amsterdam
Tel: +31 20 551 7941
andre.walter@bakermckenzie.com
1. Recent Privacy Developments

**GDPR Implementation**

On 9 December 2016, the Dutch government published a draft bill proposing a Dutch GDPR Implementation Act. The Implementation Act seeks to “implement” the GDPR as of 25 May 2018, that is to declare the GDPR applicable, replace the current Dutch Personal Data Protection Act, and fill in any room the GDPR leaves to Member States by way of opening clauses. The consultation round resulted in 67 responses, including a contribution by Baker McKenzie.

In April 2017, the Dutch Data Protection Authority advised on the draft bill. In short, the Dutch DPA advised:

- to strengthen the independent position of the Dutch DPA as a supervising authority, e.g., by making it possible for the Dutch DPA to conduct legal proceedings at the European courts in its own name;
- to exercise restraint in the Implementation Act as regards the interpretation of the standards laid down in the GDPR;
- to maintain a policy-neutral implementation of the opening clauses of the GDPR in national legislation.

No final legislative proposal has been published at the time of writing.

**Introducing a general data breach notification duty and increasing the maximum penalties**

Since 1 January 2016, a new “data breach notification” provision is in force under the Dutch Personal Data Protection Act ("Wet bescherming persoonsgegevens") (the “PDPA”). Under this provision, Data Controllers are generally obligated to report data security incidents to the Dutch Data Protection Authority (the “DPA”) in the event that such data breach (likely) has an adverse effect on the protection of the Personal Data at issue. Further, if the data breach is likely to adversely affect the privacy of the relevant Data Subjects, then these Data Subjects must be notified of the data breach as well.

At the same time the maximum amount of penalties for violations of the PDPA was increased to EUR 830,000, or 10% of the Data Controller’s annual turnover, for failure to comply with the rules of the PDPA. From 25 May 2018 under the GDPR the administrative fines for non-compliance will increase up to EUR 20 million, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The maximum penalty that can be imposed in case of a violation of the PDPA depends on the nature of the violation. The penalty for failure to notify a data protection operation with the
DPA was notably removed from the PDPA. The notification duty is still codified, but will no longer be enforced by the Dutch DPA.

**New act on cybersecurity data breach notification duties for providers of critical infrastructure**

In 2017, a new act passed the Senate introducing a specific data breach notification duty for businesses and governmental bodies that provide critical infrastructure. Under the act, these providers will be required to report data breaches and data security incidents to the National Cyber Security Centre, which is a special division of the Ministry of Security and Justice.

This notification duty is not limited to breaches of Personal Data, but will also apply to the loss of other data and security incidents such as malware, distributed denial-of-service (DDOS) attacks and “hacking" incidents.

The legislative proposal is still subject to debate in the House of Representatives. It is not clear yet how the legislative procedure will evolve.

**Various DPA investigations in the Internet and social media industry**

In 2017, the DPA investigated various Data Controllers in the Internet and the social media industry, whereby it specifically focused on profiling, the processing of Sensitive Personal Data, the processing of Personal Data by local government, the processing of Personal Data in the employment context and the security of the processing of Personal Data. Applications (apps), and the privacy terms of apps, social media services and Internet services were criticized by the DPA in public reports.

2. Emerging Privacy Issues and Trends

On 27 January 2017, the DPA published the main focus areas of its supervisory and enforcement efforts for 2017 which were: (i) the GDPR; (ii) profiling and transparency, (iii) special categories of Personal Data, (iv) and data security/data breaches.

- **GDPR:** Intensify its information provision on the GDPR requirements, educate Data Subjects on their rights and ensure that companies understand how to comply.

- **Profiling:** Focus on the transparency requirements related to profiling. The DPA considers it of importance that individuals are informed on the data that is being processed, and the purpose thereof.

- **Data security (in particular data breaches):** A data breach is considered “any failure of the technical and organizational measures to protect Personal Data”. The DPA will continue to investigate whether data breach notification obligations have been respected, and also focus on instances where data security is clearly an issue.
International cooperation

The DPA is vigorously pursuing international and cross-regulatory cooperation with other supervisors to enhance the effectiveness of investigating privacy violations. In 2017, the Dutch DPA announced that it will get together with the Dutch National Bank (DNB), the Authority for Financial Markets (AFM), and the Authority for Consumers and Markets to discuss their cooperation in fintech related matters.

3. Law Applicable

The applicable legislation is the Dutch Personal Data Protection Act (“Wet bescherming persoonsgegevens”) of 6 July 2000, implementing Directive 95/46/EC (the “Directive”)(the “PDPA”). This Act will eventually be replaced by the Dutch GDPR Implementation Act.

Further data protection provisions are included in the Telecommunications Act (“Telecommunicatiewet”) of 19 October 1998, among others, implementing the ePrivacy Directive (the “TA”).

In addition, the DPA has issued various guidelines and policy rules, which include:

- Policy on fines and penalties (2016);
- Active publication policy (2016);
- Policy on data breach notification (2016);
- Guidelines on data security (2013);
- Enforcement activity policy (2011); and
- Policy on DPA opinions on request (2009).

4. Key Privacy Concepts

Under the GDPR, the Key Privacy Concepts will to a large extent remain unchanged, as a result of which the below will apply (for the most part) under the GDPR as well.

a. Personal Data

The PDPA applies to the processing of “Personal Data”, which means any information relating to an identified or identifiable individual/natural person (“Data Subject”). Data regarding a legal entity of a person that is diseased does not fall under the scope of the definition of Personal Data. On the other hand, information relating to an individual in its capacity as representative of a legal entity or owner of a company, does qualify as Personal Data. Moreover the DPA holds the view that information that may be used to single out individuals, such as telephone numbers, license plate numbers and IP
addresses, should be treated as Personal Data. Finally data collected using cookies and similar techniques are considered Personal Data unless proven otherwise.

b. Data Processing
The concept of “Processing” is extremely broadly defined and covers any operation or set of operations performed on Personal Data including its collection, recording, organization, and even its deletion. The PDPA applies to automated data processing as well as to manual processing of Personal Data that is entered in a file or intended to be entered therein.

c. Processing by Data Controllers
The PDPA applies to those persons or entities that, alone or in conjunction with others, determine the purpose of and the means for the processing of Personal Data (“Data Controller”). The PDPA also imposes certain obligations on the Data Processor that processes Personal Data for the Data Controller. Under the PDPA, the carrying out of processing activities by a Data Processor must be governed by a (written) agreement (“Data Processing Agreement”), or another legal act whereby an engagement is created between the Data Processor and the Data Controller. In several instances, the DPA has issued guidance as to the requirements of a Data Processing Agreement; the level of detail required by the DPA.

d. Jurisdiction/Territoriality
The PDPA applies to:

- the processing of Personal Data carried out in the context of the activities of an establishment of a Data Controller in the Netherlands; or
- the processing of Personal Data by or for Data Controllers that are not established in the EEA, whereby use is made of automated or non-automated means situated in the Netherlands (unless these means are used only for forwarding/transporting Personal Data). Under the GDPR, this will change to Data Controllers that are not established in the EU, but that offer (free or paid) goods or services to, or monitor behavior of, Data Subjects in the EU. Note that where the GDPR refers to the “Union” (EU), this will likely include the other EEA countries as well, as it is expected these countries will adopt the GDPR as well.

e. Sensitive Personal Data
Specific restrictions apply to the processing of “special categories” of Personal Data. Such “Special Personal Data” largely corresponds to “Sensitive Personal Data”, but it is important to note that the two are not the same. Special Personal Data is defined as Personal Data relating to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, unlawful or objectionable conduct, criminal conduct, and data
concerning health or sexual life. The PDPA generally prohibits the processing of special Personal Data and subsequently provides for one generic and various specific exceptions.

Notwithstanding the specific exemptions for the processing of special Personal Data, in general, the prohibition to process special Personal Data does not apply where:

- the processing is carried out with the express consent of the Data Subject (see Section 5(b));
- the Personal Data has been made public by the Data Subject itself;
- the processing is necessary for the establishment, exercise, or defense of a right in law;
- the processing is necessary to comply with an obligation of international public law; or
- the processing is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy and this is provided for by law or else the DPA has granted an exemption. When granting an exception, the DPA can impose rules and restrictions. Processing Sensitive Personal Data on this basis must be notified to the European Commission.

Under the GDPR, some specific exceptions are added, including where processing is necessary in relation to employment and social security and social protection law, for reasons a substantial public interest, in relation to medicine, medical diagnosis and public health.

Further exemptions may apply to processing of Sensitive Personal Data that is carried out for the purpose of scientific research or statistics (if certain conditions are met).

The category-specific exceptions are set forth in detail in the PDPA. For example, political Personal Data may be processed by political parties; medical data may be processed by healthcare providers in the course of their treatment and data relating to union membership may be processed by the trade union concerned or the trade union federation to which this trade union belongs, provided that this is necessary to the aims of the trade union or trade union federation.

Moreover, a person’s personal identification number (“PIN”), which is created on the basis of specific legal requirements for the purpose of identifying a person (e.g., social security number), may only be used for the processing of Personal Data in execution of the said law or for purposes stipulated by the law. Even with the consent of the Data Subject, the processing of such PIN is prohibited.
f. **Employee Personal Data**

The PDPA does not provide for specific rules with respect to Employee Personal Data, however, Employee Personal Data may include both Sensitive Personal Data and non-Sensitive Personal Data.

Sensitive Employee Personal Data may be processed in the circumstances mentioned in Section 4(e), e.g., health-related Personal Data may be processed for the purpose of the reintegration of or support for employees.

Non-Sensitive Employee Personal Data may be processed by a Data Controller in certain circumstances, including the performance of the employment contract. Consent of the employee as a justification for processing of Sensitive and non-Sensitive Personal Data in the employment context will, in most cases, be considered invalid, since the DPA takes the position that employees cannot unambiguously – i.e., in freedom – give consent to the processing of the Personal Data, since an employee in most cases cannot withhold his/her consent without suffering the negative consequences thereof.

5. **Consent**

a. **General**

Obtaining consent of the Data Subject is not mandatory for the processing of Personal Data, but it is one of the six statutory processing grounds that can be relied upon.

While written consent is not required by law, if consent is relied upon it may be necessary in order to demonstrate that consent has been given at all (unambiguously and/or explicitly). The PDPA does not contain any specific requirements regarding the language of the consent. However, consent should be freely given, specific, and must constitute an informed expression of the Data Subject’s will, which implies that the Data Subject must be informed in a language that he/she is able to understand. Otherwise, the consent may be deemed invalid. Under the GDPR, the “consent demonstrability” requirements are even stronger.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data involved. When the Data Subject gives consent, it is understood to only cover the purpose(s) identified by the Data Controller when fulfilling its information requirements. “Fresh” consent is required for data processing activities for other purposes that have not been previously identified and consented to.

In addition, the Data Subject also has the right to withdraw consent at any time.
b. Sensitive Data
Where consent is relied upon to justify the processing of Sensitive (“special”) Personal Data, such consent must be given explicitly prior to the processing. Tacit or implicit consent does not suffice to meet this criterion. Explicit consent means that the Data Subject has manifested the expression of his or her will to give consent to the specific data processing verbally, in writing or by behavior.

c. Minors
For Data Subjects under the age of 16, or who have been placed under legal restraint or the care of a mentor, consent of their legal representative(s) must be obtained instead of the consent of the underage Data Subject.

d. Employee Consent
The general rule is that employee consent is not a legal justification to collect and process Employee’ Personal Data; the collection and processing of Employee Personal Data should, in principle, be justified on the ground that the processing is necessary, e.g., for the performance of an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. Online/Electronic Consent
In the Netherlands, online or electronic consent is permissible and deemed effective if properly structured and evidenced, as long as it meets the general requirements (as set out above).

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with sufficient information about:

- the organization’s identity;
- the types of Personal Data being collected;
- the purposes for collecting Personal Data;
- a description of the categories of Data Subjects and of the associated data or data categories;
- the recipients or categories of recipients to whom the Personal Data may be provided;
- the planned transfers of data to countries outside the European Union, if any; and
a general description allowing a preliminary assessment of the suitability of the (planned) organizational and technical measures to protect the Personal Data processed.

7. Processing Rules

An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and the legal obligations have been met. In other words, the organization must minimize its data processing activities.

The proportionality requirement applies to all data processing, regardless of the processing ground relied upon. In other words, even if Personal Data is collected in the basis of the Data Subject’s consent, the Data Controller is still obligated to verify that it does not process Personal Data in a manner that is unnecessary and thus excessive.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; (ii) request access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Data. Under the GDPR, additional Data Subject’s rights are introduced: (v) the right to data portability, (vi) the right to restriction of processing, and (vii) the right to object related to automated decision making.

9. Registration/Notification Requirements

An organization that collects and processes Personal Data used to be required to notify certain of its data processing activities with the Dutch DPA. Though this obligation was not removed from the Dutch Personal Data Protection Act, the obligation is no longer enforced by the Dutch DPA.

Under the GDPR the active notification requirement of Personal Data processing to the DPA will no longer exist. However, each controller and, where applicable, the controller’s representative, will have to maintain a record of processing activities under its responsibility. This obligations shall not apply to a small and medium size enterprise (SME) unless the processing they carry out is likely to result in a risk to the rights and freedoms of Data Subjects.
10. Data Protection Officers

In the Netherlands, there is no general requirement to appoint or designate a data privacy officer ("DPO") or other individual who will be accountable for the privacy practices of the organization.

Data Controllers that do appoint a registered DPO are exempt from the statutory duty to notify their processing operations and have these recorded in a publicly available register, though since this obligation is no longer enforced (see under Section 7 above), this is no longer a relevant motivation to appoint a DPO. Under the GDPR, certain private sector organisations and virtually all public sector organizations will be required to appoint a DPO.

11. International Data Transfers

Transfers of Personal Data from the Netherlands to countries within the EEA and certain "white listed countries" are generally permitted without the need for further approval, as these countries are generally considered to offer an adequate level of protection of Personal Data.

Cross-border transfers of Personal Data to a country that does not offer an adequate level of protection, may only take place if:

- the Data Subject has unambiguously consented to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or for actions to be carried out at the request of the Data Subject and that are necessary for the conclusion of a contract;
- the transfer is necessary for the conclusion or performance of a contract concluded between the Data Controller and third parties in the interests of the Data Subject;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the Data Subject;
- the transfer is carried out from a public register set up by law or from a register that can be consulted by anyone or by any persons who can invoke a legitimate interest; or
- an (unaltered) Model Contract within the meaning of Article 26 para. 4 of the Directive 95/46/EC is used.

If the above legal grounds for cross-border data transfer do not apply, the cross-border data transfer to a non-EEA country with an inadequate level of protection may be authorized by the Dutch Minister of Security and Justice.
Thus, the Data Controllers, on the basis of a data transfer agreement and after consultation with the DPA, must obtain a permit from the Dutch Minister of Security and Justice with regard to the data transfer. The DPA must be notified of and must approve any data transfer agreement in advance.

Data Transfers to the US may also be justified on the basis of the EU-US Privacy Shield arrangements, which is a framework for transatlantic data flows between the EU and the US that was agreed between them in February 2016 (as a follow up of the Safe Harbor arrangement, that was held invalid by the European Court of Justice in 2015).

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control is protected from unauthorized access and use. These requirements include that an organization must implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

In 2013, the DPA issued guidance on this topic which is still relevant to date. According to these guidelines, organizations should first conduct a Privacy Impact Assessment to determine the desired level of security. This is also included under the GDPR. Secondly, organizations are advised to adhere to “generally accepted security standards”, for example the NEN-ISO/IEC 27002:2007 standard (“Code voor Informatiebeveiliging”). The guidelines further state that organizations should conduct an evaluation of their systems on a regular basis. They also confirm the detailed requirements that – according to the DPA – apply to Data Processing Agreements.

The GDPR explicitly mentions pseudonymization and encryption as effective security measures.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual and other means to protect the Personal Data. There may be additional obligations to comply with requirements for specific sectors. In case of the occurrence of a data breach, the outsourcing organization may be held liable together with the third-party provider.

Unlike in most other European countries, Data Processors have unlimited liability for damages caused by their failure to comply with their data security obligations vis-à-vis Data Subjects.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, DPA investigations and audits, DPA orders, administrative fines, penalties or other sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

Under the GDPR the administrative fines for non-compliance will increase up to EUR 20 million, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered.

15. Data Security Breach

In addition to the general data breach obligation under the PDPA, a specific data breach notification obligation, implementing articles 4(3) and 4(4) of the ePrivacy Directive, is laid down in article 11.3a of the TA. Under this obligation, in case a data security breach takes place and such breach has detrimental effects for the protection of Personal Data, the TA imposes an obligation on providers of public electronic communication services to notify the Authority Consumers and Markets (“ACM”) as soon as possible. In addition, the provider must notify the relevant Data Subjects if their Personal Data is at risk. If the provider fails to notify the Data Subjects, the ACM may order the provider to do so.

An organization that is involved in a data breach situation may be subject to a suspension of business operations, closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, or civil actions and/or class actions, or a criminal prosecution.

The GDPR does not impose any substantial new data breach notification requirements compared to the current PDPA obligations.

16. Accountability

Subject to regulatory guidance, organizations may be required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

Under the accountability principle in the GDPR, controllers are required to implement appropriate technical and organizational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR.
For purpose of demonstrating, the GDPR encourages the establishment of data protection certification mechanisms, data protection seals and enforceable codes of conduct for the compliance with the GDPR. So far the Dutch DPA has communicated no actions in this respect.

17. Whistle-Blower hotline

Companies that employ at least 50 employees are legally required to implement a whistle-blower policy, which must comply with certain minimum requirements. A whistle-blower hotline may be established in the Netherlands, provided it is in compliance with local laws, and that appropriate filings have been made with the data authority. The prevailing opinion in the Netherlands is that hotline reports should primarily be dealt with at a local level, if possible. Only incidents that affect foreign parts of the group of companies may be reported to officers that are employed with affiliated parent companies in foreign countries.

18. E-Discovery

When implementing an e-discovery system, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

In 2012, the Netherlands implemented rules regarding cookies and similar techniques set out in Article 5 (e) of the ePrivacy Directive in article 11.7a of the TA.

Under this provision, anyone who wishes to store digital information, or gain access to digital information already stored, on the terminal equipment of a user (e.g., a computer, mobile device, etc.) – in other words: use cookies or similar techniques – may only do so after the user is provided with clear and complete information, and after the user has given his/her consent. The required consent must meet the requirements for consent set out in the PDPA. Implied consent is possible, but the website operator must be able to establish that the information was presented to the user and consent was sought prior to the cookie being deployed.

There are two exceptions to this rule. Prior information and consent are not required if, and to the extent that, the cookies are strictly necessary to: (i) carry out the transmission of communication over an electronic
communications network; (ii) provide a user with an information society service, which has been explicitly requested; or (iii) obtain information about the quality or effectiveness of a delivered service of the information society, provided that it has no or little impact on the privacy of the subscriber or user concerned (i.e., for analytical cookies with a low privacy impact and A/B testing).

The Minister of Justice and the relevant authorities (PDPA and ACM) have given extensive guidance on the consent and information requirements set out in article 11.7a of the TA. However, to date, the exact scope of the legal requirements and best practices have been subject to discussion, and the regulator’s views or activities have caused a stir from time to time. The ACM is aggressively enforcing the prior consent requirement, targeting many popular websites that are aimed at visitors to the Netherlands.

Tracking cookies are not exempted and by virtue of law, the data collected using tracking cookies is considered Personal Data, unless the website operator proves otherwise.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject's failure to respond. These anti-spam rules are laid down in the TA. The ACM is the enforcing regulator.
Espen Sandvik
Oslo
Tel: +47 98 29 45 41
esa@adeb.no

Emilie Veggeland Knudsen
Oslo
Tel: +47 99 15 47 74
evk@adeb.no
1. Recent Privacy Developments

*General Data Protection Regulation in Norway*

The General Data Protection Regulation (“GDPR”) will be applicable in the European Union from 25 May 2018. Due to the EEA Agreement, Norway will also implement the GDPR, but it has not yet been finally adopted by the EEA Committee, nor has a final implementation date been set for Norway. The government is, however, aiming at applying the framework from 25 May 2018.

In Norway, the GDPR will replace the current Personal Data Act and the subordinate Personal Data Regulation. The Norwegian Data Inspectorate is working closely with the Ministry of Justice and the Ministry of Local Government to ensure a smooth transition to the new framework.

In June 2017, the Ministry of Justice and the Ministry of Local Government published a hearing with a draft proposal to the new Personal Data Act – implementing the GDPR. The consultation paper is extensive, and governs the entire GDPR. Moreover, the consultation paper contains proposals for national regulation, where the GDPR allows for this. E.g., in accordance with article 88 of the GDPR, the consultation paper contains proposals for national regulation regarding access to employees’ emails and camera surveillance in the workplace.

There are still many unresolved matters, and the ministry has asked for input on several issues. The proposal was open for comments until 16 October 2017. Subsequent to the hearing, the proposal will be debated in Parliament.

2. Emerging Privacy Issues and Trends

*The Data Inspectorate focuses on surveillance at the workplace*

The Data Inspectorate published a report in January 2017 regarding surveillance at the workplace. The report contains assessments of the rules regarding surveillance at the workplace in the Working Environment Act and in the Personal Data Act. The report aims at guiding businesses on how to proceed when implementing surveillance measures at the workplace, and contains both practical checklists and examples of the use of different surveillance measures.

3. Law Applicable

The general regulation of Personal Data is found in the Personal Data Act 2000 (LOV-2000-04-14-31) as amended, and the subordinate Personal Data Regulation 2000 (FOR-2000-12-15-1265), which implements the Data Protection Directive (95/46/EC). Further provisions relevant to data privacy are found in the following Acts, among others:

The Marketing Act 2009 (LOV-2009-01-09-2), which restricts direct marketing.

The Health Register Act 2014 (LOV-2014-06-20-43), which governs the use of personal health data for research and quality assurance.


The Health Research Act 2008 (LOV-2008-06-20-44), which governs the use of Personal Data for health research purposes.

The Police Register Act 2010 (LOV-2010-05-28-16), which governs police processing of Personal Data.

As of May 2018, the GDPR is intended to become applicable in Norway. This has the consequence that the Personal Data Act 2000 and the subordinate Personal Data Regulation 2000 (FOR-2000-12-15-1265), which implements the Data Protection Directive (95/46/EC) will be replaced by a new Personal Data Act. The below does not reflect the rules coming in under GDPR.

4. Key Privacy Concepts

a. **Personal Data**

The Personal Data Act defines “Personal Data” as “any information and assessments that may be linked to a natural person”.

b. **Data Processing**

“Processing of Personal Data” is defined as “any use of Personal Data, such as collection, recording, alignment, storage and disclosure or a combination of such uses”. The Personal Data Act applies to (i) all processing of Personal Data wholly or partly by electronic means, (ii) the processing of Personal Data which forms part of or is intended to form part of a Personal Data register, and (iii) all forms of video surveillance.

c. **Processing by Data Controllers**

The Personal Data Act applies to those persons who determine the purpose of the processing of Personal Data and the means to be used (“Data Controller”).
**d. Jurisdiction/Territoriality**
The Personal Data Act applies to data processing activities carried out by:

- Data Controllers established in Norway; and
- Data Controllers that are not established in the EEA but that use equipment located in Norway to carry out data processing activities (other than merely for the purpose of transit).

**e. Sensitive Personal Data**
The Personal Data Act imposes additional requirements for the processing of Sensitive Personal Data – that is, Personal Data relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offense, or criminal proceedings. Specifically, the processing of Sensitive Personal Data is prohibited unless one of a number of stated conditions is met. These include:

- the Data Subject consents to the processing;
- there is statutory authority for the processing;
- the processing is necessary to protect the vital interests of a person, and the Data Subject is incapable of giving his or her consent;
- the processing relates exclusively to data which the Data Subject has voluntarily and manifestly made public;
- the processing is necessary for the establishment, exercise or defense of a legal claim;
- the processing is necessary to enable the controller to fulfill his/her obligations or exercise his/her rights in the field of employment law;
- the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where the data is processed by health professionals subject to the obligation of professional secrecy; or
- the processing is necessary for historical, statistical or scientific purposes, and the public interest in such processing being carried out clearly exceeds the disadvantages it might entail for the natural person.

Non-profit associations and foundations may process Sensitive Personal Data in the course of their activities even if such processing does not satisfy one of the conditions above. Such processing may apply solely to data relating to members or to persons who, on account of the purposes of the association or foundation, voluntarily have regular contact with it, and solely to data which is collected through such contact. The Personal Data may not be disclosed.
without the consent of the Data Subject. The Data Inspectorate may decide that Sensitive Personal Data may also be processed in other cases if this is warranted by important public interests and steps are taken to protect the interests of the Data Subject. Employee Personal Data

Employee Personal Data is likely to include both non-Sensitive Personal Data and Sensitive Personal Data (e.g., health-related information). Sensitive Employee Personal Data may be processed under the circumstances mentioned in Section 4(e) above, commonly for the purpose of carrying out the Data Controller’s obligations in the field of employment law. Non-Sensitive Employee Personal Data may be processed by a Data Controller for purposes that are necessary in order to maintain and administer the employment relationship (e.g., performance of a contract to which the Data Subject is a party, or carrying out the Data Controller’s legal obligations). Other justifications for processing non-Sensitive Employee Personal Data may include purposes that are of legitimate interest to the Data Controller and considered to be of greater weight than the Data Subject’s interest in his or her protection of personal integrity. A fallback justification for processing both Sensitive and non-Sensitive Personal Data in the employment context may be if consent is provided by the Data Subject. However, there are limitations on what is considered to constitute valid consent in the employment context (see Section 5(d) below).

5. Consent

a. General
Consent of the Data Subject will constitute a sufficient legal ground for the processing of Personal Data. The processing of Personal Data may also be allowed on other grounds and without consent, as further defined in the Personal Data Act. The consent must be voluntary, informed and explicit. Written consent is not required. Consent can be revoked at any time.

b. Sensitive Data
Consent of the Data Subject will constitute a sufficient legal basis for the processing of sensitive data, but such processing may, in some cases, be allowed on other grounds. The requirements to consent are in principle the same for the processing of sensitive data as for non-sensitive data, but the application of these principles will in practice be somewhat stricter.

c. Minors
The Personal Data Act does not specify a minimum age at which a child can provide valid consent. The Data Inspectorate has, however, together with the Consumer Ombudsman, provided guidelines under which Data Subjects can consent themselves from the age of 15. Children below 15 may only consent to the processing of their Personal Data in connection with minor competitions and similar arrangements, where the data is used for the purpose of
contacting prize winners. In case the consent relates to the processing of sensitive data, the Data Subject must be 18 in order to consent. For Data Subjects not having reached the required age, the parents can consent on their behalf. Children are, however, entitled to revoke a consent given by their parents. To the extent that minors are allowed to consent themselves, the requirement to the consent being “informed”, means that the information in question must be adapted so that it will be understood by the minor.

d. Employee Consent
In Norway, there are doubts as to when consent given in the context of an employment relationship can be considered valid. It will often be questionable whether consent qualifies as voluntary, given that the employee may feel forced to consent due to the subordinate nature of their relationship with their employer. It is, however, assumed that employee consent in some cases can be seen as voluntary and valid, as the Personal Data Regulation § 7-16 expressly give effect to consent from employees.

e. Online/Electronic Consent
Online or electronic consent is permissible and deemed effective if properly structured and evidenced.

6. Notice Requirements
An organization that collects Personal Data directly from the Data Subject must provide the Data Subject with information on: the name and address of the Data Controller and its representative (if any); the purposes for which the data is intended to be processed; whether or not the data will be transferred to a third party, and if so to whom; that it is voluntary for the Data Subject to provide the data; and other information as required for the Data Subject to be able to enforce his/her rights in the best possible manner, including the statutory right to access and rectify data.

Where data is obtained from a third party, the Data Controller will have to provide the Data Subject with the same information as referred to in the paragraph above, unless the collection of data in question has an express legal basis, notification is impossible or disproportionately difficult, or it is clear that the Data Subject is already aware of the information and could potentially have been notified.

7. Processing Rules
An organization that processes Personal Data must: limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete or anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.
8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; and request the deletion and/or destruction of the Data Subject’s Personal Data.

9. Registration/Notification Requirements

All electronic processing of Personal Data is, as a starting point, subject to notification to the Data Inspectorate. A notification is required for each category of data processing, meaning that one Data Controller may have to submit several notifications. The notifications must be filed no later than 30 days before the processing begins, and must be renewed every three years. Standard online filing forms can be used, and the information required is limited. The processing of sensitive data is subject to an authorization from the Data Inspectorate. A number of exceptions are found from these notification obligations and authorization requirements. For instance, certain categories of data, such as employee data and customer data, are exempted, provided certain conditions are met.

10. Data Protection Officers

In Norway, there is no requirement to appoint or designate a data protection officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Transfers of Personal Data from Norway to EEA Member States are generally permitted without the need for further approval. Transfers are also permitted to Canada, Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Andorra, Israel, Switzerland, New Zealand and Uruguay, which are the subject of the European Commission’s findings of adequacy (subject to the fulfillment of certain pre-conditions) in relation to their data protection laws. Transfer to the US is permitted where the recipient is certified under the US Privacy Shield arrangement.

Subject to the specific authorizations mentioned above, Personal Data may not be transferred to countries outside the EEA. Exceptions to this general prohibition are, however, expressly contemplated under the DP Act, including where:

- the Data Subject has consented to the transfer;
• the transfer is necessary to perform a contract with the Data Subject, or to take steps at his or her request with a view to entering into a contract with him/her;

• the transfer is necessary for the conclusion or performance of a contract entered into between the Data Controller and third parties in the interests of, or at the request of, the Data Subject;

• the transfer is necessary to protect the vital interests of the individual, or for reasons of public interest, or in connection with legal proceedings, or for the purpose of obtaining legal advice or establishing, exercising or defending legal rights; or

• the transfer has been specifically authorized by the Data Inspectorate.

The adoption of model contractual clauses approved by the European Commission will also provide an adequate level of protection to justify the transfer. Note that the Data Controller must, in any event, justify all of its data processing under the Personal Data Act; justification of any transfers is an additional compliance requirement. The transfer contract must be filed with the Data Inspectorate before the transfer takes place.

Where multinational organizations are transferring personal information outside the EEA, but within their group of companies, they may also adopt binding corporate rules (“BCRs”) as a means of justifying such intra-group transfers. Acceptable BCRs may include intra-group agreements, policies or procedures, and special arrangements among the group of companies that afford the requisite protection. The Data Inspectorate, along with the other DPAs across the EEA, has agreed to mutually recognize BCRs approved by one of these DPAs. For BCRs to enable the transfer of personal information freely within a corporate group, they must be approved by at least one DPA that has agreed to mutually recognize BCR applications, and by any remaining DPAs in EEA countries from which the organization transfers Personal Data and which have not agreed to mutual recognition of BCR applications. The Article 29 Working Party has adopted a model checklist and a table setting out the required contents of an application to a DPA for approval of a proposed BCR.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in their possession and control is protected from unauthorized access and use. Appropriate physical, technical and organizational security safeguards to protect Personal Data must be implemented, and the organization must be able to document such safeguards. The level of security must be in line with the amount, nature, and sensitivity of the Personal Data involved.
13. Special Rules for Outsourcing of Data Processing to Third Parties

A transfer of Personal Data must, as a general rule, be necessary for the purpose of the processing. Organizational, cost efficiency and security reasons are normally viewed as acceptable reasons for a transfer of Personal Data due to outsourcing. Although the Personal Data processing is outsourced, the controller remains responsible for the processing activities. Consequently, the controller must make sure that the provisions under the data processing agreement and other related regulations are complied with, both by the controller and the third-party service provider. The third-party service provider and its sub-processors (if any) are viewed as Data Processors. It is a statutory requirement that a written contract is entered into with the Data Processor (see Section 7 above). Moreover, should Personal Data be transferred to a country located outside of the EEA, the controller must make sure that any of the exceptions to the general prohibition on transferring Personal Data to a third country applies or that another acceptable measure for the transfer has been taken (see Section 11 above). The controller may be obliged to provide the Data Subjects with information about the transfer of their Personal Data.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Requirements to the handling of data security breaches are found in the Personal Data Regulation § 2-6. The requirements only apply to certain types of Personal Data of particular importance, namely such Personal Data for which it is necessary to “protect the confidentiality, availability and integrity” in order to “prevent the danger of loss of life and health, financial loss or loss of esteem and personal integrity”, and which are processed entirely or partly by “automatic means” cf. § 2-1. In case of a breach related to such data, measures must be taken to “re-establish the normal state of affairs, eliminate the cause of the discrepancy and prevent its recurrence”. Further, the Data Inspectorate must be notified if the breach “has resulted in the unauthorized disclosure of Personal Data where confidentiality is necessary”. Finally, the results of handling of the security breach incident shall be documented. The Personal Data Act does not expressly require that the Data Subjects be notified of the breach, but doing so may still be required for other reasons, in particular if necessary in order to assist the Data Subject to avoid a loss.
16. Accountability

Organizations implementing new information systems and/or technologies for the processing of Personal Data must first consider if the general conditions for such data processing are met. This means, among others, defining the purpose of the processing, considering if there is a legal basis to justify it, and integrating it in its security and internal control systems for Personal Data. This also means assessing the risks associated with the processing of Personal Data. Documentation of these assessments and systems must be made available upon request from the Data Inspectorate.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Norway, provided that general data privacy law requirements are observed. There is an obligation to establish whistle-blower hotlines for businesses that regularly employ five or more employees.

18. E-Discovery

An employer’s right to access employee emails or other electronic information held by employees (even if work-related and stored on the employer’s equipment) is subject to various restrictions. Firstly, the accessing must be justified by certain legitimate reasons as further defined, and secondly, certain procedures must be followed, which normally involve notifying the employee in advance and allowing the employee to be present. The rights of the employees are mandatory, and cannot be waived in advance.

19. Anti-Spam Filtering

Generally, the introduction of a spam filtering solution in an organization does not raise privacy issues. However, the individual control of such a spam filtering system will raise privacy issues (see Section 18 above).

20. Cookies

The Electronic Communication Act restricts the deployment of cookies. The consent of the user must be obtained before cookies can be used, with certain limited exceptions related partly to transfers of communication in electronic communication networks, and partly to information society services requested by the user. In practice, consent in the form of browser settings has been accepted. The use of cookies must in any case comply with general data privacy law requirements.
21. Direct Marketing
The Marketing Act restricts the use of direct marketing. Individual electronic communications for marketing purposes (such as email and SMS) to physical persons (whether in a business or consumer capacity) require either the prior consent of the recipient, or alternatively an already existing customer relationship with the recipient. Phone calls and non-electronic letters for marketing purposes cannot be sent to individuals listed in the Reservation Register.
Paraguay

Nestor Loizaga
Asuncion
Tel: +595 21 318 3000 ext. 2533
nloizaga@ferrere.com
1. Recent Privacy Developments
There have been no major privacy developments in Paraguay.

The Paraguayan Constitution protects the right to privacy; it ensures the right to information and regulates the constitutional right known as habeas data as an instrument for data protection. Habeas data guarantees individuals the right to access information or data about themselves on official or private public record. It gives individuals the right to know how the information is being used and for what purpose, and allows for the updating, rectification or destruction of incorrect and illegal information.

The first data protection legislation in Paraguay was enacted in 2001. Data protection and personal information are regulated and governed by Law No. 1682/01, as amended by Law No. 1969/02 and Law No. 5543/15 (the “Law”). The Law regulates the collection, storage, distribution, publication, modification, destruction, duration and general treatment of Personal Data contained in files, registries and databases, as well as in general any other technical means of treating public or private data destined to provide reports, in order to ensure the protection of privacy in individuals.

The major challenge imposed by the Law is that it does not provide for a specific data protection authority. Consequently, when faced with infringements, individuals or legal entities are required to file individual complaints before ordinary civil courts. Although the Law aims at protecting Personal Data and information, the underlining issue is that this legal framework primarily addresses the protection of financial and credit information.

2. Emerging Privacy Issues and Trends
There have been no noteworthy emerging privacy issues in Paraguay.

3. Law Applicable
The legal framework for Data Protection in Paraguay comprises the following:

- Paraguayan Constitution (articles 4, 33, 34, 36 and 135).
- Law No. 1682/01, which regulates private information.
- Law No. 1969/02, which amends and replaces several articles of Law No. 1682/01.
- Law No. 5543/15, which amends and replaces articles 5 and 9 of Law No. 1969/02.
- Law No. 1160/97 “Paraguayan Criminal Code” and its amendments under Laws No. 2212/03, 3440/08, 4439/11, 4614/12, 4770/12, 5016/14, 5378/14, and 5655/16.
4. Key Privacy Concepts

a. **Personal Data**
The Law doesn’t provide a specific definition to “Personal Data”, however it is generally understood as any information pertaining to an identified or identifiable person.

b. **Data Processing**
The Law does not contain a specific definition for “Data Processing”.

c. **Processing by Data Controllers**
The Law does not contain a specific definition for “Data Controllers”. Furthermore, no distinction is made between entities that hold or control personal information and data and those that process it on behalf of other entities.

The Paraguayan National Constitution (article 26) and the Private Information Law (articles 2 and 3) generally allow the collection and processing of personal information for private use. The Private Information Law regulates the following actions on Personal Data:

- collection, storage and distribution;
- publication, modification and destruction;
- the treatment of Personal Data contained in files, records and databases;
- any other technical means for dealing with public or private data aimed at submitting reports; and
- the use of information for scientific/statistical purposes, for surveys and polls of the public opinion, or for market studies.

d. **Jurisdiction/Territoriality**
The Law applies to any physical person or legal entity having a legal domicile or local offices or branches only in Paraguay.

However, the Law does contain exemptions as it does not apply to databases or sources of journalistic information. It is also unenforceable against the freedom of expression and freedom to report or inform.

e. **Sensitive Personal Data**
The Law defines “sensitive data” as that which makes reference to racial or ethnicity preferences, political preferences, individual health state, religious, philosophical or moral beliefs, sexual intimacy and information that would generally generate prejudices or discrimination, or affect the dignity, domestic intimacy, or private image of persons or families.
f. **Employee Personal Data**
The Law does not contain a specific definition for “Employee Personal Data”.

5. **Consent**

a. **General**
The Law does not require consent for the collection, storage and processing of data for personal and private purposes, nor is consent required to access information and data contained in public registries.

It is legal to collect, store, process and publish Personal Data for scientific and statistical purposes, for polls and public surveys as well as market research, provided that the publications do not individualize the person or legal entity investigated.

The only mandatory requirement for written consent refers to the publication of financial and credit information. The Law establishes that data or information that describes, reveals or estimates a patrimonial situation, economic solvency or compliance of commercial and financial obligations, may only be published when individuals or legal entities have provided express written authorization for the collection of financial information concerning obligations that have not been claimed in a court of law.

b. **Sensitive Data**
The Law prohibits the publication and disclosure of sensitive data with regard to individuals who are explicitly individualized or identifiable.

However, the Law does authorize the publication of data solely consisting of the following: name and surname, identity card, address, age, date and place of birth, marital status, occupation or profession, work place and number.

In addition, the collection, storage, processing, and publication of data or personal characteristics for scientific, statistical, survey investigations, or market study purposes are allowed as long as the targeted persons and entities are not identified in the final publication.

c. **Minors**
Pursuant to the Childhood and Adolescence Code Law No. 1680/2001, there are two specific restrictions targeting the collection or processing of information of minors: (i) public servants and authorities involved in legal cases and administrative affairs that investigate and rule on minors; and (ii) the press or any source of news whatsoever reporting on criminal events with minors involved, either as victim or alleged perpetrator, where names, photographs or any other data could identify the minor.
d. Employee Consent
There are no provisions that specifically address consent requirements for employees.

e. Online/Electronic Consent
There are no provisions that specifically address online or electronic consent, its admissibility and effectiveness. Nonetheless, the validity of electronic and digital signatures is recognized under Paraguayan Law No. 4017/10 and its amendment Law No. 4610/12.

6. Information/Notice Requirements
On account of constitutional provisions and the rights set forth by the Law, entities that collect Personal Data must provide access to the data, as well as information regarding its use and the purpose for which the data was collected.

Data Subjects are entitled to know the use and the purpose for which the data and information was collected and to request the correction of Personal Data that is erroneous, inaccurate, misleading or incomplete. In addition, Data Controllers must provide, free of charge: (i) the update, modification, or elimination of Personal Data; and (ii) an authentic copy of the record altered in the pertinent part.

7. Processing Rules
There is no specific legislation on this matter or rules addressing this issue.

8. Rights of Individuals
The Law establishes that all individuals have the right to collect, store and process Personal Data exclusively for private use.

Every person has the right to access and to know the purpose and use of information and data related to them, to their relatives, to the persons under their guardianship, and to their assets, stored in official or private registries of public nature, or stored in entities that provide information regarding their economic situation.

Data Subjects are entitled to know the use and the purpose for which the data and information was collected and to request the correction of Personal Data that is erroneous, inaccurate, misleading or incomplete.

Data Controllers must provide, free of charge:

- the update, modification, or elimination of Personal Data; and
- an authentic copy of the record altered in the pertinent part.
In addition, Data Controllers that supply information about Data Subjects’ patrimonial situation, economic solvency, or compliance of commercial and financial obligations, must stop the transmission of information in compliance with the following time periods:

- three years after an overdue obligation has not been claimed in court;
- immediately after the debt is canceled; and
- five years after a composition with creditors has been admitted in court.

Moreover, Data Controllers must implement an automatic informatics mechanism that deletes non-publishable data, in conformity with the above time periods.

9. Registration/Notification Requirements
There are no registration or notification requirements in Paraguay.

10. Data Protection Officers
Since no data protection authority was created under the Law, there is no requirement to appoint or designate data privacy officers who would be accountable for privacy practices.

Individuals are required to file individual complaints before ordinary civil courts in the case of a data breach in which, for example, Sensitive Personal Data is published.

11. International Data Transfers
There are no specific rules in Paraguay regarding international transfers of Personal Data. The Law does not establish any imposed restrictions on the cross-border transfer of personal information, nor the export of Personal Data to other jurisdictions.

Data Controllers transferring Personal Data abroad must comply with the Private Information Law’s general requirements.

12. Security Requirements
In general terms and except for certain regulated areas such as banking or tax, there are no specific legal requirements regarding security measures for the protection of Personal Data.

In terms of banking for example, for financial transactions exceeding USD 10,000:

- banks and financial entities must notify the Paraguayan Central Bank of the customer’s identity; and
• the Paraguayan Tax Law requires Data Controllers to inform the Treasury Ministry of the amount of the transaction.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

There is no specific legislation on this matter or rules addressing this issue. However, third parties processing data on behalf of a Data Controller must comply with the general requirements of the Private Information Law, including obtaining a Data Subject’s consent for processing sensitive data that explicitly individualizes or identifies a Data Subject.

14. Enforcement and Sanctions

As previously mentioned, no data protection authority was created under the Law.

The Law only contemplates monetary penalties in the event of non-compliance or infringements by individuals or legal entities which publish, distribute, supply or disclose information that describes, reveals or estimates a patrimonial situation, economic solvency or compliance of commercial and financial obligations regarding individuals or legal entities.

These penalties are also enforceable on individuals or legal entities which are obliged to rectify or provide the necessary information in order to rectify the aforementioned financial and economic solvency information and fail to do so within the legal term.

The fine shall be established according to the circumstances of each particular case and the amount varies from 50 to 200 daily minimum wages (approximately USD 711 to USD 2,844) for diverse unspecified labor activities and can be doubled, tripled and so on in the event of recidivism.

Additionally, the affected party could file civil and criminal complaints before ordinary courts.

The Paraguayan Criminal Code provides for the following penalties related to the treatment of Personal Data:

• Fines or imprisonment of up to two years for: (i) infringing the right to communicate and image; (ii) violating the confidentiality or secrecy of communication; or (iii) intercepting and transferring data without authorization

• Fines or imprisonment of up to three years for violating security systems and accessing data without authorization.

• The disclosure of private secrets is punishable with imprisonment of up to one year or fines. If the disclosure was made by a person obligated to
maintain its secrecy due to their profession, the imprisonment shall be up to three years or a fine. The disclosure of private secrets for economic purposes increases imprisonment to up to five years.

15. Data Security Breach
No specific legislation regulates the requirement of notice in the event that the security of Personal Data is compromised or breached. There is no national regulator of Personal Data in Paraguay.

16. Accountability
There are no specific rules addressing this issue.

17. Whistle-Blower Hotline
There is no specific legislation on this matter or rules addressing this issue.

18. E-Discovery
There is no specific legislation on this matter or rules addressing this issue.

19. Anti-Spam Filtering
There is no specific legislation on this matter or rules addressing this issue.

However Article 23 of the Electronic Commerce Law No. 4868/2013 regulates non-requested commercial communications sent via email.

It determines that providers of goods and services can only send such communication when they comply with the following requirements:

- expressly indicate in the email the commercial and unsolicited nature of the communication;
- include an easy way to exclude the email address of the recipient from their recipients’ email distribution list;
- the recipients data was not obtained through the infringement of his privacy rights; and
- the communication does not exceed the size set forth by the Ministry of Industry and Commerce.

20. Cookies
There is no specific legislation regarding the use of cookies, but best practice dictates using cookies only with the Data Subject’s agreement or consent.
21. Direct Marketing

There is no specific legislation on this matter or rules addressing this issue. However, Article 22 of the Electronic Commerce Law No. 4868/2013 grants protection to users’ privacy by stipulating that providers of goods and services through electronic means shall offer users or consumers the possibility to oppose the use of their data for promotional purposes by means of a simple and free procedure, at the time the data is collected and in every commercial communication sent to the user or consumer. For this purpose, there is also a national registry provided by Consumer Defense to which individuals can request their phone number to be added if they do not want to receive unsolicited marketing (Law No. 5830/2017 “Banning unauthorized publicity to users of mobile phones”).
Peru

Javier Tovar
Lima
Tel: +51 1 618 8500 Ext. 8550
javier.tovar@bakermckenzie.com

Teresa Tovar
Lima
Tel: +51 1 618 8500 Ext. 8552
teresa.tovar@bakermckenzie.com

Viviana Chavez
Lima
Tel: +51 1 618 8500 Ext. 8535
viviana.chavez@bakermckenzie.com

Eileen Infantas
Lima
Tel: +51 1 618 8500 Ext. 8536
eileen.infantas@bakermckenzie.com
1. Recent Privacy Developments

On 7 January 2017, Legislative Decree No. 1353 ("LD 1353"), which modifies the Personal Data Protection Law (the "PDPL"), was enacted. Among the main modifications introduced by the LD 1353 to the PDPL are:

a. Consent for the processing of Personal Data is no longer required in the following cases (among others):
   - When the processing of information is required to prepare and execute a contractual relationship with the Data Subject.
   - When the processing of information is necessary to prevent money laundering and the financing of terrorism.
   - When economic groups comprising companies obliged to report (as determined by the prevention of money laundering regulations) wish to share information of their clients among themselves.
   - When the processing is conducted by exercising the fundamental right to freedom of information.

b. Hiring a new Processor after the consent of Data Subjects has been obtained: When a Data Controller hires a new Processor after obtaining the consent of the Data Subjects, there is no need to obtain fresh consent. It will be sufficient to notify the Data Subjects of such new relationship.

c. Transfer of information due to a merger or similar operations: If after having obtained the consent of the Data Subjects a transfer of information – because of a merger or similar operations – takes place, the new Data Controller must notify the transfer to the Data Subjects.

2. Emerging Privacy Issues and Trends

The Data Protection Authority ("DPA") has the capacity to issue opinions regarding the interpretation of the PDPL – as requested by any individual or entity. Below are some of the latest opinions published by the DPA:

- **Video surveillance in work centers** – The DPA has stated that although video surveillance is a tool used for security (and not to access personal information), considering that the image of the Data Subjects qualifies as Personal Data under the PDPL, the consent of the Data Subjects must be obtained to conduct video surveillance activities. For that purpose, the publication of a privacy notice (containing the minimum information provided by the PDPL to obtain informed consent) would be enough.

- **Processing of information under FATCA** – The DPA was consulted on how compliance with the US Foreign Account Tax Compliance Act ("FATCA"), which provides that foreign financial entities must adopt
certain measures to identify and report clients that could be potential taxpayers of the US Treasury, should be interpreted in the context of the PDPL.

The DPA has stated that if the Peruvian government has not signed an agreement with the United States for the application of FATCA in Peru, the processing of personal information based on FATCA requires the prior and express consent of Data Subjects.

3. Law Applicable

The Peruvian Political Constitution recognizes the right to privacy as a fundamental right and provides for the writ of habeas data, a mechanism to protect such right – through a judicial process – in the case of any act or omission that violates or threatens the expectation of privacy.

Nevertheless, the Peruvian data protection legal framework – Law No. 29733 and its Regulation approved by Supreme Decree No. 003-2013-JUS – seeks to guarantee the fundamental right of privacy while recognizing specific rights of Data Subjects and obligations of those who are responsible for the processing of such data.

4. Scope of the Law

a. Personal Data

“Personal Data” is defined as any information regarding a natural person (“Data Subject”) that identifies him/her or makes him/her identifiable through means that can be reasonably used.

b. Data Processing

“Data Processing” is defined as any operation or technical proceeding, automated or not, that facilitates the collection, storage, organization, modification, usage, suppression, transfer – among other actions – that allows the access, correlation or interconnection of Personal Data.

c. Processing by Data Controllers

The PDPL applies to holders of a database (“Data Controllers”), who are the natural persons, private legal persons or public entities that process Personal Data within a database and that must adopt the security measures to guard the Personal Data.

d. Jurisdiction/Territoriality

The PDPL applies to Personal Data contained or intended to be included in private or public databases whose processing is performed within the Peruvian territory. It is not applicable to Personal Data contained or intended

---

1 Modified by Legislative Decree No. 1353, as detailed in Section 1.
to be included in databases created by natural persons for private or family use, nor is it applicable to Personal Data contained or intended to be included in databases of public entities for the strict fulfillment of their responsibilities in the areas of national defense, public security and criminal investigation and repression.

e. Sensitive Personal Data
According to the PDPL, “Sensitive Data” includes biometric data, data related to racial and ethnic origin; income; opinions or convictions regarding politics, religion, philosophy or morality; union membership; and information related to health or sexual life. The Regulations have stated that “Sensitive Data” also consists of information related to the emotional characteristics of a person; the facts and circumstances of his/her personal and familiar life; his/her personal habits; and information that corresponds to his/her most intimate sphere.

f. Employee Personal Data
There are no specific requirements on this regard, therefore, it is understood that the general provisions contained in the PDPL are applicable.

5. Consent

a. General
The processing of Personal Data requires prior, informed, express and unequivocal consent. Consent can never be implied.

The PDPL also states that consent is not required in specific cases, including:

- when Personal Data relates to a person’s health:
  - if necessary in a situation of risk, prevention, diagnosis or medical or surgical treatment of the owner of the information, provided such processing is carried out by a medical institution or by health professionals, complying with professional secrecy obligations;
  - for public health reasons; or
  - for undertaking epidemiologic or equivalent studies;

- when the Personal Data is public information;

- when Personal Data relates to the financial solvency or creditworthiness of a person;

- when necessary for preparing, reaching and executing a contractual relationship;

- when necessary to prevent money laundering and financing of terrorism;
• when the processing is conducted by exercising the fundamental right to freedom of information; and

• other exceptions to be established in regulations of the PDPL and those established in other laws.

b. Sensitive Data
When referring to Sensitive Data, the prior, informed, express and unequivocal consent of the Data Subject must be granted in writing.

c. Minors
Consent can be obtained from minors, provided they are 15 or above, the information given to them at the time of collection is expressed in a comprehensive manner, and the products or services offered are not restricted to their age. Regarding minors below 15 years, the consent must be obtained from their legal representatives.

d. Employee Consent
There are no specific requirements in this regard, therefore, it is understood that the general provisions contained in the PDPL are applicable.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in Peru if properly structured and evidenced.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about the organization's identity; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; where the Personal Data is to be transferred; where the Personal Data is to be stored; how to exercise the rights recognized by the legal framework; and the term for which the information will be stored.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize the Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject; access the Data
Subject’s Personal Data, subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; impede its transference to third parties and exercise the writ of habeas data.

In exercising the right to access Personal Data (when it comes to databases of public administration), the Data Subject may have to shoulder the costs for producing the same (e.g., costs for photocopying the documents).

9. Registration/Notification Requirements
The PDPL creates the National Registry for the Protection of Personal Data (“Registry”), which is open to the public. The Registry is in charge of the National Authority for the Protection of Personal Data, for the purposes of registering:

- private or public databases and information about Data Subjects that would be necessary for the exercise of their rights;
- authorizations issued under the Regulations;
- sanctions, and precautionary and corrective measures imposed by the National Authority for the Protection of Personal Data;
- codes of conduct of the entities that manage private databases; and
- communications regarding cross-border transfers of data.

10. Data Protection Officers
Organizations may be required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers
International transfer of Personal Data requires consent from the owner of the information and can be made only if the recipient country has adequate levels of protection, similar to those under the PDPL.

If the recipient country does not have an adequate level of protection, the data transmitter must guarantee that the processing of the Personal Data will comply with the PDPL. This is not applicable if:

- the transmission of Personal Data is conducted within the framework of an international judicial cooperation or the application of international trades in this regard;
- international cooperation is required between intelligence agencies;
- the Personal Data is necessary to execute a contractual relationship with the Data Subject;
• referring to banking and security transfers;
• the transfer is made for the purposes of protecting, preventing, diagnosing and providing medical treatment to the Data Subject;
• the Data Subject has granted his/her consent for the transfer of data under these conditions; and
• the Personal Data is necessary for the development of a scientific or professional relationship with the Data Subject.

In the case of cross-border transfers of Personal Data, organizations are required to notify the DPA.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control is protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved. A Security Directive, approved by the DPA through Directorial Resolution No. 019-2013-JUS/DGPDP, contains the security measures that should be implemented considering the characteristics of the data banks involved (including the amount and nature of the information they contain). Although this Directive is not mandatory, following its guidelines guarantees compliance with the obligation to implement adequate security measures.

13. Special Rules for Outsourcing of Data Processing to Third Parties

If a Data Controller outsources the processing of Personal Data to a third party (a “Processor”), such party must also comply with the PDPL (keeping the confidentiality of the information processed; using the Personal Data only for the purposes authorized; modifying inaccurate information, among others). After the execution of the outsourcing agreement, the Personal Data processed must be removed, unless the Data Subject provides express consent to do otherwise.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, DPA investigations/audits, DPA orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

There are no specific rules addressing data security breaches. However, as Data Controllers are generally liable for any data security breach, it is highly
advisable to inform the affected Data Subjects as soon as the Data Controller becomes aware of a data security breach.

In addition, the Security Directive (as mentioned in Section 12) provides that, to comply with the general duty of security, any data breach should be notified to the Data Subjects as soon as it is confirmed. Such notification must include: (i) the nature of the incident; (ii) the Personal Data involved in the data breach; (iii) recommendations to the Data Subject; and (iv) corrective measures implemented.

Thus, it is highly recommended that organizations that are involved in a data breach take steps to mitigate the harm to impacted Data Subjects; take steps to contain the breach; take steps to prevent future similar breaches; assist authorities with any investigation relating to the breach; and comply with DPA orders and court orders.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
There are no specific legal references in this regard. Nevertheless, if the data obtained as a consequence of the implementation of a whistle-blower hotline is collected by the Data Controller for creating a database, such database should be registered before the National Authority for the Protection of Personal Data.

18. E-Discovery
There is no law/rule that regulates e-discovery in Peru.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to opt out from the spam-filtering solution.

20. Cookies
There are no specific laws/rules in Peru that regulate the use and deployment of cookies. In general, the use and deployment of cookies must comply with
data privacy laws. The consent of Data Subjects must be obtained before cookies can be used.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. The consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent.
Philippines

Bienvenido Marquez
Manila
Tel: +63 2 819 4936
bienvenido.marquez@quisumbingtorres.com

Divina Ilas-Panganiban
Manila
Tel: +63 2 819 4961
divina.ilaspanganiban@quisumbingtorres.com

Neonette Pascual
Manila
Tel: +63 2 819 4908
neonette.pascual@quisumbingtorres.com
1. Recent Privacy Developments

a. **National Privacy Commission issues Rules and Regulations implementing the Data Privacy Act**


In addition to the more general requirements of the Data Protection Act on the processing of personal information, the Rules impose several registration and compliance obligations on covered controllers and processors. The most important of these obligations are:

- **Registration of Personal Data Processing Systems.** Personal Data processing systems operating in the Philippines that involve the processing of sensitive personal information belonging to at least 1,000 individuals shall be registered with the NPC. Controllers or processors that employ less than 250 persons are generally exempt from the registration requirement, subject to certain conditions;

- **Reportorial Requirements.** Personal information controllers are required to notify the NPC and affected Data Subjects of a data breach within 72 hours from the discovery thereof. In addition, covered entities shall also report to the NPC with a summary of documented security incidents and data breaches on an annual basis, and also notify the Commission when automated processing becomes the sole basis of making decisions about a Data Subject;

- **Nature of Consent of Data Subjects.** The Rules clarify that in cases not exempt from the consent requirement, the Data Subject’s consent to the personal information processing is time-bound in relation to the purpose of the processing. Data sharing, even between entities belonging to the same corporate organization, should also have the prior consent of the affected Data Subjects; and

- **Minimum Security Requirements; Contents of Data Transfer Agreements between Controllers and Processors.** The Rules enumerate the specific minimum organizational, physical, and technical requirements which controllers and processors are required to implement while processing personal information. These security standards are subject to periodic evaluation and updating by the NPC via subsequent issuances. The Rules also contain the minimum requirements as to the compliance provisions to be included in any data processing agreement between personal information controllers and its processors.
Subsequent to issuing the Rules, the NPC also released several circulars and advisories which cover the requirements and guidelines on the following matters: (a) public sector’s compliance with the DPA, (b) Personal Data breach management and notification, (c) the NPC’s rules on practice and procedure, (d) appointment of data protection officers and compliance officers for privacy, (e) registration of data processing systems with the NPC, and (f) conduct of privacy impact assessments.

b. Creation of the Department of Information and Communications Technology

Republic Act No. 10844 or the Department of Information and Communications Technology Act of 2015 (“DICT Act”) was signed into law on 23 May 2016. It created the Department of Information and Communications Technology (“DICT”), which is mandated to be the primary policy, planning, coordinating, implementing and administrative agency of the Executive Branch of the Philippine Government, and is tasked to plan, develop, and promote the national Information and Communications Technology (“ICT”) development agenda.

The new law also renames the existing Department of Transportation and Communications (DOCT) to Department of Transportation, and abolishes all of its agencies and units dealing with communications such as the National Computer Center (NCC), National Telecommunications Training Institute (NTTI), Information and Communications Technology Office (ICTO), Telecommunications Office (TELOF), and the National Computer Institute (NCI). The powers, functions, appropriations, personnel, and property of these agencies are transferred to the DICT. Existing agencies pertaining to ICT are also attached to the DICT for policy and program coordination, such as the National Telecommunications Commission (NTC), NPC, and Cybercrime Investigation and Coordination Center (CICC).

c. Implementing Rules and Regulations of the Cybercrime Act

The implementing rules and regulations of the Cybercrime Prevention Act of 2012 (Republic Act. No. 10175) were issued by the Department of Justice, Department of Science and Technology, and Department of Interior and Local Government. The rules do not cover the law’s provisions criminalizing online libel and unsolicited commercial communications or “spam”, and those which allow a warrantless takedown of internet material, which were declared as unconstitutional and therefore void by the Supreme Court in 2014.¹

2. Emerging Privacy Issues and Trends

The organization of the NPC resulted in the early stage of enforcement of the DPA, as may be seen from the commission’s investigation of and decision in

¹ Disini v. The Secretary of Justice, G.R. No. 203335, 11 February 2014.
the Commission of Elections (COMELEC) data breach which occurred in 2016, and the compliance checks on a number of financial institutions which appear to have been involved in data breaches.

The NPC is also consistent in its efforts to educate the public on data privacy as shown by the commission’s conduct of seminars and roadshows, including a bi-monthly forum for data protection officers.

The NPC’s apparent commitment to its mandate as the Philippine data privacy authority will definitely show a continuing and perhaps even an upward trend towards data privacy awareness and enforcement in the country.

3. Law Applicable

Republic Act No. 10173 or the Data Privacy Act of 2012 is the main legislation governing data privacy in the Philippines. Its implementing rules and regulations took effect on 9 September 2016.

Prior to the Act, there was no law dealing specifically with data privacy. While the Philippine Constitution and jurisprudence recognize and protect a person’s right to privacy, it deals with the protection of personal information in a general manner.

There are also provisions scattered across several statutes, such as the Civil Code, the Revised Penal Code, the Anti-Wire Tapping Law and the Electronic Commerce Act, dealing with an individual’s right of privacy. However, these provisions do not squarely address the issue of data privacy and so were inadequate and, in some instances, inapplicable in addressing the issue of Personal Data privacy. There is also no government agency overseeing the protection of Personal Data.

4. Key Privacy Concepts

a. Personal Data

The Act defines “Personal Information” as any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

b. Data Processing

The Act defines “Processing” as any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
c. **Processing by Data Controllers**

Under the Act, a personal Data Controller may transfer personal information to a third party for processing. However, the personal Data Controller remains responsible for such data and remains accountable for compliance with the Act. The Act’s implementing rules and regulations contain the minimum provisions, such as specific obligations of the Data Processor, which should be included in data processing or sharing agreements.

d. **Jurisdiction/Territoriality**

The Act applies to an act done or practice engaged by an entity in and outside of the Philippines if:

a. the act, practice or processing relates to personal information about a Philippine citizen or a resident;

b. the entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

1. a contract is entered in the Philippines;
2. a juridical entity unincorporated in the Philippines but with central management and control in the country; and
3. an entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

c. the entity has other links in the Philippines, for example if:

1. the entity carries on business in the Philippines; and/or
2. the personal information was collected or held by an entity in the Philippines.

However, personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, are not covered by the provisions of the Act even if the personal information is being processed in the Philippines. The Act’s implementing rules and regulations, however, state that Data Controllers and Processors which process personal information originally collected from residents of foreign jurisdictions must implement security measures under the Act.
e. Sensitive Personal Data

Under the Act, “sensitive personal information” refers to personal information:

1. about an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

2. about an individual’s health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

3. issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or cm-rent health records, licenses or their denials, suspension or revocation, and tax returns; and

4. specifically established by an executive order or an act of Congress to be kept classified.

f. Employee Personal Data

Under the Act, there is no substantial difference between the rules applicable to employee data and any other kind of Personal Data.

Employees are not entitled to be notified when the following information entered, collected and processed in the processing system of the employer are for obvious purposes:

1. a description of the personal information to be entered into the system;

2. the purposes for which they are being or are to be processed;

3. the scope and method of the personal information processing;

4. the recipients or classes of recipients to whom they are or may be disclosed;

5. the methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized;

6. the identity and contact details of the personal information controller or its representative;

7. the period for which the information will be stored; and

8. the existence of their rights, i.e., to access and correction, as well as the right to lodge a complaint before the NPC.
5. Consent Requirements

a. General
The Data Privacy Act differentiates “personal information” from “sensitive personal information” and provides for different treatment. The processing of personal information is permitted, if not otherwise prohibited by law and when at least one of the conditions stated in the law exists. On the other hand, the processing of sensitive personal information is prohibited, except in specific instances enumerated under the law. For both types of information, however, consent of the Data Subject is the common underlying requirement for processing to be considered lawful. To be valid, “consent” must be freely-given, specific and informed. The purpose for which the collection of information is done must be specific, legitimate and made known to the Data Subject before, or as soon as reasonably practicable after, collection and information must be later processed in a way compatible with such declared, specified and legitimate purpose. For sensitive personal information in particular, the consent must be specific to the purpose and obtained prior to the processing of such information.

b. Sensitive Data
See Section 4(e).

c. Minors
A minor cannot consent to the collection of his or her personal information. Consent must be obtained from the parents or legal guardian.

d. Employee Consent
There is no provision that specifically addresses consent requirements for employees. However, the general rule on collection of personal information about individuals applies.

e. Online/Electronic Consent
Electronic consent is allowed. Under the Act, consent shall be evidenced by written, electronic or recorded means.

6. Information/Notice Requirements
The Data Subject is entitled to:

a. be informed whether personal information pertaining to him or her shall be, is being or has been processed; and

b. be furnished with the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
1. a description of the personal information to be entered into the system;
2. the purposes for which they are being or are to be processed;
3. the scope and method of the personal information processing;
4. the recipients or classes of recipients to whom they are or may be disclosed;
5. methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized;
6. the identity and contact details of the personal information controller or its representative;
7. the period for which the information will be stored; and
8. the existence of their rights, i.e., to access and correction, as well as the right to lodge a complaint before the NPC.

Any information supplied or declaration made to the Data Subject on these matters shall not be amended without prior notification to the Data Subject. However, the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service, or when necessary or desirable in the context of an employer-employee relationship, between the collector and the Data Subject, or when the information is being collected and processed as a result of a legal obligation.

7. Processing Rules
Processing of personal information must adhere to the principles of transparency, legitimate purpose, and proportionality. The specific processing rules are detailed in the implementing rules and regulations of the Act.

8. Rights of Individuals
A Data Subject is entitled to reasonable access to, upon demand, the following:
1. contents of his or her personal information that was processed;
2. sources from which personal information was obtained;
3. names and addresses of recipients of the personal information;
4. manner by which such data were processed;
5. reasons for the disclosure of the personal information to recipients;
6. information on automated processes where the data will or is likely to be made the sole basis for any decision significantly affecting or that will affect the Data Subject;

7. date when his or her personal information concerning the Data Subject was last accessed and modified; and

8. the designation, or name or identity and address of the personal information controller.

In addition to the foregoing access rights, generally, a Data Subject is entitled to:

a. be informed if personal information pertaining to him or her shall be, is being or has been processed;

b. subject to certain exceptions, be furnished with the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
   1. the description of the personal information to be entered into the system;
   2. the purposes for which they are being or are to be processed;
   3. the scope and method of the personal information processing;
   4. the recipients or classes of recipients to whom they are or may be disclosed;
   5. the methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized;
   6. the identity and contact details of the personal information controller or its representative;
   7. the period for which the information will be stored; and
   8. the existence of their rights, i.e., to access and correction, as well as the right to lodge a complaint before the Commission. Any information supplied or declaration made to the Data Subject on these matters shall not be amended without prior notification to the Data Subject;

c. dispute an inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by
recipients thereof, provided that the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the Data Subject;

d. suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller’s filing system upon discovery and substantial proof that the personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or is no longer necessary for the purposes for which it was collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information;

e. be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information; and

f. where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of the data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the Data Subject.

9. Registration/Notification Requirements

Personal Data processing systems operating in the Philippines that involve the processing of sensitive personal information belonging to at least 1,000 individuals shall be registered with the NPC. Controllers or processors that employ less than 250 persons are generally exempt from the registration requirement, subject to certain conditions. Existing controllers and processors were given until 9 September 2017 to register with the NPC the appointment of their respective Data Protection Officers. Data processing systems covered by the registration requirement should be registered with the NPC on or before 8 March 2018.

Personal Data Controllers and Processors shall report to the NPC with a summary of documented security incidents and data breaches on an annual basis, and also notify the Commission when automated processing becomes the sole basis of making decisions about a Data Subject.

The personal information controller shall promptly notify the NPC and affected Data Subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected Data Subject. The notification shall be made within 72 hours of
discovery of the data breach and shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system, except that there should be no delay if the breach involves at least 100 Data Subjects, or the disclosure of sensitive personal information will harm or adversely affect the Data Subject.

1. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with Section 20 of the Act (Security of Personal Information) and existence of good faith in the acquisition of personal information.

2. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected Data Subjects.

3. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

10. Data Protection Officers

There is no requirement under the Act for appointment of a data protection officer. The Act, however, requires a personal information controller to designate an individual or individuals who are accountable for the organization’s compliance with the Act. The identity of the individual(s) designated shall be made known to any Data Subject upon request.

The Act’s Rules, however, specifically require the appointment of a data protection officer. The NPC allows the appointment of a common data protection officer for a group of related companies, provided that a compliance officer for privacy who will be supervised by the data protection officer is also appointed for each member of the group.

11. International Data Transfers

The Data Privacy Act does not appear to specifically require that personal information collected from Philippine citizens or residents should be stored or processed in the Philippines. It also does not appear that the Act prohibits the off-shore storage or the transfer of such personal information to foreign jurisdictions. The Act, however, considers the “personal information controller” to continue to be responsible for personal information that may have been “transferred to a third party for processing, whether domestically or internationally”.

Baker McKenzie | 543
There is an old law, Presidential Decree 1718, that prohibits the transfer of documents or information relating in any manner to any business carried on in the Philippines, unless such taking, sending or removal is:

- consistent with and forms part of a regular practice of furnishing to a head office or parent company or organization outside of the Philippines;
- in connection with a proposed business transaction requiring the furnishing of the document or information;
- required or necessary for negotiations or conclusions of business transactions, or is in compliance with an international agreement to which the Philippines is a party; or
- made pursuant to the authority granted by the designated representative(s) of the President.

The Office of the President has yet to issue rules and regulations implementing the law since its passage on 21 August 1980. Hence, the law is not strictly enforced.

12. Security Requirements

The Act requires that:

a. the personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

b. the personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

c. the determination of the appropriate level of security must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines the Commission may issue from time to time, the measures implemented must include:

1. safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of its functioning or availability;

2. a security policy with respect to the processing of personal information;
3. a process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

4. regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach;

d. the personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision; and

e. the employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information is not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

Under the Act, a personal information controller may subcontract the processing of personal information. However, the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally comply with the requirements of the Act and other laws for processing of personal information. The personal information controller remains responsible for the personal information, even information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. The Act further makes the personal information controller accountable for complying with the requirements of this Act and requires him/her to use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.

14. Enforcement and Sanctions

Potential civil, administrative, or criminal sanctions may be imposed for specific violations of the Act (e.g., unauthorized processing, accessing due to negligence, improper disposal, processing for unauthorized purposes, unauthorized access or intentional breach, concealment of security breaches, malicious disclosure, and unauthorized disclosure of personal information and sensitive personal information).
The NPC is also vested with quasi-judicial powers to adjudicate privacy complaints and award civil damages to private complainants. It is also vested with regulatory powers to impose on erring covered entities compliance and enforcement orders, cease and desist orders, bans on personal information processing, or payments of administrative fines.

15. Data Security Breach

The personal information controller shall, within 72 hours of the discovery of a data breach, notify the NPC and affected Data Subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected Data Subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system, except that there should be no delay if the breach involves at least 100 Data Subjects, or the disclosure of sensitive personal information will harm or adversely affect the Data Subject.

1. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with Section 20 of the Act (Security of Personal Information) and existence of good faith in the acquisition of personal information.

2. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected Data Subjects.

3. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

16. Accountability

There is no law in the Philippines that requires an organization to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

There are no laws/rules that govern whistle-blower hotlines in the Philippines.
18. E-Discovery System

The Data Processor is required to obtain the consent of the members or employees prior to the implementation of an e-discovery system which monitors and stores electronic information.

19. Anti-Spam Filtering

A spam-filtering solution may arguably be considered a violation of the right to privacy of communications of the persons within the organization. To eliminate or minimize the risk of privacy violation issues, the consent of the individuals/employees should be obtained.

20. Cookies

There are no laws/rules that govern the use and deployment of cookies in the Philippines.

21. Direct Marketing

There are no laws/rules that regulate direct marketing in the Philippines.
Poland

Magdalena Kogut-Czarkowska
Warsaw
Tel: +48 22 445 3452
magdalena.kogut-czarkowska@bakermckenzie.com

Radoslaw Nozykowski
Warsaw
Tel: +48 22 445 3210
radoslaw.nozykowski@bakermckenzie.com

Jakub Falkowski
Warsaw
Tel: +48 22 445 3294
jakub.falkowski@bakermckenzie.com
1. Recent Privacy Developments

**New legislation to align Polish privacy laws with the GDPR requirements**

Poland is currently in the process of amending its privacy laws in order to align them with the GDPR requirements. On 14 September 2017, the Ministry of Digitization published a *draft of the new Personal Data Protection Act* ("PDPA") for public consultations. The main provisions of the draft include:

1. introducing a new data protection authority – the President of the Office for Personal Data Protection ("PUODO") will replace the Inspector General for Personal Data Protection;
2. defining the powers and tasks of the PUODO;
3. new rules of civil liability for data protection infringement;
4. new criminal sanctions for obstructing investigations carried out by the PUODO;
5. introducing certification and accreditation mechanisms;
6. derogations for GDPR applicability in relation to press, literary and artistic activities, as well as processing for purposes of “academic expression”;
7. new rules of appointing and notifying data protection officers (DPOs).

Additionally, the draft PDPA provides that minors over 13 years of age may consent to data processing without additional consent from their parents or legal guardians. This change is important for international online service providers.

Together with the PDPA, the Ministry of Digitization proposed an *Act on Introducing the PDPA*, which contains a number of derogations from the GDPR to be introduced in specific legal acts. According to the proposal, among other things the derogations will apply in the context of data processed:

1. for the purposes of national security, e.g., in relation to soldiers’ and military data;
2. by public schools, libraries, museums and some other educational and cultural institutions and facilities;
3. by legal professionals;
4. in public archives and various public registries;
5. by collective management societies;
6. for the purposes of public statistical information authorities;
7. by various types of public and government authorities, such as tax authorities;
8. by hotels (limited exceptions apply);
9. by banks and insurance sector companies (limited exceptions and special permissions apply);
10. by the courts, judicial authorities and registries (e.g., National Criminal Registry);
11. by the National Health Fund in the context of the public healthcare system.

The proposal also includes important changes to the Labor Code, in particular regarding the processing of employees’ data (for more detailed information see point 2 “Emerging Privacy Issues and Trends”).

2. Emerging Privacy Issues and Trends

**New rules on processing employees’ data**

Polish legislators are currently working on legal acts aimed at aligning Polish privacy laws with the requirements set forth in the GDPR. One of these draft acts introduces important changes to the rules of processing employees’ Personal Data (the Act on Introducing the Personal Data Protection Act).

Generally, the draft bill outlines three categories of employee data: (i) data that may be processed without the employee’s consent, (ii) data that may be processed only with the employee’s consent and (iii) categories of information that may not be processed, even with the employee’s consent. The proposal includes additional conditions for obtaining the valid consent of employees.

The proposed approach is important since under the existing provisions of the Labor Code there were serious doubts as to whether an employee may effectively give its consent for the employer to process types of data other than those expressly listed in the Labor Code (basic data such as name, surname, date of birth, education etc.). Processing of any other data, such as biometric data (fingerprints) used in access control systems, was highly disputable among privacy law experts and forbidden in the opinion of the Polish data privacy authority.

Under the proposed amendment to the Labor Code, employers will be expressly allowed to process other data on employees, provided that these data relate to the work relationship and that the employee has expressed his/her consent to the processing. Additionally, the amendment will also regulate CCTV monitoring for work purposes.
3. Law Applicable

The processing of Personal Data in Poland is regulated by the Law on the Protection of Personal Data ("PPD") of 29 August 1997 (as amended), and the Ordinance of the Minister of Internal Affairs and Administration of 29 April 2004, specifying the required documentation for processing Personal Data and the technical and organizational requirements which should be fulfilled by equipment and computer systems used for processing Personal Data. Furthermore, the Minister of Administration is working on an ordinance specifying the tasks of Data Protection Officers, which should enter into force later this year. In general, the PPD implements the provisions of the EU Data Protection Directive (95/46/EC).

The PPD applies to the processing of Personal Data in files, indices, books, lists and other registers, as well as those contained in computer systems (even if they do not constitute a data filing system).

With regard to the collection of Personal Data which is compiled on a short-term basis exclusively for technical or training purposes or in connection with teaching purposes in schools of higher education, and which, upon being used is immediately removed or treated so as to make them anonymous, only limited provisions of the PPD apply, in particular those related to security requirements.

Apart from the PPD, several other statutes provide specific provisions regarding Personal Data protection, e.g., the Act on Providing Services through Electronic Means. In addition, Article 173 of the Telecommunication Law refers to the use of cookies.

Links:

Effective from 25 May 2018, the PPD will be replaced by new legal acts whose aim is to align Polish regulations with GDPR requirements. For more details please refer to Section 1 – “Recent privacy developments”.

4. Key Privacy Concepts

a. Personal Data

The PPD applies to the processing of any information ("Personal Data") relating to an identified or identifiable natural person ("Data Subject").

Under the GDPR the concept of “Personal Data” remains substantially unchanged. The GDPR introduces also the concept of pseudonymization of data, which may be helpful for organizations in satisfying their obligations of “privacy by design” and “privacy by default".
b. **Data Processing**

“Processing” is broadly defined to include the collection, recording, storage, organizing, changing, disclosure, and deletion of Personal Data. The PPD regulates both automated and manual data processing.

Under the GDPR the concept of “processing” remains substantially unchanged. Minor amendments made do the definition’s wording are unlikely to cause any practical difference.

c. **Processing by Data Controllers**

The PPD applies to those natural persons, legal entities or organizational units who determine the purposes for which and the manner in which any Personal Data is, or is to be, processed (“Data Controllers”). Certain provisions of the PPD apply also to persons to which the Data Controllers entrust the processing of Personal Data (“Data Processors”).

Under the GDPR both the distinction between Data Controllers and Data Processors has been preserved. GDPR will however provide more detailed regulation for Data Processors.

d. **Jurisdiction/Territoriality**

The PPD applies in particular to data processing activities carried out by:

- Data Controllers that have their registered seat or place of residence in Poland; and
- Data Controllers that have their registered seat or place of residence in a third country, i.e., a country outside the EEA, but use technical means based in Poland to carry out data processing activities (other than merely for the purpose of transit).

The definition of the territorial scope of the applicability of the PPD may give rise to concerns in the light of the “Weltimmo” case (C-230/14) decided by the Court of Justice of the European Union. The PPD itself does not provide for its applicability to the entities established in other EU member states and pursuing commercial activities in the territory of Poland, which may be incompatible with the EU law.

The territorial applicability of the GDPR provisions has been extended when compared to the current rules under Directive 95/46/EC. In particular, organizations established outside the European Union that do not use any “means of processing” in the EU, but offer good or services to EU residents, may be subject to the compliance obligations imposed by the GDPR.

e. **Sensitive Personal Data**

The PPD imposes additional requirements for the processing of Sensitive Personal Data – that is, information revealing racial or ethnic origin, political
opinions, philosophical or religious beliefs, religion, party or trade union membership, health, genetic code, sexual life, convictions, penal judgments, fines, and other decisions issued in court or administrative proceedings. Specifically, the processing of Sensitive Personal Data is prohibited, unless certain conditions are met, including:

- the Data Controller obtains the written consent of the Data Subject (see Section 5(b) below), unless the processing consists of the deletion of Personal Data;
- the provisions of other specific statutes provide for the processing of such Personal Data without the need to request the Data Subject’s consent and provide adequate safeguards;
- processing is necessary to protect the vital interests of the Data Subject or of other persons where the Data Subject is physically or legally incapable of giving his consent until a guardian or a curator is appointed;
- processing is necessary for the purpose of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non-profit-seeking organizations or institutions with a political, scientific, religious, philosophical, or trade union aim and on the condition that the processing relates solely to the members of those organizations or institutions, or to persons who have regular contact with them in connection with their activities, and subject to providing suitable protection of the processed Personal Data;
- processing relates to Personal Data necessary for the establishment of legal claims;
- processing is necessary for the purpose of carrying out the obligations of the Data Controller with regard to employment of its employees and other persons, and the scope of processing is provided for by the law;
- processing is required for the purpose of preventative medicine, the provision of care or treatment, where the Personal Data is processed by a health professional involved in treatment, other health care services, or the management of health care services and subject to providing suitable protection for the Personal Data;
- processing relates to Personal Data that is manifestly made public by the Data Subject;
- processing is necessary to conduct scientific research, including preparation of a thesis required for graduating with or receiving a university degree; any results of scientific research cannot be published in a way which allows Data Subjects to be identified; or
• processing is conducted by a party in court or administrative proceedings in order to exercise rights and duties resulting from decisions issued in those proceedings.

Generally, the catalogue of Sensitive Personal Data included in the GDPR remains significantly unchanged, except for genetic and biometric data which have been expressly categorized as special categories of Personal Data. Also, there are specific provisions relating to processing data relating to criminal convictions and offenses.

f. **Employee Personal Data**

Employee Personal Data is likely to include non-Sensitive and Sensitive Personal Data (e.g., trade union membership information). Sensitive Employee Personal Data may be processed in the circumstances identified in Section 4(e) above. Under the Polish Labor Code, an employer has the right to demand from employees and the candidates for employment the following non-Sensitive Personal Data:

• given name(s) and surname;
• parents’ given names;
• date of birth;
• address (and mailing address);
• details of education; and
• details of employment history.

Once the candidate is employed, the employer has the right to demand Personal Data other than the types of Personal Data listed above, including:

• names, surnames, and dates of birth of employees’ children, provided that such data is required for the employee to benefit from special rights as provided for in the labor law;
• the PESEL number of each employee; and
• Personal Data other than that provided for above, if the obligation to provide such data arises under other provisions of law (i.e., other than the Polish Labor Code).

Currently Polish government is working on material amendments to the laws governing the rules of processing employees’ data. Based on the most up-to-date version of the proposed legislation, they will be significantly liberalized when compared to the current regulations.
5. Consent

a. General
Under Polish Law, consent of the Data Subject is not mandatory, but it is contemplated as a justification for the processing of Personal Data (i.e., may constitute a basis for the processing in case another statutory basis does not apply). In practice, it is often one of the more straightforward ways to justify processing. Consent must be express and cannot be presumed or implied from any other consents or declarations. Consent must be voluntary, informed and unambiguous. Written consent is not required. The language of consent must not be too abstract – that is, consent must not refer to processing of Personal Data in general. Consent must refer to a particular situation and particular categories of Personal Data and should clarify the methods and the purposes of such processing. Consent may be unlimited in time or provide for a certain timeframe. Data Subjects may withdraw their consent for data processing at any time.

The GDPR will retain the concept of consent as a processing condition, and the requirements for consent will largely remain unchanged, although certain new conditions will apply. Overall, the GDPR sets a higher standard for Data Subject’s consent to be valid.

b. Sensitive Data
The PPD imposes additional requirements for the processing of Sensitive Personal Data, which includes information relating to racial or ethnic origin, political opinions, philosophical or religious beliefs, religion, party or trade union membership, health, genetic code, sexual life, convictions, penal judgments, fines, and other decisions issued in court or administrative proceedings. Sensitive Personal Data may, however, still be processed without obtaining the written consent of the Data Subject in certain prescribed circumstances.

The most important novelty under the GDPR in respect of rules of processing of sensitive data is that express consent of Data Subjects is no longer required to be in writing. According to the GDPR provisions the Data Subject’s explicit consent may be given in any form, e.g., including electronic.

c. Minors
As a rule, a person under the age of 18 cannot give valid consent for data processing. A parent or legal guardian must give consent on such minor’s behalf.

Those rules will be amended by GDPR, which provides a number of specific provisions regarding children’s data, including minor’s consent in the context of offering of “information society services”.
d. Employee Consent
Under Polish Law, consent is not required from an employee for the processing of Personal Data because processing of Employee Personal Data for employment purposes is derived from legal provisions. The rulings of the Supreme Administrative Court, however, provide that an employer cannot seek employee consent for the processing of Personal Data outside the statutory scope.

Currently Polish government is working on material amendments to the laws governing the rules of processing employees’ data. Based on the most up-to-date version of the proposed legislation, they will be significantly liberalized when compared to the current regulations. For instance, the revised rules of employees’ data processing will allow employers to process certain “additional” categories of employees’ data upon their freely given consent.

e. Online/Electronic Consent
Polish law does not prescribe any particular form in which consent should be given (exceptions apply to Sensitive Data, which in general requires written consent). However, bearing in mind the general principle that consent must not be implied, and also that it is the Data Controller who has to prove that it processes Personal Data in a lawful manner, electronic consent may not be sufficient.

The rules described above will remain substantially unchanged also under the GDPR, except for liberalized requirements for obtaining consent for processing Sensitive Personal Data. Pursuant to the rules set forth in the GDPR, a requirement for mandatory hand written consent for processing Sensitive Personal Data will no longer apply.

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity, the purposes for collecting Personal Data, third parties to which the organization will disclose the Personal Data, and the rights of the Data Subject.

Under the GDPR, the contents of privacy notices have been substantially extended.

7. Processing Rules
An organization that processes Personal Data must: (i) limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; (ii) anonymize the data whenever possible; and (iii) delete/anonymize personal information once the stated purposes have been fulfilled and legal obligations met.
GDPR introduces new general processing principles, such as transparency and accountability principles, and makes the existing ones more detailed and sometimes restrictive. Furthermore, general rules such as “privacy by design” and “privacy by default” will materially change current approach of Data Controllers to business operations involving Personal Data processing.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; and (iv) request the deletion and/or destruction of the Data Subject’s Personal Data.

Data Subjects’ rights listed above will be retained under the GDPR, however, they will also be accompanied by brand new ones, such as data portability right, right to be forgotten or a right to restrict processing.

9. Registration/Notification Requirements

Generally, the PPD imposes on a Data Controller a general obligation to register a Personal Data database with the GIODO; however, some exceptions apply. In particular, such exceptions apply if the Personal Data (other than Sensitive Data) is not processed with the use of computer systems or if the Data Controller appointed a Data Protection Officer and notified him/her to GIODO.

The Data Controller may commence processing of a database upon submitting the database to the GIODO for registration. However, the Data Controller may start the processing of Sensitive Data in the database only after registration of the database.

Under the GDPR the registration obligation currently existing in the Polish law will be abolished.

10. Data Protection Officers

a. General and conditions

In Poland, organizations may appoint a Data Protection Officer ("DPO"). The appointment is voluntary. The DPO must fulfill the following conditions:

- have full legal capacity and full public rights;
- have no criminal record for intentional crimes; and
- have sufficient knowledge of Personal Data protection.

The appointment and the recalling of the DPO should be notified to GIODO.
According to the rules set forth in the GDPR, there will be an obligation to appoint a DPO in the following circumstances: (i) the processing is carried out by a public authority or body; (ii) the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of Data Subjects on a large scale; or (iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and Personal Data relating to criminal convictions and offenses.

b. Tasks
The tasks of the DPO include:

- ensuring compliance with the provisions on processing Personal Data in the organization;
- preparing periodic and ad hoc (special) reports for the Data Controller;
- supervising the preparation and update of documentation on Personal Data processing and compliance with the rules provided in this documentation;
- ensuring that the persons authorized to process Personal Data are familiar with the data protection laws; and
- keeping a publicly available register of the databases held by the Data Controller.

Under the GDPR, the tasks of the DPO will be prescribed in a more detailed manner, however in substance the role of DPO in the organization will be similar to their current function.

c. Legal Position
The DPO must answer directly to the “head of organizational unit” or the natural person who acts as the Data Controller. The Data Controller must create the conditions and “separation within its organization” necessary for the independent exercise of tasks by the DPO.

According to the GDPR provisions, the position of the DPO within its organization will be strengthened in comparison to the current regulations. Especially, it has been explicitly said that the organization cannot instruct the DPO in performance of his or her duties, and cannot be dismissed or otherwise penalized for performing the DPO’s duties.

11. International Data Transfers
a. General
International data transfers to a country that does not provide in its territory an adequate level of data protection may take place subject to the prior consent
of the GIODO, issued by way of an administrative decision, provided that the Data Controller ensures adequate safeguards with respect to the protection of the privacy, rights and freedoms of the Data Subject.

GIODO does not recognize US law generally as providing a level of protection equivalent to that of Poland, however, Privacy Shield will be recognized.

In principle, the GDPR will retain the cross-border data transfer rules of the Directive 95/46/EC.

b. Exceptions
There are certain exceptions to the general rule against transfer of Personal Data to territories with inadequate data protection laws, the most relevant being where:

- the transfer is required by other laws or by the provisions of any ratified international agreement, which guarantee an adequate level of Personal Data protection;
- the Data Subject has given his written consent;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or takes place in response to the Data Subject’s request;
- the transfer is necessary for the performance of a contract concluded in the interests of the Data Subject between the Data Controller and a third party;
- the transfer relates to Personal Data that has been made public;
- the transfer is necessary on public interest grounds or for the establishment, exercise, or defense of legal claims; or
- the transfer is necessary to protect the vital interests of the Data Subject.

The derogations listed above remain in principle unchanged also under the GDPR. The only noteworthy change is that according to the new rules the Data Subject’s consent must no longer be granted in writing.

c. Data transfer agreements
Data transfer agreements can render a Personal Data transfer legitimate. The GIODO’s approval is not required if the Data Controller ensures adequate safeguards for the protection of privacy and the rights and freedoms of the Data Subject by applying binding corporate rules approved by the GIODO or standard contractual clauses approved by the European Commission.

With respect to Polish law, the GDPR do not introduce any material changes in this field.
12. Security Requirements

Organizations are required to take steps to: (i) ensure that Personal Data in their possession and control are protected from unauthorized access and use; (ii) implement appropriate physical, technical and organization security safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

Similarly to the current legislation, the GDPR leaves a significant amount of discretion to the controller, in terms of the technical and organizational measures to be implemented to guarantee data security. What is new, the GDPR explicitly provides that adherence to the approved codes of conduct may serve as evidence of compliance with the safety requirements.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. They are also required to comply with sector-specific requirements. Furthermore, organizations that outsource the processing of data shall be held liable together with the third-party provider in case of breach by the latter.

Disclosing the Personal Data between public entities does not require them to enter into outsourcing agreements, as long as processing activities serve the same public purpose. In such case, the public entities shall be considered one and the same Data Controller. The above solution is doubtful in practice and has been criticized among data protection specialists.

Under the GDPR, the concept of a “processor” does not change. However, whereas the Directive 95/46/EC generally imposes direct compliance obligations solely on controllers, the GDPR treats controllers and processors equally, and both controllers and processors will face direct compliance obligations as well as serious penalties if they do not comply with them. Moreover, the obligatory contents of outsourcing agreements have been determined directly in the GDPR.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, civil actions, criminal proceedings and/or private rights of action.

Under the GDPR the data protection authorities have been armed with new complex powers of both investigative and corrective character. Non-compliance with GDPR requirements may result in imposing severe sanctions by data protection authorities, including financial fines amounting up to 4% of...
a yearly global turnover of the company or EUR 20 millions, whichever will be higher. Private enforcement instruments have been strengthened and unified as well.

15. Data Security Breach

In general, there is no legal obligation under the PPD to provide notice of a data security breach. Exception applies to the providers of publicly available telecommunication services, which must inform GIODO about security breaches no later than within three days. The Data Protection Officer usually keeps records of data security breaches, which identify and describe the breach and the measures taken to address the breach (e.g., remedies implemented to prevent future breaches). In case of an audit, such records should be produced to the GIODO. Furthermore, organizations that are involved in data breach situations are required to: (i) gather information about the breach; (ii) assess the potential risk of harm to Data Subjects; (iii) take steps to mitigate the harm to impacted Data Subjects; (iv) take steps to contain the breach and to prevent future similar breaches; and (v) assist authorities with any investigation relating to the breach.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database, civil actions, and/or criminal prosecution.

The GDPR will bring material change by introducing broad data breach notification requirements which will require organisations to report data breaches to the relevant supervisory authority, and frequently also the individuals affected. Moreover, Data Controllers will be legally obliged to keep records and properly document all events of data security breaches.

16. Accountability

The “accountability principle” is understood as a requirement to have sufficiently detailed documentation of data processing activities in place, which includes Personal Data security policy and the instruction for managing IT systems, as well as the register of data processing authorizations.

Under the accountability principle as codified in the GDPR, controllers will be required to implement appropriate technical and organizational measures to ensure compliance and be able to demonstrate that data processing is performed in accordance with the GDPR.

17. Whistle-Blower Hotline

There are no specific provisions regarding whistle-blower hotlines. Thus, the processing of Personal Data collected via whistle-blower hotlines is subject to the general provisions of the PPD. To the extent that data collected via whistle-blower hotlines concern employees, the employer is not required to
comply with the obligation to provide notice of the data processing to the GIODO. Finally, considering that the GIODO usually follows the opinions of the Article 29 Working Party, the guidelines of document WP 117 should be observed.

18. E-Discovery

Implementing an e-discovery process in which electronically stored information is reviewed, processed and presented by an organization for the purposes of litigation or regulatory requests may raise questions as to: (i) the legal basis of processing the data contained in the electronically processed information; as well as (ii) the right of privacy of the employees in the organization. For this reason employers should inform their employees of the implementation of an e-discovery system, including the monitoring of electronic communications. Nevertheless, employees may request the employer to destroy any private information stored as a consequence of the implementation of the e-discovery system.

19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

20. Cookies

There are specific laws that regulate the deployment of cookies. The Telecommunications Law provides for specific rules regarding the use and collection of data by means of the deployment of cookies, in order to secure the privacy of end users. Additionally, the use of cookies must comply with data privacy laws.

Consent of Data Subjects must be obtained before cookies can be used. Consent may be expressed through appropriate settings of the online browser.

Under the GDPR “online identifiers” have been explicitly recognized as Personal Data. Some types of cookies are likely to identify an individual, although they may be considered Personal Data under the GDPR.

21. Direct Marketing

Polish law recognizes direct marketing activities of controller’s own products and services as processing carried out for controller’s legitimate interest, therefore Data Subject’s consent for data processing is not required.
However, separate legal provisions of the Polish law require organizations carrying out electronic direct marketing activities to obtain specific types of customer’s consents:

1. a consent to use telecommunications terminal equipment or automated calling systems for direct marketing purposes;
2. a consent to receive unsolicited marketing communications via means of electronic communication, including emails.

Similarly as under current legislation, the GDPR recognizes direct marketing activities as processing carried out for controller’s legitimate interest. However, also under GDPR and presumably until the e-privacy Regulation is passed into law and enters into force, those specific consent requirements for electronic direct marketing will still apply.
Portugal

César Bessa Monteiro
Lisbon
Tel: +351 217 231 800
bessa.monteiro@abreuadvogados.com

César Bessa Monteiro, Jr.
Lisbon
Tel: +351 217 231 800
cesar.bmonteiro@abreuadvogados.com

Ricardo Henriques
Lisbon
Tel: +351 217 231 800
ricardo.henriques@abreuadvogados.com
1. Recent Privacy Developments

a. Retention of Personal Data resulting from Call Recording

On 27 July 2017, the Portuguese Data Protection Authority (CNPD) has issued Decision 1039/2017 which amends prior Decision 629/2010, and in particular the maximum permissible periods for retaining Personal Data resulting from call recordings.

Pursuant to Decision 629/2010, the processing of Personal Data resulting from call recording is only allowed in three situations: (i) in the context of a contractual relationship, for purposes of evidencing the existence of commercial transactions and any other communications regarding the contractual relationship; (ii) in the context of emergency situations; and (iii) for purposes of monitoring the quality of the service.

Also pursuant to said Decision 629/2010, Personal Data resulting from call recordings in the situations (i) and (ii) above may only be retained for a maximum period of 90-days, while Personal Data resulting from call recordings for purposes of quality monitoring may only be retained for a maximum period of 30-days.

In view of the increase of distance contracts and taking into account that the 90-day maximum retention period for “contractual” purposes was, in some cases, non-compliant with retention duties imposed by law in certain contractual relationships, CNPD issued Decision 1039/2017 which amends the maximum retention period applicable to Personal Data resulting from call recording in the context of contractual relationships (under (i) above).

According to this new Decision, the Personal Data resulting from call recording in the context of a contractual relationship, for purposes of evidencing the existence of commercial transactions and any other communications regarding the contractual relationship shall be retained as follows:

a. In relation to generic distance contracts, the Personal Data resulting from call recording may be retained for a maximum period of 24 (twenty-four) months plus the corresponding statute of limitation period. Where the distance contract refers to an insurance activity, the Personal Data must be retained for the duration of the contractual relationship, or longer if contractual obligations are still to be fulfilled;

b. In relation to electronic communications contracts with minimum binding periods, Personal Data resulting from call recording must be retained for the duration of the binding period (6, 12 or 24 months) plus the statute of limitation period which, in these cases, is six months. Nonetheless, the maximum retention period must not exceed 30 months in any event (i.e., regardless of the binding period agreed);
c. In relation to electronic communications contracts in general, Personal Data resulting from call recording must be retained for the duration of the contract plus the statute of limitation period which, in these cases, is six months, with a maximum retention period of 30 months. In the event of termination of the contract, Personal Data may only be retained for the six months following the termination. Where the contract is not concluded, call records must be deleted;

d. Finally, in relation to financial operations, the Law against Money Laundering and Terrorist Financing requires the retention of any records, including call records, for a period of seven years in order to allow the reconstitution of the operation. However, the CNPD clarifies that the retention duty is only established for supervision and control purposes. Therefore, for purposes of evidence of the commercial transactions, the general retention period applies.

b. Access to Metadata by the Information Services of the Portuguese Republic

Organic Law 4/2017, published on 25 August 2017, regulates the access by the Security Information Service (SIS) and the Strategic Defense Information Service (SIED) to telecommunications and internet data. This Law has entered into force on 30 August 2017.

Information Services are now able to access the identification, location and traffic data relating to the users of electronic communications services, for purposes of national defense, internal security and prevention of acts of sabotage, espionage, terrorism, proliferation of weapons of mass destruction and highly organized crime.

However, the access by the Information Services to such data is not unrestricted and is subject to certain conditions, including prior and subsequent judicial control.

Thus, Organic Law 4/2017 largely reflects the recent case law of the Court of Justice of the European Union in the Digital Rights Ireland judgment of 8 April 2014 and in the Tele2/Watson judgment of 21 December 2016, both reinforcing the need for intrusions in electronic communications to be subject to clear limits and objective material and procedural conditions.

This Law is a second attempt to regulate the access of the Information Services to metadata, after a first unsuccessful attempt in 2015, which was declared unconstitutional by the Portuguese Constitutional Court (Judgment 403/2015, of 27 August 2015), following a preventive control of the constitutionality.

The constitutionality of Organic Law 4/2017 is also being called into question by two political parties as well as the CNPD. The latter, in its opinion of 30
May 2017 on this Law, has considered that the same “infringes the prohibition of intrusion in the electronic communications provided for in the Constitution of the Portuguese Republic, as well as the rules of the Constitution, the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights regarding private and family life, personal data protection and privacy in the communications”.

Therefore, we may see this question of constitutionality being brought before the Portuguese Constitutional Court.

2. Emerging Privacy Issues and Trends

a. Data retention

The CNPD has concluded that the Portuguese Data Retention Law 32/2008, of July 17 infringes the Constitution of the Portuguese Republic, namely the principle of proportionality and the right to privacy, and recommends the revision of the Data Retention Law. The Data Retention Law transposes into national law Directive 2006/24/EC of 15 March 2006 which was declared invalid by the Court of Justice of the EU in April 2014.

The CNPD has issued on 9 May 2017, Decision 641/2017 which criticizes the Data Retention Law as follows:

- the data retention regime applies to all traffic and location data of all users of electronic communications in Portugal without differentiation
- the security measures established by the Data Retention Law are generic and the established 1-year retention period is excessive
- the Data Retention Law is silent as to objective criteria regarding the profile and the number of persons which may access and use the retained data and, as such, there is a risk of misuse of data.

On 18 July 2017, the CNPD has issued Decision 1008/2017 stating that it will no longer apply the Data Retention Law in the cases submitted to it for assessment.

By way of contrast, in its recent Decision 420/2017, issued on 13 July 2017, the Portuguese Constitutional Court has declared the constitutionality of the provision of the Data Retention Law, which requires the providers of publicly available electronic communications services or of a public communications network to retain for a period of one year following the conclusion of the communication, the data necessary to identify the source of a communication, namely the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.
Besides arguing that the Data Retention Law has not merely reproduced Directive 2006/24/EC, but goes further and specifies its provisions, the Portuguese Constitutional Court has stated that it is necessary to consider, on the one hand, the relatively non-invasive nature of the data in question (basic data) and the 1-year retention period and, on the other hand, the particularly serious nature of the crimes in question and the importance of this data for conducting criminal investigations. The Court has also highlighted the limitations on the categories of Data Subjects whose data may be disclosed and the need for prior authorization.

b. GDPR

Ordinance 7456/2017, of August 24 has created a Working Group with the purpose of preparing the Portuguese legislation for the application of the new General Data Protection Regulation (GDPR).

According to the Ordinance, this Working Group is responsible for:

a. conducting a public consultation;

b. identifying the security rules in the processing of Personal Data, resulting from the GDPR, and presenting the different alternatives on the institutional architecture necessary for the operationalization of the GDPR;

c. presenting a draft law proposal until 31 December 2017;

d. assessing, together with other entities, the best option to ensure the training of Public Administration officials on the GDPR.

For the purposes of drafting the legislation referred to hereabove, the Working Group shall work with the relevant departments of the Portuguese Government and Public Administration.

Following the referred Ordinance, the Portuguese Government has held until 30 September 2017, a public consultation on the following topics:

1. additional requirements and limits on the processing of special categories of Personal Data – genetic, biometric and health data;

2. the need for specific rules on the processing of Personal Data in the labor context and corresponding guarantees;

3. the need for specific rules on data portability between entities providing financial, banking, insurance and communications services, or other areas or sectors of activity;

4. conditions applicable to the consent of children as to information society services;

5. reinforcement of the right to erase data (“right to be forgotten”);
6. reinforcement of the exceptions applicable to individual automated decisions, including profile definition;

7. appointment, position and duties of the data protection officer.

3. Law Applicable


Data protection rules may also be found in the following laws:

1. Constitution of the Portuguese Republic (available in English at http://www.cnpd.pt/english/bin/legislation/article_35.HTM);


3. Law 41/2004 of 18 August 2004 on the processing of Personal Data and the protection of privacy in the electronic communications sector, as modified by the Law 46/2014 of 29 August 2014 (available in English at http://www.anacom.pt/render.jsp?contentId=976164#.V7W7IVQrKUk);


9. Law 51/2006 of 29 August 2006 (only available in Portuguese at http://www.cnpd.pt/bin/legis/nacional/LEI51-2006-VVG-AUTOESTRADAS.pdf) regarding surveillance cameras; and


4. Key Privacy Concepts
   a. Personal Data

   Personal Data shall mean any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person (“Data Subject”). An “identifiable person” is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

   It is worth noting that data will only be considered “anonymous”, and therefore not “Personal Data”, provided that the individual to whom it relates cannot be identified, whether by the Data Controller or by any other person, taking account of all the means likely to be reasonably used by either the controller or any other person to identify that individual.

   b. Data Processing

   Data Processing is defined as any operation or set of operations performed on Personal Data, whether wholly or partly by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

   c. Processing by Data Controllers

   The DPL applies to a natural or legal person, public authority, agency or any other body that, alone or jointly with others, determines the purposes and means of the processing of Personal Data (“Controller”).

   Therefore, where the purposes and means of processing are determined by laws or regulations, the controller shall be designated in the act establishing the organization and functioning or in the statutes of the legal or statutory body competent to process the Personal Data concerned.
d. Jurisdiction/Territoriality
The DPL shall apply to the processing of Personal Data carried out:

- in the context of the activities of an establishment of the controller in Portugal;
- outside Portugal, but in a place where Portuguese law applies by virtue of international public law; and
- by controllers who are not established in European Union territory and who, for purposes of processing Personal Data, make use of equipment, automated or otherwise, situated in Portuguese territory, unless such equipment is only used for purposes of transit through the territory of the European Union.

Thus, the DPL is applicable according to jurisdictional criteria and independently of the nationality of the Data Subjects whose data is being processed.

“Establishment” shall be considered, irrespective of its legal structure, as any stable installation allowing the effective and real undertaking of an activity. Please note that a mere representative may sometimes be sufficient to conclude the existence of an “establishment”, as the EU Court of Justice has already decided that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.

e. Sensitive Personal Data
The DPL defines “Sensitive Personal Data” as any information regarding philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data.

As per Article 7 of the DPL, the processing of such data is permitted if:

- the Data Subject has given his/her explicit consent for such processing;
- it is foreseen in a legal provision;
- it is essential for exercising the legal or statutory rights of the controller based on important public interests grounds;
- it is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his/her consent;
• it is carried out with the Data Subject’s consent in the course of its legitimate activities by a foundation, association or non-profit seeking body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to a third party without the consent of the Data Subjects;

• it relates to data which is manifestly made public by the Data Subject, provided his/her consent for the processing can be clearly inferred from his/her declarations; or

• it is necessary for the establishment, exercise or defense of legal claims and is exclusively carried out for that purpose.

In such case, data relative to those assessments will fall within the category of sensitive data and will be subject to specific security measures, and the processing of such data will be subject to prior authorization from the CNPD.

Furthermore, processing of data relating to health and sex life, including genetic data, is only permitted if necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided that data is processed by a health professional bound by professional secrecy or by another person also subject to an equivalent obligation of secrecy and is notified to the CNPD, and where suitable safeguards are provided.

Finally, although not qualified by the DPL as “sensitive data”, there are special categories of data processing of which is subject to certain requirements, such as prior authorization from the CNPD, pursuant to Article 28 of the DPL:

a. data processing relating to suspicion of illegal activities, criminal and administrative offenses and decisions applying penalties, security measures, fines and additional penalties is only permitted if:

   o central registers to persons suspected of these activities were created and kept by public services vested with that specific responsibility by virtue of the law establishing their organization and functioning, subject to observance of procedural and data protection rules provided for in a legal order, with the prior opinion of the CNPD; or

   o such processing is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the Data Subject are not overriding. However, it is mandatory to obtain authorization from the CNPD and to observe rules for the protection of data and the security of information; and
b. Personal Data relating to credit (worthiness) and the solvency of the Data Subjects. It should also be noted that the CNPD has issued Guideline 156/09 on credit information.

f. Employee Personal Data

There is no specific legal framework in the EU governing data processing in the context of employment. In the (outgoing) Data Protection Directive, employment relations are specifically referred to only in Article 8 (2), which concerns the processing of sensitive data.

Notwithstanding the above, Employee Personal Data may include Sensitive Personal Data and non-Sensitive Personal Data. With regard to sensitive Employee Personal Data, its processing is subject to the conditions stated above in paragraph (d) in accordance with number 4 of Article 17 of the Portuguese Labour Code. In addition, Articles 18, 19, 20, 21 and 22 of the aforementioned code are also applicable when considering the privacy of the employee’s private life, such as medical examinations and biometric data.

Regarding the **monitoring of the employee’s email** by the employer, the Portuguese Labour Code does not govern this matter in detail, only stating in Article 22 that the employer has the right to monitor, having however to take into account the employee’s right of privacy. Nevertheless, the CNPD has approved official Guidelines concerning the monitoring of the use of electronic communications by employees at the workplace and the procedures to be adopted by the employers.

In general terms, these Guidelines establish that when an employer monitors the use of emails, calls and/or the Internet to verify whether the employee’s use is only for professional purposes and not for excessive private (non-permitted use), then it needs to have an adequate policy in place and obtain prior authorization from the CNPD.

Employers should adopt security measures, which do not include a specific verification of the employee’s private information, even if it is intended for disciplinary purposes. Examples of specific security measures, include: implementing measures to avoid access to information by non-authorized personnel; use registration to identify the user; restrict access to servers; implementing logs that register who made such access, date and hour (timestamp), controlling the operations made through such access by a sequential number (ID), and applying a hash field to the previous elements.

The controller should identify all irregular situations in order to develop a warning system to alert irregular use. A policy concerning the use of logs should be implemented, as well as the preparation of periodic analysis reports. Logs can only be stored for a maximum period of one year.
Additionally, with regard to **Sensitive Employee Personal Data**, the CNPD has approved official Guidelines on the processing of Personal Data for preventive and curative medicine purposes regarding the control of psychoactive substances given to employees.

Furthermore, the CNPD has also approved Guidelines on the general principles regarding the processing of Personal Data as a result of the **use of geolocation devices in an employment context**. In an employment context, these devices are mainly used in vehicles, smartphones or laptops owned by the employer but made available to the employee to perform his or her professional activity.

The CNPD considers the use of such geolocation devices as processing of sensitive data stipulated in paragraph 2 of Article 20 of the Portuguese Labour Code. This provision allows the employer to use means of remote supervision in the workplace being, for this reason, legitimate grounds for processing data.

The CNPD likewise considers consent given by the employees as valid grounds for processing of this type of data.

According to the Guidelines, geolocation is expressly prohibited for the following purposes:

1. employee performance control;
2. proof of compliance with contractual obligations;
3. ensuring compliance with road traffic legislation; and
4. tracking the vehicle when it is being used for private purposes.

As for vehicles, the CNPD has allowed the processing of data resulting from the use of geolocation devices in an employment context, for the following purposes:

1. Fleet management on external service – (i) external technical assistance or home assistance, (ii) goods distribution, (iii) passenger transportation, (iv) goods transportation, and (v) private security; and
2. Goods Protection – (i) criminal investigation and goods recovery in case of theft, (ii) transportation of dangerous materials, and (iii) high value materials.

Regarding smartphones and laptops, the CNPD stated that the employer cannot use geolocation devices on these or access the information when available by telecommunications operators or install mobile applications on smartphones which activate GPS sensors. However, the CNPD has considered the installation of MDM (Mobile Device Management) technologies admissible to ensure the remote protection of companies’ information.
The Guidelines also cover situations where the employer knows of criminal evidence resulting from the processing of sensitive data. In this case, the CNPD has declared that this information can be used, under certain circumstances, in criminal and disciplinary proceedings.

The employer must inform the employees of the existence of geolocation devices, especially when they are imbedded in cars, smartphones or laptops used by employees to perform their work, and must obtain an authorization from the CNPD by means of a specific form, available at https://www.cnpd.pt/bin/legal/forms.htm, prior to such processing of sensitive data.

As per Article 6 of the DPL, non-Sensitive Personal Data may be processed by a Data Controller (e.g., the employer), in particular, for the performance of a contract to which the Data Subject is a party (e.g., an employment contract), for compliance with a legal obligation to which the controller is subject or where processing is necessary for the purposes of legitimate interests of the controller to whom the data is disclosed, except where such interests should be overridden by the interests for the fundamental rights, freedoms and guarantees of the Data Subject.

Pursuant to the GDPR, the processing of sensitive data will be specifically allowed if it is necessary for carrying out the obligations and exercising specific rights of the controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law.

In addition, non-Sensitive Personal Data may be processed if the Data Subject (e.g., the employee) has unambiguously given his/her consent. It is worth noting that consent as a legal basis for processing employment data must be analyzed carefully given the fact that the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether consent was given in a free basis or not (see Section 5 (e) below).

The CNPD has issued two exemptions concerning the prior notification requirement for data processing regarding employment Personal Data. The authorizations for the exemptions set some conditions which need to be met in order to have the data processing exempted. The data processing exempted from notification concerns the following purposes:

1. Exemption 1/99 – Processing of employees’ salaries and retributions; and
2. Exemption 3/99 – Invoicing and contacts with clients, suppliers and service providers.
The CNPD has also issued several **Guidelines related to the processing of Employee Personal Data**, some of which are already referred to above:

- principles applicable to the processing of Personal Data as a result of the use of geolocation devices in an employment context (2014);
- principles applicable to the monitoring of the use of information technologies for private purposes in the workplace (2013);
- principles applicable to the processing of data in relation to preventive and healing medicine within the scope of alcohol and drug controls performed on employees (2010);
- principles applicable to the processing of data within the scope of information management for Health and Safety Services in the workplace (2010);
- principles applicable to the processing of data with the purpose of internal communication of irregular financial management acts – Ethics Lines (2009); and
- principles applicable to the processing of biometric data for access and assiduity control (2004).

### 5. Consent

#### a. General

According to the DPL, a Data Subject’s consent shall mean any freely given, specific and informed indication of his/her wishes, by which the Data Subject signifies his/her agreement to Personal Data relating to him/her being processed.

A Data Subject’s consent is one of the legitimate grounds for data processing. Thus, consent as a legal basis for processing Personal Data must be free, informed and specific. On the other hand, consent must be given unambiguously by acting in a way that leaves no doubt that the Data Subject agrees to the processing of his or her data.

Moreover, there are no limitations as to how consent may be obtained: on paper with hand-written signature, electronically, via the Internet or intranet or via email. Preferably, it should be in a format that can easily be reproduced as evidence.

Lastly, consent can be withdrawn at any time and there should be no requirement to give reasons for withdrawal and no risk of negative consequences over and above the termination of any benefits which may have derived from the previously agreed data use.
b. **Sensitive Data**

As mentioned in Section 4 (e) above, the processing of sensitive data is prohibited unless the Data Subject has given his/her explicit consent for such processing.

Therefore, consent to sensitive data processing must be explicit and given in any form.

c. **Minors**

Under Portuguese legislation, in particular the Data Protection laws, regarding the execution of contracts by minors, it is determined that the following relevant age ranges are to be considered:

1. 0-16 – may not conclude a valid contract under Portuguese law.
2. 16 – 18 – equally may not conclude a valid contract under Portuguese law. However, there are some exceptions: agreements commonly concluded in small, current day-to-day activities and legal transactions related to the minor’s profession, art or occupation, where the minor was authorized to exercise or practice in the exercise of profession, art or occupation. Additionally, minors over 16 can carry out administrative acts or dispose of goods that they have acquired with the profits of their profession. Only minors above the age of 16 may be criminally liable.

The CNPD has issued a Guideline where it stated that children have, inter alia, the right to access data, amend it, and block it. Children also have the right to oppose the processing of their data.

However, based on the Guideline (which referred to the national regulations), it seems that minors below 13 will not be able to provide a valid consent for the processing of their data. Minors aged 13 and over will be able to grant such consent, subject to a lack of opposition (their parents should be aware of the facts) from their parents (or other legal representative).

In terms of the above-mentioned Guideline, it is determined that “**minors have the right to be informed of the processing from adolescence**” and, “**from a certain age, minors have legitimacy to consent to the processing of some Personal Data**” (e.g., regarding their religious beliefs or the disclosure of information on the Internet).

In accordance with Portuguese Civil and Criminal law, we hold the opinion that only minors above 16 have such capacity, and therefore minors of said age do not have the capacity to exercise their own rights, which should be supplied by parental responsibility or alternatively by guardianship.

In addition, parents or legal guardians have the right to access the information once provided by the minor and to rectify or erase their Personal Data.
Finally, the General Data Protection Regulation clarifies that in relation to the offer of information society services directly to a child on the basis of the child’s consent, the processing of the Personal Data of a child shall be lawful where the child is at least 16 years old, and, if younger, consent must be given or authorized by the holder of parental responsibility over the child. The GDPR allows Member States to provide for a younger age of consent (which must not be below 13).

d. Employee Consent

Although Portuguese Legislation does not govern this matter in detail, the CNPD has followed the opinion of the Article 29 Working Party.

The Article 29 Working Party has analyzed the significance of consent as a legal basis for processing employment data. The Working Party found that the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether consent was given freely or not. The circumstances under which consent is requested should, therefore, be carefully considered when assessing the validity of consent in the employment context.

The Working Party acknowledges, however, that there will be cases where it is appropriate for an employer to rely upon consent, for example, in an international organization where employees wish to take advantage of opportunities in a third country.

e. Online/Electronic Consent

Although Portuguese Legislation does not have specific regulation on electronic consent, it is understood that consent may be given electronically. In its Opinion 15/2011 on consent, the Article 29 Working Party stated that “In the online environment, explicit consent may be given by using electronic or digital signatures. However, it can also be given through clickable buttons depending on the context, sending confirmatory emails, clicking on icons, etc”.

Thus, online/electronic consent may be given, e.g., by clicking a button, and not being required to provide an advanced electronic signature under Article 2(2) eSignature Directive 1999/93/EC.

6. Information/Notice Requirements

As per Article 10 of the DPL, a Data Subject must be informed of the following when data relating to himself or herself is collected:

- the identity of the controller and of his/her representative, if any;
- the purposes of the processing;
- other information, such as:
  - the recipients or categories of recipients;
whether replies are obligatory or voluntary, as well as the possible
csequences of failure to reply; and

o the existence and conditions of the right of access and the right to
rectify, provided they are necessary, taking into account the specific
circumstances of collection of data in order to guarantee to the Data
Subject that it will be processed fairly.

The documents supporting the collection of Personal Data shall contain the
information set down above.

Under the GDPR, the information/notice requirements will expand.

7. Processing Rules
An organization that processes Personal Data must limit the use of the
Personal Data to only those activities which are necessary to fulfill the
identified purpose(s) for which the Personal Data was collected; and
delete/anonymize Personal Data once the stated purposes have been fulfilled
and legal obligations met.

8. Rights of Individuals
Portuguese law expressly provides rights to be granted in favor of Data
Subjects. These rights include the access, rectification, cancellation and
objection for the collection and treatment of Personal Data.

Data Subjects must be informed of the existence of their right of access. In
substance, any Data Subject has the right to obtain from the Data Controller:

1. confirmation as to whether or not data relating to him or her is being
processed and information at least as to the purposes of the processing,
the categories of data concerned, and the recipients or categories of
recipients to whom the data is disclosed, as well as whether replies are
obligatory or voluntary and the possible consequences of failure to reply; and

2. communication in an intelligible form of the data undergoing processing
and of any available information as to their source.

The right of access consists of the right to obtain free of charge information on
his/her Personal Data, its origin and its communication.

On the other hand, a Data Subject must be informed of additional rights.

1. Rights of rectification or cancellation: by means of these rights, the Data
Subject may request amendment, or even deletion, of its data where
he/she considers that the data is inaccurate or incomplete. Cancellation
implies that the Personal Data shall be blocked and only maintained at
the disposal of public entities or courts in connection with potential
liabilities arising from the data processing and during relevant statutes of limitation.

2. Right of objection: Data Subjects have the right to request that the processing of his or her Personal Data not be carried out or ceased in certain situations, such as when consent is not necessary or when the purpose of processing is advertising or commercial research activities.

As per the above, a Data Subject must be informed about his/her right to request the rectification of inaccurate data, as well to object, at any time and for free, to the processing of the data for direct marketing purposes.

9. Registration/Notification Requirements

Data controllers are obliged to notify or request prior authorization from the CNPD regarding Personal Data files. This notification or authorization must be performed prior to the use of any file or any data processing operation. Any change of contents of the file or its use, including its cancellation, must be communicated to the CNPD. This obligation must be performed by means of the forms available at the CNPD’s webpage and must be sent by the Data Controller electronically. (http://www.cnpd.pt/bin/legal/forms.htm).

Nevertheless, there are some exemptions to the above-mentioned obligation of notification, namely the following:

1. Exemption 1/99 – Processing of employees’ salaries and retributions;
2. Exemption 2/99 – Management of libraries’ and archives’ users;
3. Exemption 3/99 – Invoicing and contacts with clients, suppliers and service providers;
4. Exemption 4/99 – Administrative management of employees, staff and service providers;
5. Exemption 5/99 – Access control (entries and exits) in buildings; and

These exemptions are subject to certain conditions and limitations, in order to avoid the notification obligation before the CNPD.

The notification and authorization files should be completed electronically, which requires the payment of a EUR 75.00 fee and EUR 150.00 fee, respectively.

After receiving the files, the CNPD should issue a formal confirmation for the collection and processing of Personal Data. However, when the Data Controller is only requested to notify the CNPD of the collection and processing of Personal Data, it can automatically proceed with the data
processing activities. On the contrary, when it has submitted an authorization file, the Data Controller should obtain prior confirmation from the CNPD that it is possible to collect and process Personal Data.

The notification form requires detailed information, including the following:

1. the surname, first names and full address or legal name and registered office, activity, phone number and email of the Data Controller;
2. the contact person of the Data Controller;
3. the processing entities;
4. the purpose, or purposes, of the processing;
5. the categories of Personal Data to be processed including a detailed description of the same;
6. if Sensitive Personal Data is collected and a description of the same;
7. if Personal Data is disclosed/transferred to third parties (whether within the EU/EEA or outside the EU/EEA) and the grounds for such transfer when the third parties are located outside the EU/EEA;
8. if there is combination of data between different databases from the same Data Controller or from different Data Controllers;
9. the manner in which Data Subjects are informed, and to whom access requests should be submitted;
10. the period of time that Personal Data is stored; and
11. a general description of security measures;
12. If the Personal Data is to be transferred to a foreign country, the categories of Personal Data to be transferred, the purposes, the legal grounds on which said transfer relies on and the destination country to which each category of Personal Data may be transferred.

Besides the general notification form, there are forms available for the notification of (i) video surveillance, (ii) the monitoring of use of the telephone, internet and email at the workplace, (iii) the control of psychoactive substances, (iv) the control, by means of biometric data, of the access and attendance of the employees, (v) the geolocation of vehicles in an employment context, and (vi) clinical research.

10. Data Protection Officers

No specific requirements apply. The appointment of a data protection officer is not regulated under Portuguese law. Nevertheless, such appointment may become necessary under the General Data Protection Regulation.
11. International Data Transfers

Transfers of Personal Data from Portugal to countries offering an equivalent level of protection may take place freely, if it is a country that has been recognized by the European Commission as having adequate data protection laws. Said countries are EU and EEA Member States, Argentina, Israel, Andorra, Faroe Islands, Canada, Switzerland, Guernsey, the Isle of Man, Jersey, New Zealand, Uruguay, and any other countries deemed to grant an equivalent level of protection under a decision of the European Commission. International transfers to third countries not granting an equivalent level of protection, such as the US, may only take place under the DPL where the prior authorization of the CNPD has been obtained. Exceptions to this situation are where:

1. the Data Subject has given its unambiguous consent to the transfer;
2. the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or for the implementation of pre-contractual measures taken upon the Data Subject’s request;
3. the transfer is necessary for the performance of a contract concluded or to be concluded in the interest of the Data Subject between the Data Controller and a third party;
4. the transfer is necessary for litigation purposes; and
5. the transfer is in the public interest, for tax or other authorities.

The transfer of Personal Data to a non-EU/EEA country with inadequate protection levels is also permitted with the prior authorization of the CNPD if a data transfer agreement is used and the agreement incorporates the EU model contractual clauses for the transfer of Personal Data to third countries adopted by the European Commission on 15 June 2001 and 27 December 2004 (Data Controller to Data Controller) or on 5 February 2010 (Data Controller to Data Processor). Please note that if the EU model contractual clauses are used as grounds to such transfers, the CNPD will still process the authorization request as if it were a mere notification, since it considers that the level of data protection will be adequate in such case. This will allow immediately starting the international transfers of data upon filing. That said, the Court of Justice of the European Union is currently considering the validity of the Standard Contractual Clauses.

Finally, as of 1 August 2016, transfers to the US are permitted where the recipient has certified itself under the EU-US Privacy Shield and provided that the transfers would be legal within Portugal.
12. Security Requirements

In order to guarantee the security of processing, the Data Controller must implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, having regard to the state of the art and the cost of their implementation. Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

With regard to sensitive data, Data Controllers shall take the appropriate measures to:

- prevent unauthorized persons from entering the premises used for processing such data (control of entry to the premises);
- prevent data media from being read, copied, altered or removed by unauthorized persons (control of data media);
- prevent unauthorized input and unauthorized obtaining of knowledge, alteration or elimination of Personal Data input (control of input);
- prevent automatic data processing systems from being used by unauthorized persons by means of data transmission premises (control of use);
- guarantee that authorized persons may only access data covered by the authorization (control of access);
- guarantee the checking of the entities to which Personal Data may be transmitted by means of data transmission premises (control of transmission);
- guarantee that it is possible to check a posteriori, in a period appropriate to the nature of the processing, which Personal Data is input, when and by whom (control of input); and
- in transmitting Personal Data and in transporting the respective media, prevent unauthorized reading, copying, alteration or elimination of data (control of transport).

Furthermore, the Law 12/2005 of 26 January 2005 on Genetic and Health Information foresees the following specific security measures:

- health information, including recorded clinical data, analysis results and other tests, interventions and diagnosis, is owned by the employee.
- the access to health information is provided by a health professional;
• protection of confidentiality;
• security of facilities and equipment;
• control of the access to sensitive data.

Additionally, please also take into consideration that the CNPD has approved several official Guidelines concerning the processing of health and medical information, specifically on clinical trials, clinical studies and medicinal products for human consumption.

According to the CNPD, the controllers and processors of such health data must observe special security measures in order to comply with specific security standards stated by the authority. For this reason, the CNPD has established the following measures, among others:

• separation (physical and logical) between health data and administrative data by creating user profiles with different access levels;
• users’ passwords should be frequently changed;
• control of access to information by avoiding access by unauthorized staff;
• encrypted transmission of health data;
• sensitive data backups; and
• logging of all access to health information.

Finally, in what concerns the processing of Personal Data and the protection of privacy in the electronic communications sector, companies providing electronic communication services must take appropriate technical and organizational measures in order to guarantee the security of their services, such as:

• ensuring that only authorized staff have access to Personal Data and only to legally authorized purposes;
• protecting Personal Data against destruction, loss, alteration, disclosure or unauthorized access;
• ensuring the implementation of a safety policy in the processing of Personal Data.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

It is possible for the Data Controller to entrust the processing of Personal Data to a processor. In what concerns the processing of Personal Data by a third-party processor, the Data Controller must choose a processor who is capable of offering sufficient guarantees in respect of the technical security measures
and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

The controller is defined as the one who determines the purposes and means of the processing of Personal Data. If this power is delegated to a third-party processor, the controller must be able to interfere with the decisions of the processor regarding the means of processing. Thereafter, the relationship between controller and processor, i.e., the carrying out of processing by way of a processor, must be governed (i) by a written contract or legal act binding the processor to the controller, (ii) the processor shall act only on instructions from the controller, and (iii) the processor must comply with the security measures as foreseen in Portuguese legislation.

In addition, an equal obligation must be observed by any person acting under the authority of the controller or the processor, including the processor himself/herself, who has access to Personal Data, to not process the data except on instructions from the controller, unless he/she is required to do so by law.

14. Enforcement and Sanctions

Civil and criminal penalties, as well as private rights of action, can be applicable.

The CNPD has the power to investigate complaints and cases, and to order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions including administrative fines. These orders can be appealed to the courts.

Individuals can file complaints with the CNPD, and seek a judicial remedy for violations of the law. As the DPL can be applicable, fines ranging from EUR 250.00 to EUR 2,500.00 in the case of natural persons and fines ranging from EUR 1,500.00 to EUR 15,000.00 in the case of legal persons, and imprisonment of up to one year, can be imposed for breach of data protection laws.

The above fines may be increased to double the amount (i.e., EUR 500.00 and up to EUR 5,000.00 in the case of natural persons, and EUR 3,000.00 up to EUR 30,000.00 in the case of legal persons) if referring to the requirements of sensitive data or Data Subject to prior authorization. In this case, it is also possible to be subject to imprisonment for up to two years.

In addition, infringement of the access to personal information storage in the user’s terminal equipment is punishable with a fine ranging from a minimum of EUR 1,500.00 to a maximum of EUR 25,000.00 when the offender is an individual, and from a minimum of EUR 5,000.00 to a maximum of EUR 5,000,000.00 when it is the legal entity that breaches the duty (according to paragraph 1 of Article 14 of Law No 41/2004, August 18).
Finally, directors and individuals within a company may also face legal sanctions for the breach of data protection laws.

15. Data Security Breach

In Portugal, the only data breach notifications that are legally required concern electronic communication providers.

As per Article 3-A of the Law 41/2004 of 18 August 2004 on the processing of Personal Data and the protection of privacy in the electronic communications sector, as modified by the Law 46/2014 of 29 August 2014, if there is a risk that the breach will negatively affect the Personal Data, the subscriber or individual whose data could be affected must be notified by the electronic communications service provider.

This notification obligation will not apply if the companies offering publicly available electronic communications services are able to prove to the CNPD that they have taken the necessary technological protection measures and that these measures were applied to the data breached.

This legal disposition also requires companies that offer electronic communication services to notify the CNPD whenever there is a Personal Data breach.

Whenever the CNPD verifies the infringement of any duty or obligation, it shall notify the offender of such fact and give him/her the opportunity to respond within a minimum period of 10 days and, if appropriate, to end the non-compliance.

Infringement of the notification duty amounts to an administrative offense punishable with a fine ranging from a minimum of EUR 1,500.00 and a maximum of EUR 25,000.00 when the offender is an individual, and from a minimum of EUR 5,000.00 and a maximum of EUR 5,000,000.00 when it is the legal entity that breaches the duty.

Non-compliance with the notification requirements is punishable with a fine ranging from a minimum of EUR 500.00 and a maximum of EUR 20,000.00 when the offender is an individual, and from a minimum of EUR 2,500.00 and a maximum of EUR 2,250,000.00 when it is the legal entity that breaches the duty.

16. Accountability

Accountability requires the active implementation of measures by controllers to promote and safeguard data protection in their processing activities. Similar information is foreseen in number 2 of Article 5 of the DPL, in which the controller shall ensure that Personal Data is processed in accordance with the rules established therein.
In accordance with the Article 29 Working Party’s opinion, the essence of accountability is the controller’s obligation to:

- put measures in place which would – under normal circumstances – guarantee that data protection rules are adhered to in the context of processing operations; and
- have documentation ready which proves to Data Subjects and to supervisory authorities what measures have been taken to achieve adherence to the data protection rules.

The principle of accountability requires controllers to actively demonstrate compliance and not merely wait for Data Subjects or supervisory authorities to point out shortcomings.

17. Whistle-Blower Hotline

The CNPD issued Guidelines 765/2009 for data processing in the context of whistle-blower hotlines, namely its implementation and how to proceed. This type of data collection and processing is applicable to Personal Data related to accounting, internal accounting controls and auditing matters. The hotline may be used against bribery, banking and other financial crimes.

The processing of Personal Data relating to whistle-blower hotlines is qualified as a special category of Personal Data pursuant Article 8 of the same law and, for that purpose, it is subject to prior control and authorization from the CNPD.

The authorization file should specify in detail the legitimacy and the need for the proposed processing, and Data Controllers must inform their employees about the existence of the whistle-blower hotline and how they can use it, for example by means of a company Privacy Policy.

The following categories of data are considered sufficient:

- Identity and professional category of the whistleblower;
- Identity and professional category of the denounced;
- Identity and professional functions of the people that collect and process Personal Data;
- The facts that are included in the suspicious activities;
- The elements collected regarding the investigation procedure;
- The whistle-blower purpose.
18. E-Discovery

The implementation of an e-discovery system within an organization, whereby employers are entitled to monitor equipment (phone calls, email and Internet access) used by employees in their professional activities, raises issues regarding the right of privacy and the right to the secrecy of communications.

Pursuant to Articles 26 and 35 of the Constitution of the Portuguese Republic, all citizens have the right to privacy and the right to protection of their own Personal Data. On the other hand, the secrecy of communication is established in Articles 32 and 34 of the Constitution of the Portuguese Republic and in Article 194 of the Portuguese Criminal Code, in which any intrusion in communications is punishable as a crime.

Other rules regarding this subject may be found in Article 80 of the Portuguese Civil Code and in the Portuguese Labour Code.

Furthermore, the CNPD has approved Guidelines regarding the monitoring of employees in the workplace. These Guidelines have stated the general principles:

- The employer shall – before starting any kind of processing – inform the employee about the conditions under which equipment belonging to the company may be used for private purposes and the level of tolerance admitted; the existence of the processing, its purpose, the means of control adopted, the data processed and its storage, as well as the consequences for the misuse of the communications equipment must be made available to the employee.

- The data processing and the means of control shall be adequate to the business management, to the development of the productive activity and be compatible with the rights and duties of the employees, and must not be abusive or disproportionate in relation to the level of protection of the employee’s private sphere.

- The employer shall use generic monitoring methodologies.

In order to comply with the constitutional rights described above, the CNPD established the following procedures to be adopted by the employers:

1. The level of private use allowed on equipment issued to the employee by the company, the conditions for data processing and the definition of the means of monitoring adopted shall be included in the internal Rules of Procedure ("RoP"), which shall be submitted to the workers’ council for its opinion.

2. The employer shall disclose the content of the RoP, namely by posting it in the company’s headquarters and in all other working places, in order to allow the employees to have full knowledge of it.
3. The employer, as Data Controller, has to request authorization from the CNPD to conduct data processing, enclosing the RoP in the process and specifying the ways used to disclose the conditions of the data processing to the employees.

19. Anti-Spam Filtering

Although there are no specific laws that regulate the use of anti-spam filtering, in general terms and to the extent that the use of an anti-spam filtering solution would involve the use of an organization’s email system for data processing, anti-spam filtering will have to be authorized by the CNPD and will have to comply with data protection laws.

Additionally, it is necessary to inform employees of the monitoring of their emails, namely by referring to the purpose of the spam filtering solution and which entities will process the information contained in it.

20. Cookies

The use of cookies should comply with data protection laws and, therefore, the cookie consent requirement set forth by Directive 2009/136/EC, amending ePrivacy Directive 2002/58/EC, was implemented into Portuguese jurisdiction by Law 46/2012 on August 29, which amended Law 41/2004 of August 18 concerning the processing of Personal Data and the protection of privacy in the electronic communications sector, which determined that:

1. the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information about the purposes of the processing;

2. the Data Controller must give users the possibility to withdraw their consent freely and in an easy manner; and

3. nevertheless, the consent requirement does not prevent any technical storage or access of data:
   a. for the sole purpose of carrying out the transmission of a communication over an electronic communications network; and/or
   b. as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Regarding cookies, the CNPD has not issued formal Guidelines but has expressed its understanding that consent should be explicit. Companies in the market are taking different approaches. Most use a banner on the front page of the website. However, while there are some that opt for an implied consent
when there is continued browsing, others opt for the need to actively dismiss the banner or actively consent to the use of the cookies (which are more prudent approaches). Organizations should also make available a specific cookie policy on their website, together with the privacy policy, in order to comply with the information obligations.

21. Direct Marketing

For direct marketing purposes, Law 46/2012 of August 29, which amended Law 41/2004 of August 18 concerning the processing of Personal Data and the protection of privacy in the electronic communications sector, determined that:

1. the sending of unsolicited communications for direct marketing purposes, namely the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, are subject to the prior and explicit consent of a subscriber;

2. a provider of a certain product or service, that obtained from its customers their electronic contact details, in the context of the commercial relationship or of the service provided, can use such electronic contact details for direct marketing purposes for the service provider’s own similar products or services. However, customers should be clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details:
   a. at the time of their collection; and
   b. on the occasion of each message, in case the customer has not initially refused such use; and

3. it is prohibited to send electronic mails for the purpose of direct marketing if it disguises or conceals the identity of the sender on whose behalf the communication is made, particularly if it does not have a valid address to which the recipient may send a request to stop receiving communications or which encourage recipients to visit websites that are contrary to the purposes of data protection.

The Directorate-General of Consumers is responsible for keeping an updated national list of persons who express their wish not to receive unsolicited direct marketing communications. The Portuguese Direct Marketing Association, through an agreement with the Directorate-General of Consumers, is making available the list to its members free of charge, and to non-members by means of an annual subscription. However, there is some uncertainty as to the completeness of this list as it is not very well known to consumers.
Therefore, companies that send unsolicited communications for direct marketing purposes should keep their own up-to-date list of persons who have consented to receive such communications, as well as of customers who did not object to the reception of the same.
Russia

Edward Bekeschenko
Moscow
Tel: +7 495 787 2717
edward.bekeschenko@bakermckenzie.com

Dmitry Lysenko
Moscow
Tel: +7 495 787 2700
dmitry.lysenko@bakermckenzie.com

Vadim Perevalov
Moscow
Tel: +7 495 787 3184
vadim.perevalov@bakermckenzie.com
1. Recent Privacy Development

**Broader interpretation of Personal Data**

Previously Russian authorities used a rather narrow interpretation of Personal Data, in particular, noting that information constitutes Personal Data only if it allows unambiguous identification of an individual. However, this no longer appears to be the case, as Russian authorities have recently changed their approach and currently apply a broader interpretation of Personal Data.

**Increased fines for data protection violations**

In mid-2017, Russia increased the fines for different violations of Personal Data laws to a maximum of RUB 75,000 (approx. USD 1,300) per violation and introduced different types of punishable offenses.

**Database localization requirements**

Starting from 1 September 2015, Data Controllers collecting Personal Data must ensure that the recording, systematizing, accumulating, storage, verification (including updating and modifying) and retrieval of Personal Data of citizens of the Russian Federation is carried out using databases located on the territory of the Russian Federation. The requirement is very general and applies both to local and foreign Data Controllers collecting Russian citizens’ data.

This requirement is subject to several narrowly defined exceptions. For example, an exception applies if processing Personal Data is necessary in order to execute an international treaty of the Russian Federation in accordance with Russian legislation. On these grounds, booking of airline tickets by airlines was previously considered to be exempt from localization.

While the language of the requirements is still unclear, the regulator has published a non-binding opinion that duplication/mirror databases can be located outside Russia, provided the original (or “master”) databases are located in the Russian Federation and all other conditions for cross-border transfer of Personal Data are met (e.g., the consent of all Data Subjects has been obtained, there is a data transfer agreement with the receiving party setting out the scope and purposes of transfer, etc.).

**Blocking websites for data processing violations**

Federal Law No. 242-FZ also introduced a procedure for blocking websites through which Personal Data is processed in violation of Personal Data laws.

Roskomnadzor, the Russian data protection authority, may bring a civil lawsuit against a person whose website allegedly violates Russian Personal Data laws. Based on a court decision recognizing the violation, Roskomnadzor must notify the website owner through its hosting provider by email about the
court-confirmed violation. If the violation is not cured within three business days following the email notification, Roskomnadzor may order all Russian internet access service providers to block access to the non-compliant website.

Importantly, the above procedure may be applied equally to both Russian and foreign websites, in addition to mobile apps.

The regulator’s authority to conduct inspections relating to data processing rules and exchange of data on the internet has been extended. In addition, the restrictions relating to the frequency and length of inspections and prior notification available under Federal Law No. 294-FZ to safeguard the interests of business have been waived. The regulator now actively monitors various websites for compliance with Russian Personal Data laws, which may also give grounds to non-scheduled (or “surprise”) inspections for Russian companies or additional inquiries into operators of foreign websites.

2. Emerging Privacy Issues and Trends

Russia has recently started enacting laws that require mandatory identification of internet users. As of today this primarily applies to instant messengers and possibly online chats. Use of public Wi-Fi also requires mandatory identification. However, similar restrictions may be introduced for other types of online services, such as social networks and online games, as the relevant initiatives are debated from time to time.

In addition, there are multiple discussions on how to regulate the use of internet users’ data (e.g., geolocation data, cookies, etc.), as well as “Big Data”.

Specific legislative proposals in these areas could potentially be announced in 2018.

3. Law Applicable

The Russian legal regime governing the collection and processing of Personal Data is principally set out in the Federal Law on Personal Data (the “Personal Data Law”) of 27 July 2006 (as amended).

Chapter 14 of the Russian Labor Code also regulates the treatment of employees’ Personal Data.

A number of other laws contain more specific provisions on Personal Data treatment. However, such regulations are based on the same principles as the Personal Data Law.
4. Key Privacy Concepts

a. Personal Data
The Personal Data Law defines “Personal Data” to mean any data related to a directly or indirectly identified or identifiable individual (“Personal Data Subject”).

Unlike in the EU, Russian law does not have any guidance for the interpretation of “directly or indirectly identifiable individuals”, which can potentially result in a very broad definition of Personal Data.

Previously Russian authorities used a rather narrow interpretation of Personal Data, in particular, noting that information constitutes Personal Data only if it allows unambiguous identification of an individual. However, this no longer appears to be the case, as Russian authorities have recently changed their approach and currently apply a broader interpretation of Personal Data.

For instance, Roskomnadzor (Russia’s data protection authority) has initiated several law enforcement actions against telecom companies for selling user activity data to advertising companies, while the Ministry of Communications (the regulator in the area of Personal Data) has issued non-binding clarifications, where it concluded that personal mobile phone numbers and emails by themselves constitute Personal Data.

As of today, Russian authorities have started to accept that IP addresses, IMEI numbers and other device identifiers by themselves constitute Personal Data, which substantially extends the scope of Russian Personal Data laws.

b. Data Processing
Under the Personal Data Law, Personal Data processing has been defined very broadly as any action (operation) or collection of actions (operations) involving Personal Data, performed with or without computer equipment, including the collection, recording, systematization, accumulation, storage, verification (updating and amending), retrieval, use, transfer (dissemination, disclosure, access), depersonalization, blocking, deletion and destruction of Personal Data.

Russian data protection legislation regulates both manual and automated data processing. Neither the Personal Data Law nor the Labor Code distinguishes among various types of data processing, except that they prohibit Data Controllers and other parties from relying solely on automatically processed data in making legally binding decisions with respect to Personal Data Subjects, including employees, unless their consent is obtained.

c. Processing by Data Controllers
The Personal Data Law regulates general and specific issues related to the processing of Personal Data by state and municipal bodies, private legal
entities and individuals engaged in the processing of Personal Data ("Data Controllers"). The Personal Data Law determines the major principles of processing Personal Data. Personal Data may only be processed by Data Controllers with the consent of the Personal Data Subjects. However, consent is not required in a number of cases explicitly stated in the Personal Data Law. Data Controllers must ensure the confidentiality of Personal Data, unless otherwise provided for by the Personal Data Law (e.g., Data Controllers may only disclose Personal Data subject to an obligation of non-disclosure). The Labor Code also expressly determines the purposes for which, and the procedure pursuant to which, an employee’s Personal Data is to be processed by Data Controllers.

The Personal Data Law does not distinguish between Data Controllers and Data Processors, except that Data Processors are exempt from the duty to obtain Data Subjects’ consents for processing Personal Data.

d. Jurisdiction/Territoriality

The relevant Russian laws do not specify the territory covered by them. The laws apply to protect Personal Data and the rights of Personal Data Subjects irrespective of the location of the Data Controllers. The regulator currently opines that the Russian laws apply to any Personal Data processing that physically takes place on the Russian territory, or with respect to online processing if it involves or targets individuals located in Russia (the specific criteria for online processing is still under consideration). Existing law enforcement practice confirms the extraterritorial application of the Personal Data Law.

e. Sensitive Personal Data

Generally, the processing of certain categories of Personal Data, which include data on an individual’s political, religious, philosophic or other beliefs, race and national identity, state of health and private life ("Sensitive Personal Data"), is restricted. The Personal Data Law only allows the processing of Sensitive Personal Data in a limited number of cases explicitly stated in the Personal Data Law. For instance, processing Sensitive Personal Data is allowed if the Personal Data Subject has agreed to such processing in writing, if the Personal Data is processed by medical professionals for medical purposes, or if the processing is required for execution of justice, criminal prosecution and other cases specifically referred to in the Personal Data Law. Under the Russian Labor Code, Sensitive Personal Data may only be processed by an employer upon written consent of the employee and if such processing is required for the purposes of resolving a matter directly related to the employment relationship. An employer may not seek or process the Personal Data of an employee with respect to the employee’s affiliation with a non-governmental entity or trade union activities, except in cases expressly provided for by law.
There are special restrictions on the processing of data related to personal physiological and biological parameters by which an individual can be identified (“Biometric Personal Data”). Under the Personal Data Law, such Biometric Personal Data may only be processed by Data Controllers with the written consent of Personal Data Subjects. The consent of a Personal Data Subject is not required if the data is processed for the purposes of the execution of justice, a criminal investigation, and other cases explicitly stated in the applicable Russian legislation.

It is expressly prohibited to process data related to a person's criminal record other than by authorized state bodies for designated purposes.

f. Employee Personal Data

Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information) and non-Sensitive Personal Data. Sensitive Personal Data may be processed in the circumstances mentioned in Section 4(e) above and, in particular, if an employee wishes to observe a religious holiday not officially recognized in Russia as a public holiday. Employees’ non-Sensitive Personal Data provided in connection with employment may be processed by the employer. An employer should only obtain employees’ Personal Data from the employees, unless the employees give their consent in writing to obtain data about them from third parties.

Using global HR management IT tools should now be carefully scrutinized in light of the Russian Personal Data localization requirements, since many software vendors do not offer products that fully comply with these requirements “out of the box”.

5. Consent

a. General

The Data Subject’s consent is generally required prior to the collection, processing and disclosure of Personal Data, except in certain prescribed circumstances. Consent must always be voluntary, informed, explicit and unambiguous.

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

When the Data Subject gives consent, it is understood to only cover the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to.

There are generally no specific requirements for the form or manner in which consent must be obtained from Data Subjects. However, in some cases, consent must be in writing.

The Data Subject has the right to withdraw consent at any time.
b. Sensitive Data
Russian law recognizes Sensitive Data as a special category of Personal Data. It is subject to additional and special consent requirements. While Sensitive Data may only be collected and processed upon the written consent of the Data Subject, Sensitive Data may be processed without obtaining consent in certain prescribed circumstances.

Consent is not required for processing Sensitive Personal Data, including Biometric Personal Data, by medical professionals for medical purposes, if Personal Data is made publicly available by the Personal Data Subject, or if processing is required for the execution of justice, criminal prosecution, and other cases as stated in the Personal Data Law.

c. Minors
While consent from minors is not specifically addressed in any law, the general rule is that minors are considered incapable of giving consent. However, parents or legal guardians of minors are allowed to provide consent on behalf of the minor, and may even be allowed to obtain information about the minor from third parties without the need of the minor’s consent.

d. Employee Consent
In Russian law, there are doubts as to whether consent given in the context of an employment relationship can be considered valid given that the employee may feel forced to consent due to the subordinate nature of their relationship with their employer. However, we are not aware of any notable cases where an employee’s consent was successfully invalidated on these grounds.

The general rule is that employee consent is required to collect and process an employee’s Personal Data. However, there are instances when employee consent is not required, e.g., to carry out an employment contract or administer an employment relationship, or to fulfill a legitimate interest of the employer.

e. Online/Electronic Consent
As stated in Section 5(a), nothing in Russian law prohibits the use of electronic consent, except where written consent is expressly required. However, online/electronic consent must be given in a verifiable form, and the onus of proof that the consent has been given lies on the Data Controller.

6. Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about:

- the organization’s identity;
- the types of Personal Data being collected;
• the purposes for collecting Personal Data;
• its privacy practices (which must be given in a clear and transparent way);
• third parties to which the organization will disclose the Personal Data;
• the rights of the Data Subject;
• how the Personal Data is to be retained;
• where the Personal Data is to be transferred;
• where the Personal Data is to be stored;
• how to contact the privacy officer or the person accountable for the organization’s policies and practices;
• how to make an inquiry or a complaint;
• how to access and/or correct the Data Subject’s Personal Data;
• the duration of the proposed processing; and
• the means of transmitting the Personal Data.

7. Processing Rules
An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected. The organization must also delete/anonymize Personal Data once the stated purposes have been fulfilled and all legal obligations have been met.

8. Rights of Individuals
Data Subjects have the general right to: be informed by an organization of the Personal Data that the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data; and exercise the writ of habeas data.

9. Registration/Notification Requirements
Before a Data Controller commences processing Personal Data, it must file a notification of its intention to process Personal Data with the competent state authority responsible for Personal Data protection (currently Roskomnadzor). The notice may be submitted online (in which case it must be signed with a qualified advanced electronic signature). The notice may also be sent by
regular mail. The notification must contain the details of the Data Controller, categories of data and Data Subjects, time period of Data Processing, legal grounds, purpose and methods of the Data Processing, and security measures applied. A person responsible for Data Processing must be appointed by the Data Controller and notified to the competent authority. The information about the Data Controllers and the data processed by them must be publicly available.

There are certain exceptions from the notification obligation. For instance, no notification is necessary when only the names, patronymics and surnames are processed or when the processing of data is carried out solely for the purpose of executing a contract with the Data Subject.

10. Data Protection Officers
In Russia, organizations are required to appoint or designate a data privacy officer or other individual who will be accountable for the privacy practices of the organization. In addition, such data privacy officer or other individual must be located in Russia.

11. International Data Transfers
Organizations may transfer Personal Data outside of Russia, provided that the receiving jurisdiction provides a similar level of protection for Personal Data; the affected Data Subjects have been informed or have provided consent; and reasonable steps have been taken to safeguard the Personal Data being transferred. Furthermore, international data transfers will be considered valid, provided that appropriate data transfer agreements (i.e., Model Contractual Clauses) or other prescribed measures are put in place.

If a jurisdiction is not deemed to ensure adequate protection of Personal Data subject rights, transferring the Personal Data will only be possible subject to the written consent of the Data Subject or for the performance of a contract to which the Data Subject is a party.

12. Security Requirements
Organizations are required to take steps to: ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved in accordance with various Russian bylaws and regulations.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. If a data breach
occurs, the outsourcing organization may be held liable together with the third-party provider.

In some cases, outsourcing of Data Processing to third parties may require the consent of the Data Subjects.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority compliance orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, administrative or criminal proceedings, and the blocking of non-compliant websites, mobile apps or online services.

15. Data Security Breach
Depending on how the breach was discovered, the organization may be required to notify the data authority or the Data Subject.

16. Accountability
In Russia, organizations are required to: conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data; furnish the results of the privacy impact assessments to privacy regulators upon request; and furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-Blower hotline
There are no laws/rules that regulate whistle-blower hotlines in Russia. However, practical implementation of whistle-blower hotlines may face difficulties in light of the Personal Data localization requirements mentioned above.

18. E-Discovery
There are no laws/rules that regulate the implementation of an e-discovery system in Russia.

19. Anti-Spam Filtering
There are no laws/rules that regulate the implementation of an anti-spam filter solution in Russia.

20. Cookies
There are no laws/rules that directly regulate the use and deployment of cookies in Russia. However, the recent statements of the regulator give rise to an opinion that cookies and IP addresses qualify as Personal Data that cannot be lawfully collected and processed without the user’s consent.
21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject's failure to respond.
Saudi Arabia

George Sayen
Riyadh
Tel: +966 11 265 8900, Ext. 8911
george.sayen@bakermckenzie.com

Haifa Bahaian
Riyadh
Tel: +966 11 265 8900, Ext. 8968
haifa.bahaian@bakermckenzie.com
1. Recent Privacy Developments

There is a draft data privacy law which remains unpublished and has not entered into force as of 31 January 2018. The data privacy law consists of general provisions and aims to give legal and natural persons the right to view data retained by public governmental entities (with the exception of “confidential data”).

The draft law defines “data” as any written, recorded, copied or stored data, documents or statistics. It also provides a definition of “confidential data” which includes Personal Data that, if disclosed, could result in violation of the person’s privacy.

The draft law does not provide details on how governmental entities should protect confidential data – it only addresses the right to access non-confidential data and how such data should be stored by such entities.

2. Emerging Privacy Issues and Trends

a. Electronic Signatures

Electronic signatures are regulated under the Electronic Transactions Law, which provides that a Certification Service Provider (“CSP”), i.e., a person licensed to issue digital certificates or perform any other service or task related thereto and to electronic signatures in accordance with the law, shall maintain, along with his/her staff, the confidentiality of information obtained in the course of business, excluding information that certificate holders permit – in written or electronic form – to be published or disclosed, or as provided for by law.

Nonetheless, a certificate holder shall be responsible for the integrity and confidentiality of his/her own electronic signature system, and any use of such system shall be deemed to have originated from him/her. Any person relying on an electronic signature of another person shall exercise due diligence in verifying the authenticity of the signature, by using relevant electronic signature verification data in accordance with the procedures set forth by the law.

Staff of the Ministry of Communications and Information Technology, Communications and Information Technology Commission and the National Center for Digital Certification shall maintain the confidentiality of information relating to CSPs or clients thereof, obtained in the course of their work and may not disclose such information for any reason, except in cases provided for by law.

When the activities of a CSP cease to exist, the obligation of confidentiality continues as the law obligates the CSP to deliver all information and documentation in its possession to the Communications and Information
Global Privacy and Information Management Handbook
Saudi Arabia

Technology Commission, to be disposed of in accordance with the provisions and standards provided for in the Electronic Transactions Regulations.

b. Cyber Crime/Cyber Security

In 2007, Saudi Arabia issued the Anti-Cyber Crime Law to regulate cyber crimes taking place in Saudi Arabia. The law aims to enhance the security of information and to protect the confidentiality and privacy of Personal Data.

The law defines “data” as information, commands, messages, voices or images which are prepared or have been prepared for use in computers. This includes data that can be saved, processed, transmitted, or constructed by computers, such as numbers, letters, codes, etc. The law also defines “unauthorized access to Personal Data” as the deliberate, unauthorized access by any person to computers, websites, information systems, or computer networks.

The law provides a variety of sanctions and penalties for wrongfully accessing or disclosing Personal Data. The sanctions for violating Personal Data depend on the severity of the violation. Examples of some of the sanctions include:

- The act of spying on, intercepting or receiving data transmitted through an information network or a computer without legitimate authorization is punishable by imprisonment for a period not exceeding one year and a fine not exceeding SAR 500,000.

- The act of unlawfully accessing bank or credit data is punishable by imprisonment for a period not exceeding three years and a fine not exceeding SAR 2 million.

- The act of unlawfully accessing computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data is punishable by imprisonment for a period not exceeding four years and a fine not exceeding SAR 3 million.

The competent court may exempt an offender from such punishments if the offender informs the competent authority of the crime prior to its discovery and prior to the infliction of damage. If the culprit informs the competent authority after the occurrence of the crime, the exemption from punishment shall be granted if the information he or she provides eventually leads to the arrest of the other culprits and the seizure of the means used in committing the crime.

In October 2017, the Saudi Arabian government established a new authority for cyber security called the “National Cyber Security Center” to enhance the protection of networks, information technology systems and data in Saudi Arabia. The newly established center aims to protect the communications and information systems of Saudi Arabia’s government, as well as critical national infrastructure operators, against network penetration, by providing defense
systems, technology and guidance to maintain the confidentiality, integrity, processes and availability of such systems.

3. Law Applicable

There are no specific laws or regulations in Saudi Arabia that prescribe or control the collection, storage or transfer of Personal Data. However, there are certain rights of privacy under various laws which provide for privacy in certain aspects including, but not limited to, an individual’s financial and personal information, and the privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks, unless otherwise provided for by statute or royal decree.

While we are not aware of any legal regime that specifically controls data privacy, it should be noted that Saudi courts may use general notions of fairness to resolve any dispute related to matters of privacy and may rely on general principles of *Shariah* (Islamic Law).

The following is a list of laws and regulations which discuss certain rights of privacy in certain sectors in Saudi Arabia:

<table>
<thead>
<tr>
<th>Applicable Laws</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Laws</td>
<td>Links</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

4. Key Privacy Concepts

a. Personal Data

“Personal Data” is not defined in any laws or regulations in Saudi Arabia. Nonetheless, the privacy of Personal Data has been regulated in different areas under Saudi laws. The following are the laws and regulations addressing the privacy and protection measures of Personal Data:

**Shariah**

Under Shariah, there is no specific data protection regime. However, the wrongful disclosure of a person’s private information by a person to whom it has been entrusted for a specific purpose, may, in proper circumstances, create a cause of action for damages: for example, in a case where the information is of an extremely sensitive nature and potentially slanderous, or where its negligent disclosure or loss, including through inadequate data security measures, would cause direct damages to an individual.

As an example, an employer may be liable for disclosing information to the public that would damage an employee’s reputation. However, the collection and use of the information for legitimate employment purposes and retained in confidence would not ordinarily be actionable.
Law of Civil Affairs

This law provides that the contents of civil registers (including all Personal Data therein such as a person’s name, date of birth, ID number, and that person’s picture) are considered confidential; and it is prohibited to move such registers out of the Civil Affairs Departments and offices in any case, except if required otherwise by a judicial authority or an official investigation authority.

Telecommunications Regulations

The Telecommunications Regulations generally prohibit the disclosure of a customer’s personal information without his/her consent. In particular, Article 58 requires a service provider to operate its telecommunications facilities and telecommunications network with due regard for the privacy of its users, except as permitted or required by law, or with the consent of the person to whom the personal information relates. A service provider shall not collect, use, maintain or disclose user information or user communications for any purpose.

Anti-Cyber Crime Law

The Anti-Cyber Crime Law protects the confidentiality and privacy of personal information (for further information, see section 2).

Regulations for Consumer Credit

Personal Data obtained from consumers, guarantors or any other person in connection with the execution and management of agreements must be kept confidential. Such consumer data may be processed only for the purpose of assessing the financial situation of the borrowers or guarantors and their ability to repay the agreed credit.

The Saudi Credit Bureau operates a central database for the purpose of registering and maintaining credit information of consumers and guarantors. Personal Data received may be processed only for the purpose of assessing the financial situation of the consumer and the guarantor and their ability to repay.

Banking Consumer Protection Principles

These Principles apply to the activities of banks operating by way of a license and under the supervision of the Saudi Arabian Monetary Agency (“SAMA”), and who are dealing with persons who are, or may become, consumers. It also applies to the activities of any third party engaged by the banks for outsourced activity.

The sixth principle is the Principle of Protection of Privacy, which means that consumers’ financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should
define the purposes for which data may be collected, processed, held, used and disclosed (especially to third parties).

Under the Principles, banks are responsible for protecting consumer data and maintaining the confidentiality of the data, including when it is held by a third party. Banks are also required to: (i) provide a safe and confidential environment in all of their delivery channels to ensure the confidentiality and privacy of consumer data; (ii) have sufficient procedures, system controls and checks and employee awareness to protect consumer information; and (iii) identify and resolve any causes of information security breaches. In addition, banks must ensure that all employees sign a customer information confidentiality form, and make sure that the financial and/or personal information of consumers can be accessed and used by authorized employees only. These confidentiality obligations apply to such employees both during and after employment.

**Insurance Market Code of Conduct Regulation**

Insurance companies must, at all times, ensure that customer Personal Data is protected. This means that the data must be obtained and used only for specified and lawful purposes, kept by the insurance company in Saudi Arabia, provided to the customer upon his/her written request and not disclosed to any third party without the prior authorization of SAMA. When dealing with third parties, insurance companies must set up data confidentiality agreements before initiating a business relationship.

The regulations also protect information collected through a website, as insurance companies must ensure the confidentiality of all information collected through their websites and not disclose such information to any party without the written approval of SAMA. Furthermore, it is the responsibility of the insurance company to establish appropriate procedures and controls to secure the confidentiality of information.

**Insurance Intermediaries Regulation**

Intermediaries shall ensure that clients' data and confidential documents are stored safely with restricted access. Intermediaries are also required to treat all data and information acquired about the insurance company and clients with the utmost confidentiality, and to take appropriate measures to maintain the secrecy of confidential documents in their possession. This means that the data must be obtained and used only for specified and lawful purposes, kept secure and up to date, and not disclosed to any third party without prior authorization from SAMA.
b. **Processing by Data Controllers**

Since there are no laws in Saudi Arabia that regulate or control data privacy, the concept of Data Controllers does not exist yet and is not defined in any laws or regulations in Saudi Arabia.

5. **Consent**

a. **General**

Under the Electronic Transactions Law, it is a criminal offense to use an applicant’s information for purposes other than for certification without the applicant’s consent in written or electronic form. CSPs can only obtain an applicant’s personal information, directly or indirectly, with that applicant’s written consent. However, the law does not outline the required content of the consent. It is also unclear whether electronic consent is sufficient for the purpose of collecting data. The law is silent on whether or not it applies to implied or inferred consent or consent by minors.

Also, as mentioned in section 4(a) above, the Telecommunications Regulations generally prohibit the disclosure of a customer’s personal information without his/her consent, except as permitted or required by law.

6. **Information/Notice Requirements**

There are no specific laws or regulations that we are aware of that regulate information/notice requirements in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

7. **Processing Rules**

We are not aware of any specific laws or regulations that regulate processing rules in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

8. **Rights of Individuals**

We are not aware of any specific laws or regulations that regulate rights of individuals in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

9. **Registration/Notification Requirements**

We are not aware of any specific laws or regulations that regulate registration/notification requirements in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.
10. Data Protection Officers

We are not aware of any specific laws or regulations that regulate data protection officers in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

11. International Data Transfers

There are no specific laws or regulations that regulate international data transfers in Saudi Arabia. We note here that recently the telecom regulator (the Communications and Information Technology Commission) has issued a draft regulation for cloud computing (still not enacted yet) and which includes limitations and controls applicable to the transfer, storage and processing of user content outside Saudi Arabia and prohibits the disclosure of user data or user content to a third party for any purpose other than the provision of the cloud services, unless permitted by the laws of Saudi Arabia or with the user’s consent. We can provide more information on the data protection under cloud computing law once it is enacted in its final version.

12. Security Requirements

We are not aware of any specific laws or regulations that regulate security requirements in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

13. Special Rules for Outsourcing of Data Processing to Third Parties

We are not aware of any specific laws or regulations that regulate outsourcing of data processing to third parties in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

14. Enforcement and Sanctions

The Banking Control Law imposes penalties on bank employees in cases of violating the confidentiality of information possessed by such employees while performing their duties. Violators shall be liable to imprisonment for a term not exceeding two years and/or a fine not exceeding SAR 20,000.

The Anti-Cyber Crime Law imposes penalties and fines that vary from SAR 500,000 to SAR 3 million and imprisonment for a term of one to five years (please refer to section 2).

The Electronic Transactions Law imposes fines not exceeding SAR 5 million and/or imprisonment for a period not exceeding five years.

In 2007, a spokesman for the Communications and Information Technology Commission has issued a stern warning to companies that send unsolicited
spam messages to customers, stating that such companies could face fines of up to SAR 5 million or even the cancellation of their business license.

The Telecommunications Law does not specify a penalty for violations of privacy, but it has set up a violations committee which has the jurisdiction to hear and decide on all matters relating to such violations. No other sanctions or penalties are discussed in the relevant laws.

15. Data Security Breach
We are not aware of any specific laws or regulations that regulate data security breaches in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

16. Accountability
We are not aware of any specific laws or regulations that regulate accountability in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

17. Whistle-Blower Hotline
We are not aware of any specific laws or regulations that regulate whistle-blower hotlines in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

18. E-Discovery
We are not aware of any specific laws or regulations that regulate e-discovery in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.

19. Anti-Spam Filtering

a. Definition of Spam under Saudi Law
The Regulation for Reduction of Spam issued pursuant to the Communications and Information Technology Commission resolution number 259/1431 dated 28 March 2010 defines “spam” as any electronic message transmitted without the prior consent of the recipient through various communication modes including, but not limited to, emails, SMS, MMS, fax and Bluetooth.

b. Control Measures
The Regulation for Reduction of Spam provides a number of rules to control electronic message transmissions. The Regulation prohibits any person from sending or causing to send electronic messages, unless the recipient has given a prior consent to receive such messages or there exists a prior commercial or business relationship between the sender and the recipient. Also, the electronic messages must include the name and address of the
sender and the subject of the message in order to enable the recipient to send a request to cancel the subscription if they no longer want to receive such messages. Once a request has been sent, the sender is prohibited from sending any messages after 48 hours of such request.

It should be noted that the Regulation specifically prohibits sending messages to electronic addresses obtained by automatic systems that use methods of combining names, letters, numbers, punctuation marks or symbols and prohibits the use of any computer software used for searching the internet for gathering email addresses.

c. Duties and Responsibilities of Service Providers

Certain duties and responsibilities are imposed on licensed internet service providers and mobile service providers, that such providers shall, on a continuous basis, take effective measures to make their subscribers aware of these controls, the importance of the compliance therewith, and the consequences of the violation thereof.

d. Applicability of Controls

The controls are applicable to all electronic messages originated from inside Saudi Arabia. International conventions shall apply on messages originated from outside Saudi Arabia.

Any person who is exposed to spam may file a complaint within 30 days from the date of receiving the spam.

20. Cookies

We are not aware of any specific laws or regulations that regulate cookies in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available. Also, given the broad language included in the cyber crime regulations regarding intrusion, there is a risk that the use of cookies be problematic in Saudi Arabia.

21. Direct Marketing

We are not aware of any specific laws or regulations that regulate direct marketing in Saudi Arabia. It should be noted that the Saudi regulatory authorities often issue circulars and decisions that are not publicly available.
Singapore

Ken Chia
Singapore
Tel: +65 6434 2558
ken.chia@bakermckenzie.com

Anne Petterd
Singapore
Tel: +65 64342573
anne.petterd@bakermckenzie.com

Ren Jun Lim
Singapore
Tel: +65 64342721
ren.jun.lim@bakermckenzie.com

Daryl Seetoh
Singapore
Tel: +65 64342257
daryl.seetoh@bakermckenzie.com
1. Recent Privacy Developments

**Personal Data Protection Act**

The Personal Data Protection Act (Act 26 of 2012) ("PDPA") was passed by the Singapore Parliament on 15 October 2012. The PDPA establishes a baseline data protection framework that applies to all organizations in the private sector. The PDPA also seeks to establish a national Do Not Call ("DNC") registry, which is intended to provide individuals with a simple and efficient way to opt out of receiving certain unsolicited marketing messages.

The requirements associated with the implementation of the DNC registry came into force on 2 January 2014, while the substantive data protection obligations came into force on 2 July 2014.

**Public consultation for proposed amendments to the PDPA**

On 27 July 2017, the Personal Data Protection Commission ("PDPC"), which is tasked with the administration and enforcement of the PDPA, launched the first public consultation on the PDPA, with the objective of maintaining a robust data protection regime relevant to current developments, while continuing to allow businesses to leverage on information sharing to innovate. The public consultation addresses the following two areas: (i) an enhanced framework for the collection, use and disclosure of Personal Data; and (ii) proposed mandatory data breach notification. An aim of the consultation paper is to allow for a more progressive approach to collecting and using Personal Data, and to provide greater transparency when data breaches occur.

In relation to the first heading, in view of the potential impracticality of seeking consent at every instance of data collection or use, given the rise of the digital economy and the sheer volume of data transactions, the PDPC proposes to provide for the collection, use or disclosure of Personal Data without consent where: (i) it is necessary for a legal or business purpose, and it is not desirable or appropriate to obtain consent and the benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual; or (ii) it is impractical for the organization to obtain consent and the collection, use or disclosure of Personal Data is not expected to have any adverse impact on the individuals. In the latter case, organizations will have to provide appropriate notification of the purpose of the collection, use or disclosure of the Personal Data, and where it is feasible for the organization to allow individuals to opt out of the collection, use or disclosure, information about how individuals may opt out.

**Proposed changes to the Computer Misuse and Cybersecurity Act**

With effect from 1 June 2017, the Computer Misuse and Cybersecurity Act ("CMCA") was amended to address the increasingly borderless nature of
cybercrime and strengthen Singapore’s cybersecurity enforcement regime. Salient amendments include criminalizing acts which enable cybercrime and extraterritorial acts which cause significant harm in Singapore, as well as enhanced penalties for offenses. In addition, and of particular relevance to data privacy, the reach of the CMCA has been extended by criminalizing acts which are enabled by cybersecurity attacks. In this regard, it is an offense to use Personal Data obtained via an act in breach of the CMCA. For example, it is an offense to deal in Personal Data obtained by hacking, even if the act of hacking was committed by another.

**Singapore’s Notice of Intent to Participate in the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems**

Singapore has submitted its Notice of Intent to participate in APEC’s Cross-Border Privacy Rules (“CBPR”) and Privacy Recognition for Processors (“PRP”) Systems, with a view to strengthening confidence among businesses when sharing their data across borders. CBPR and PRP provide validation of businesses’ data protection practices which will be recognized by participating jurisdictions. It is envisioned that the proposed Trustmark certification (as described in further detail below) will be harmonized with these data protection standards in order to facilitate cross-border flow of data, which will potentially lead to lower costs for businesses.

**Other developments**

There has been recent emphasis by the PDPC on the importance of implementing and complying with data protection policies, including the designation of data protection officers (“DPOs”). In this regard, PDPC has sent letters to various organizations advising them to voluntarily register their DPO.

On 27 July 2017, the Minister for Communications and Information (the “Minister”) announced that the PDPC is “prepared to work with companies who adopt accountability practices to create regulatory sandboxes” with a view to allowing the PDPC to understand how the proposed enhanced framework for the collection, use and disclosure of Personal Data is to work in practice, prior to the PDPA being amended.

At the same time, the Minister announced the intention to launch a Data Protection Trustmark certification scheme by the end of 2018. This scheme will allow businesses to obtain a certification which serves as a visible indicator that they adopt sound practices and keep their processes updated regularly. The aim of the scheme is to facilitate the cross-border information exchange of locally based businesses, while attracting more businesses to conduct data innovation activities in Singapore.
On 2 July 2014, the Personal Data Protection Regulations ("PDPR") came into force. The PDPR expands on, among other things, the PDPA’s Access and Correction Obligation and Transfer Obligation.

In particular, the PDPR requires organizations to respond to each access request as accurately and completely as necessary and reasonably possible within 30 days of such request being made. However, if an organization is unable to comply with this requirement, it must (within the 30-day period) inform the applicant in writing of the time by which it will respond to the request.

Further, as discussed below, the PDPR requires an organization transferring Personal Data (please refer to definition in Section 4 below) outside Singapore to take appropriate steps to ascertain whether, and to ensure that, the recipient of the Personal Data in that country or territory outside Singapore is bound by legally enforceable obligations to provide to the transferred Personal Data a standard of protection that is at least comparable to the protection under the PDPA.

Advisory Guidelines

The PDPC has the power to issue advisory guidelines, which provide an indication as to how the PDPC will interpret the PDPA. However, the advisory guidelines are not legally binding and do not limit or restrict the PDPC’s administration and enforcement of the PDPA.


The recent amendments to the Key Concepts Guidelines provide further clarity on what constitutes Personal Data, including the types of data which, on its own, constitutes Personal Data. The recent amendments to the Selected Topics Guidelines provide further clarity for organizations using and disclosing anonymized data, including further information on the considerations for assessing and managing the risks of re-identification from anonymized data. The recent amendments to the Do Not Call Guidelines provide further clarification on responding to requests for information through a third party, sending specified messages to Singapore telephone numbers obtained through third-party sources, and the definition of “ongoing relationship”.

On 8 August 2017, the PDPC published the Advisory Guidelines on Application of PDPA to Election Activities, which highlight how key provisions
of the PDPA apply to political parties and election candidates when carrying out election activities.

As at 29 September 2017, the following Advisory Guidelines have been issued by the PDPC:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act, which elaborate on and provide illustrations for the key obligations in the PDPA and the interpretation of key terms in the PDPA (published on 23 September 2013).

- Advisory Guidelines on the Personal Data Protection Act for Selected Topics, which elaborate on how the PDPA applies to particular issues and domains (published on 24 September 2013).

- Advisory Guidelines on the Do Not Call Provisions, which provide an explanation of how the DNC provisions, as set out in the PDPA, may apply in different scenarios, and allow organizations and individuals to better understand their requirements (published on 26 December 2013).

- Advisory Guidelines on Requiring Consent for Marketing Purposes, which provide guidance on whether organizations must obtain consent to send marketing materials to individuals or to use the individual’s Personal Data for other marketing activities (published on 8 May 2015).


- Advisory Guidelines on Application of PDPA to Election Activities which highlight how key provisions of the PDPA apply to political parties and election candidates when carrying out election activities (published on 8 August 2017).


- Industry-led Specific Guidelines and other guides on topics such as Securing Personal Data in Electronic Medium and the Guide on Data Protection Clauses for Agreements relating to the Processing of Personal Data. On 27 July 2017, the PDPC published the Guide to Data Sharing, which provides information to help organizations identify the appropriate approaches for sharing Personal Data within and between organizations.

**DNC registry**

Organizations must check the DNC registry before sending marketing messages to consumers through their Singapore telephone numbers.
The PDPA prohibits organizations from sending marketing messages to telephone numbers listed on the relevant register (there are three: No Voice Call, No Text Message and No Fax Message), unless they have obtained “clear and unambiguous” consent from the relevant individual. Such consent should also be evidenced in writing or such other form suitable for subsequent reference, and should not be imposed as a condition for the provisions of goods or services. In practice, this is typically achieved by providing customers with a check box whereby they can opt in to receiving marketing messages on their telephone numbers on a voluntary basis.

Organizations can set up an account at www.dnc.gov.sg and begin purchasing credits to be used in conducting checks on the registry in preparation for the effective date.

The PDPC has issued an exemption allowing organizations with an on-going relationship with an individual to send marketing messages related to the subject of the on-going relationship to the individual via text or fax (but not voice calls), subject to the satisfaction of certain conditions, including providing a means for the individual to opt out of receiving further marketing messages under the exemption.

2. Emerging Privacy Issues and Trends

Data security breaches

While there is no mandatory requirement regarding security breach notifications under the PDPA, the PDPC has taken action against organizations that are found to have taken inadequate security measures to protect Personal Data in their possession or under their control from unauthorized disclosure. For example, the PDPC imposed financial penalties and issued directions to companies for failing to make reasonable security arrangements to prevent unauthorized disclosure or access of Personal Data, including by failing to implement proper and adequate measures to secure their website and/or server. The PDPC has also issued a warning to other companies for failing to make such reasonable security arrangements to prevent unauthorized disclosure of or access to Personal Data where mitigating factors were present.

The PDPC has also proposed in its public consultation for proposed amendments to the PDPA that organizations will have to mandatorily notify the PDPC within 72 hours where a data breach poses any risk of impact or harm to the affected individuals, or where the scale of the data breach is significant (this is currently proposed to be where the Personal Data of more than 500 individuals is affected, even if it does not pose any risk of impact or harm to the affected individuals). Individuals will also have to be notified as soon as practicable where there is risk of harm to the affected individuals.
because the data breach affects Personal Data such as NRIC numbers, health, financial information and passwords.

**Cybersecurity**

Given the recent uptake in cybersecurity attacks, a new, standalone Cybersecurity Act will be tabled in Parliament in 2018. The draft Cybersecurity Bill was issued for public consultation by the Ministry of Communications and Information and the Cyber Security Agency (“CSA”) of Singapore from 10 July 2017 to 24 August 2017. The draft bill provides that a Commissioner of Cybersecurity be appointed, who may designate specific computers or computer systems as critical information infrastructure (“CII”), and compels operators of CII to take proactive steps to secure such CII and report incidents of cybersecurity breaches, including by complying with a new licensing regime. The new Act will empower the CSA to manage cyber incidents and raise the standards of cybersecurity providers. CII operators (and potentially other businesses that deal with them) will need to establish additional policies and procedures (if they have not already done so) to deal with cyber incidents, and comply with new reporting obligations.

**Interface between the PDPA and social media**

It might be said that there is an inherent tension between data protection and interactions on social network platforms, which rely on the sharing of information, including Personal Data, to engage users. While the PDPA contains a number of broad exemptions that may be applicable in this context, including exemptions for the collection, use and disclosure of publicly available Personal Data, we foresee that data protection issues may nevertheless arise. For example, it is questionable whether a professional blogger who has been subjected to insulting or derogatory remarks on social media could collect and post personal information regarding the individuals who made such wanton postings without contravening the PDPA.

There was also a recent case in which the operator of an online forum was forced to disclose the identity of an individual who had allegedly made defamatory remarks under a pseudonym. In the absence of clear safeguards in the relevant terms of use, it may not be clear how the operator of a social networking platform should react if such a request were filed directly with the operator, particularly if the transgression complained of does not amount to an offense or is committed overseas.

In a 2017 enforcement decision by the PDPA it was stated that any act or conduct engaged in by a person in the course of his/her employment shall be treated as done or engaged in by his/her employer as well as by him/her, whether or not the employer had knowledge of or approved of it.
**Do Not Call registry**

The DNC registry rules came into force in January 2014. As at February 2016, around 9,700 valid public complaints had been made. Between January 2015 and March 2017, 6,970 complaints were lodged with the PDPC, including complaints with regard to the DNC registry. The PDPC has also reported on two decisions since the inception of the DNC registry rules. In the first case, a home tuition agency and its director were fined SGD 39,000 each for sending marketing messages to telephone numbers registered with the DNC registry. In the second case, a property agent was charged with 27 counts of contravening the obligation to check the DNC registry before sending telemarketing messages to Singapore telephone numbers.

**Data Protection Enforcement**

As of 14 August 2017, the PDPC has taken enforcement actions against 37 organizations in Singapore for breaches of the PDPA. The PDPC has issued 23 organizations with directions (18 of which included financial penalties), while 15 others were issued warnings. The largest financial penalty to date (SGD 50,000) was imposed on a company for failing to put in place sufficient security measures to protect the Personal Data of 317,000 members, particularly because it had inadequate data protection policies and had failed to appoint a DPO.

Meanwhile, in recent cases involving the unauthorized disclosure of a customer’s Personal Data to a single other customer, and the unauthorized disclosure of Personal Data of passengers contained in a flight manifest where there were no complaints of any actual unauthorized access, the PDPC issued directions to the respective organizations to enhance their Personal Data protection policies.

Further, a recent case involved the failure by a data intermediary to implement reasonable security measures when making modifications to a log-in system, including by failing to adhere to its standard operating procedures and those of the organization on whose behalf it was processing the data, which involved reviewing, testing and verifying modifications before their application. In this case, Sensitive Personal Data of one customer was disclosed without authorization, and the Personal Data of 2.78 million users was unlawfully modified, resulting in the PDPC imposing a financial penalty of SGD 10,000 on the organization.

**3. Law Applicable**

Prior to the introduction of the PDPA, Singapore’s approach towards data protection was sectoral in nature. In the private sector, only organizations in certain industries (e.g., banking and medical) were subject to some form of mandatory regulation. Even then, the regulation was generally limited to more sensitive data, such as information on bank accounts and health records.
The PDPA does not have any impact on mandatory requirements imposed under sectoral regulations. Organizations subject to such sectoral regulations are expected to comply with the baseline requirements set out in the PDPA, as well as additional requirements under such sectoral regulations.

The PDPA does not affect the rights of organizations to collect, use or disclose Personal Data to the extent that such collection, use or disclosure is authorized under other written laws.

4. Key Privacy Concepts

a. Personal Data
The definition of “Personal Data” in the PDPA covers information, whether true or not, about an individual who can be identified from that piece of data or from other data to which the organization has or is likely to have access. Business contact information falls outside the scope of the PDPA. Unlike the approach adopted in certain jurisdictions, limited protection is afforded to Personal Data of deceased individuals, in that obligations relating to the safeguarding and disclosure of such Personal Data continue to apply for a period of 10 years.

The PDPA definition also covers all forms of Personal Data, whether electronic or non-electronic.

It is recognized that in line with the pro-consumer definition of Personal Data, it is not feasible for the PDPA to prescribe a definitive list of personal information that should be protected. The scope of the definition would depend on the context, as well as technological developments which may bring about new forms of Personal Data that are not currently envisaged.

b. Data Processing
The data protection rules in the PDPA apply to the collection, use and disclosure of Personal Data.

c. Processing by Data Controllers and Data Intermediaries
Under the PDPA, a data intermediary processing Personal Data on behalf of and for the purposes of another organization pursuant to a contract, which is evidenced or made in writing, has limited obligations in respect of the Personal Data. The data intermediary is only required to take reasonable security measures to safeguard the Personal Data and to delete or anonymize the Personal Data when it is no longer required for legal or business purposes. An organization, on the other hand is held responsible for the processing of Personal Data in its custody or under its control. All private sector “organizations” in Singapore fall within the ambit of the PDPA. This covers natural persons, trusts and other entities, corporate or unincorporated. However, acts of a natural person acting in a personal or domestic capacity are excluded.
The PDPA does not apply to public agencies in Singapore.

d. Jurisdiction/Territoriality
The PDPA does not state that it applies only to Personal Data or organizations in Singapore. An “organization” is defined as including any individual, company, association, or body of persons, corporate or unincorporated, whether or not: (i) formed or recognized under the law of Singapore; or (ii) resident, or having an office or a place of business, in Singapore. In general, every organization (unless exempted or excluded) is required to comply with the PDPA in respect of activities relating to the collection, use and disclosure of Personal Data in Singapore. Hence, the PDPA arguably has extraterritorial effect and foreign companies which engage in data collection activities in Singapore would still be required to comply with the PDPA.

e. Sensitive Personal Data
The PDPA is intended to establish the minimum or baseline standards applicable to the processing of Personal Data by private sector organizations, and will be supplemented by other legislative and regulatory regimes, such as the existing sectoral requirements mentioned in Section 3 above.

That being the case, the PDPA does not provide for a separate regime governing Sensitive Personal Data. If more stringent requirements are required to be imposed in respect to the processing of such Sensitive Personal Data, such concerns are likely to be addressed in sector-specific laws that apply concurrently.

f. Employee Personal Data
The PDPA covers Personal Data collected from employees of the organization. The rules which apply to the collection of such Employee Personal Data may be slightly different (see Section 5(d) below).

5. Consent

a. General
The regime prescribed by the PDPA is based on consent, purpose and reasonableness. An organization would only be allowed to collect, use or disclose Personal Data with consent from the individual concerned. The consent obtained may be express or implied, depending on the circumstances. For example, if an individual voluntarily provides his/her Personal Data to a clinic when registering or making an appointment for medical treatment, he/she may be deemed to have given consent to the collection and use of such Personal Data by the clinic for that purpose.

The organization is also required to ensure that the collection, use or disclosure of Personal Data is for a reasonable purpose which the
organization has disclosed to the individual before the collection of the Personal Data. The reasonableness of the purpose would be measured against what a reasonable person would consider appropriate in the circumstances.

The organization may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of Personal Data beyond what is necessary to provide that product or service. Consent obtained through deception or by providing misleading or incomplete information would not be deemed to be validly given.

The individual should be allowed to withdraw his/her consent at any time. Where the organization receives notice from the individual pertaining to the withdrawal of consent, the organization may inform the individual of the likely consequences of such withdrawal, but cannot prohibit such withdrawal.

b. Sensitive Data
The PDPA is intended to prescribe the baseline requirements for the processing of Personal Data by private sector organizations and does not recognize a special category of Personal Data as Sensitive Personal Data.

c. Minors
The PDPC has clarified in its Selected Topics Guidelines that it shall adopt the “rule of thumb” that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent to the collection, use and/or disclosure of his/her Personal Data by an organization on his/her own behalf. However, if an organization has reason to believe that the minor would not, the organization should obtain consent from the minor’s parent or guardian.

Similarly, consent may be obtained from a guardian or trustee appointed for the individual, an attorney appointed under a power of attorney, or any person with written authorization from the individual to act on his or her behalf.

d. Employee Consent
The PDPA provides for certain exemptions that apply to the collection, use and disclosure of Personal Data of employees. There is a general exemption in respect of the reasonable collection, use and disclosure of Personal Data by an employer for the purposes of managing or terminating an employment relationship between the organization and an employee.

In order to be able to rely on this exemption, the organization needs to notify the employee that it is collecting Personal Data for such purposes and provide the contact information of an officer who can answer queries regarding the organization’s data protection policies upon request, but is not required to seek consent from the employees.
e. **Online/Electronic Consent**

The PDPA does not specifically address the issue of online/electronic consent, although the Key Concepts Guidelines and the PDPC’s publication “A Guide to Notification” provide some examples where consent may be obtained online or electronically.

Further, we note that it is likely that any consent provided online or electronically would be considered validly given under the Electronic Transactions Act.

6. **Notice Requirements**

An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) its privacy practices (which must be given in a clear and transparent way); (v) third parties to which the organization will disclose the Personal Data; (vi) how to contact the privacy officer or the person accountable for the organization’s policies and practices; (vii) how to make an inquiry or file a complaint; and (viii) how to access and/or correct the Data Subject’s Personal Data.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purposes for which the Personal Data was collected, and delete/anonymize the Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**

The PDPA provides Data Subjects the general right to be informed by an organization of the Personal Data the organization holds about the Data Subject and to access and correct Personal Data held by organizations.

Organizations are allowed to charge a reasonable fee to defray any costs that they would incur in allowing individuals to have such rights of access and correction.

9. **Registration/Notification Requirements**

The PDPC undertakes education and awareness efforts and is responsible for the enforcement of the PDPA. However, in order to keep compliance costs down for organizations, particularly small and medium-sized enterprises, the PDPC has adopted a complaint-based approach in exercising its oversight duties, and will only investigate cases of non-compliance where a complaint is filed. Organizations will not be required to submit reports to, or be audited by, the PDPC on a regular basis.
In keeping with the foregoing, the PDPA does not impose any mandatory requirements relating to registration with or notification to the PDPC.

10. Data Protection Officers

Under the PDPA, organizations are required to designate one or more employees to be responsible for ensuring their compliance with the law. Notwithstanding the fact that the designated employee(s) would be accountable for the organization’s compliance with the PDPA, the designation of such employee(s) does not relieve the organization of its statutory obligations.

The business contact information of the designated employee(s) should be made known to individuals from whom Personal Data is collected, and to consumers generally. Such designated employee(s) should be able to address queries regarding the organization’s data policies on the collection, use and disclosure of Personal Data and the organization’s compliance with the law.

11. International Data Transfers

The PDPA provides that an organization should not transfer Personal Data outside of Singapore unless it complies with requirements prescribed under the Act to ensure that Personal Data would be afforded a comparable standard of protection. Under the PDPR, a transferring organization is required to take appropriate steps to ascertain whether, and to ensure that, the recipient of the Personal Data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations to provide to the transferred Personal Data a standard of protection that is at least comparable to the protection under the PDPA.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use, implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect the Personal Data. The organization may be liable together with the third-party provider in case of breach by the latter.
14. Enforcement and Sanctions

Failure to comply with the PDPA can result in complaints and investigations/audits by the PDPC. The PDPC has broad powers to give directions to the infringing organization, including ordering the payment of a financial penalty of up to SGD 1 million. Individuals who suffer loss or damage as a result of contravention of the data protection obligations in the PDPA have private rights of action and can commence civil proceedings against the organization. A contravention of the DNC provision in the PDPA is criminal in nature and may lead to fines of up to SGD 10,000 per offense.

15. Data Security Breach

While organizations that are involved in a data breach situation are not required by the PDPA to report the breach, such organizations shall assist authorities with any investigation relating to the breach, and comply with data authority orders and court orders in addition to the PDPC Guidelines on Data Security Breaches.

16. Accountability

There is currently no requirement for organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Singapore provided they are in compliance with local laws.

18. E-Discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is involved. However, it may be possible for the organization to argue that the implementation of the e-discovery system falls within the scope of the employment exemption mentioned in Section 5(d) above, in which case specific consent is not required, although the organization should notify the employees regarding the implementation of the system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

Similarly, when implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace in order to rely on the employment exemption mentioned in Section 5(d) above.
20. Cookies

The Selected Topics Guidelines has clarified that the PDPA applies to the collection, use or disclosure of Personal Data using cookies. In particular, consent is generally required for cookies that collect Personal Data. However, for internet activities that the user has clearly requested, there may not be a need to seek consent for the use of cookies to collect, use and disclose Personal Data where the individual is aware of the purposes of such collection, use and disclosure and voluntarily provided his/her Personal Data for such purposes.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject (e.g., direct marketing is made to a Singapore telephone number subject to the Do Not Call requirements discussed in Section 1) is required to obtain the Data Subject’s prior express (opt-in) consent, which cannot be inferred from a Data Subject’s failure to respond. The organization must obtain consent for a specific activity, as bundled consent may not be considered clear and unambiguous consent.
South Africa

Darryl Bernstein
Johannesburg
Tel: +27 (0) 11 911 4367
darryl.bernstein@bakermckenzie.com

Deepa Ramjee
Johannesburg
Tel: +27 (0) 11 911 4368
deepa.ramjee@bakermckenzie.com
1. Recent Privacy Developments

Enactment of Data Protection and Privacy Legislation

While South African law recognizes a general right to privacy in relation to a person’s information, there is currently nothing in South African law which expressly regulates the processing of personal information.

On 26 November 2013, the Protection of Personal Information Act, 2013 (“Act”) was enacted. The Act seeks to bring South Africa in line with international data protection laws by regulating the processing of the information of natural and juristic persons and placing more onerous obligations on “responsible parties” that process such information.

Only certain sections of the Act have commenced, namely Section 1 of Part A of Chapter 5 and Sections 112 and 113. These sections are specific to the establishment of the Information Regulator and its authority to draft and put forward regulations under the Act. In September 2017, the Information Regulator published draft regulations for public comment. The Information Regulator has also indicated its intention to table the regulations in the South African Parliament before the end of 2017.

The Act sets out the essential parameters for the lawful processing of personal information, including:

- eight “core-information-protection principles”;
- a number of substantive issues concerning, inter alia, the processing, collecting, transferring and maintaining of personal information;
- exemptions from the information protection principles;
- the rights of Data Subjects regarding unsolicited electronic communications and automated decision making;
- the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of the Act and the Promotion of Access to Information Act, 2000;
- the regulation of trans-border information flows; and
- enforcement mechanisms.

The Act introduces terminology and concepts which are, to a certain extent, novel to South African law, the broad formulation of which is likely to have significant implications in respect of both the citizens of South Africa whose information is processed by companies and public bodies, and the companies and public bodies doing the actual processing (whether this is in South Africa or not).
The Act will not apply to the processing of information:

- in the course of a purely personal or household activity;
- that has been “de-identified” (i.e., deleted to the extent that it cannot be retrieved);
- by or on behalf of the State, relating to national security, investigation of offenses, and the like;
- for exclusively journalistic purposes by responsible parties who are subject to a code of conduct by virtue of office;
- by cabinet, provincial executive councils and municipal councils; and
- relating to the judicial conduct of a court.

We note the following salient principles arising from the Act:

- Personal information may only be processed in a fair and lawful manner that is transparent to the individual, and requires an individual’s explicit consent.
- Responsible parties processing information must ensure that personal information is only processed for specific, explicitly defined and legitimate reasons relating to the functions or activities of the organization, and the organization must take steps to make affected Data Subjects aware of the purposes for which the personal information will be processed. Personal information may only be kept for as long as it is required to fulfil the purpose for which it was collected.
- A responsible party is required to:
  - appoint an Information Officer and Deputy Information Officer to ensure compliance with the conditions set out in the Act and deal with complaints from Data Subjects who seek to enforce the Act;
  - maintain documentation of all processing; and
  - secure the integrity and confidentiality of personal information in its possession or under its control and ensure that it is appropriately safeguarded against loss, destruction or unlawful access.

2. Emerging Privacy Issues and Trends

a. The Act

The enactment of the Act itself, largely based on similar US and UK data protection legislation, is the most significant development in the South African privacy landscape. The timeline for the commencement of the entire Act is
unclear. Once fully operative, responsible parties will have one year to ensure legal compliance.

Given the limited transitional period provided for compliance coupled with potentially severe penalties, clients have already commenced implementing initiatives in an effort to comply with the prescriptive principles under the Act. The focus of many compliance programs has been on the overlap between the Act and other laws, since a law which gives the Data Subject greater protection will prevail over the Act. Implementation of the Act and the enforcement issues which will no doubt flow from it will continue to be a hot topic moving forward.

b. Electronic Signatures
In South Africa, our Supreme Court of Appeal has recently handed down an award in relation to amendments to an agreement which are required to be in writing and signed by the parties. An agreement, which provided for consensual cancellation to be recorded in writing and signed by the parties to be valid, was terminated by an exchange of emails. Although not physically reduced to pen and paper, the court was prepared to uphold the cancellation.

3. Law Applicable
The Constitution of the Republic of South Africa, 1996 (“Constitution”) recognizes a general right to privacy. Data protection and privacy issues are also currently regulated under the common law and various sector specific statutes and laws governing particular aspects of data protection.

Under common law, privacy embraces all those personal facts which the person concerned has determined to exclude from the knowledge of outsiders and intends to keep private. The Constitution provides, in section 14, that everyone has the right to privacy, which includes, on a broad interpretation, the right:

• to protection against the unlawful collection, retention, dissemination and use of personal information; and/or

• not to have the privacy of their communications infringed.

The constitutional right of privacy is not absolute and an infringement of the right may be justifiable in terms of the general limitation clause in the Constitution. What constitutes a reasonable and justifiable limitation will depend on the circumstances of each case. A high level of protection is given to the intimate personal sphere of life, and a lower level is given to the business, commercial and public spheres of life.

Generally, ordinary delictual (tort) remedies such as a claim for personal injury, patrimonial loss and/or an injunctive relief would be available for a claim arising from wrongful data processing.
The Electronic Communications and Transactions Act, 1998 ("ECT Act") prescribes certain principles for the electronic collection of personal information of individuals. Under the ECT Act, a Data Controller (being a person who electronically requests, collects, collates, processes or stores personal information from or in respect of any natural person) would only be required to subscribe to the data protection principles if it has voluntarily agreed to do so with the Data Subject.

The stated purpose of the Act is to give effect to the constitutional right to privacy. The Constitution, together with the Act, will regulate the parameters for the lawful processing and protection of personal information by automated and manual means.

4. Key Privacy Concepts

a. Personal Data

The Act applies to the processing of personal information of natural and juristic persons. “Personal information” is defined as information relating to identifiable, living natural and juristic persons, including:

- information relating to demographics, such as the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, or contact details, such as the email address, physical address, telephone number or other particular assignment to the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person or the views or opinions of another individual about the person;
- correspondence sent by the person that is of a private or confidential nature; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

The Act applies to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of the Act. If any other legislation provides for conditions for the lawful processing of personal
information that are more extensive than those set out in Act, the extensive conditions prevail.

b. Data Processing

The Act applies to manual and automated data processing. “Processing” is broadly defined as activity, whether automated or not, concerning personal information, which includes:

- the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, blocking, degradation, erasure or destruction of information.

Personal information may only be processed if:

- the Data Subject or a competent person, where the Data Subject is a child, consents to the processing;
- processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party;
- processing complies with an obligation imposed by law on the responsible party;
- processing protects a legitimate interest of the Data Subject; and/or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

c. Processing by Data Controllers

The Act applies to those responsible parties who determine the purposes for which and the manner in which any personal information is, or is to be, processed. A responsible party is defined in the Act as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

d. Jurisdiction/Territoriality

The provisions of the Act will apply to the processing of personal information entered in a record by or for a responsible party that is domiciled in South Africa. The Act will also apply where the responsible party is not domiciled in South Africa but is using either automated or non-automated means to process personal information in South Africa.
e. **Sensitive Personal Data**

Subject to specific limitations and additional requirements, the Act expressly prohibits the processing of “special personal information” – that is, personal information relating to:

- the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or

- the criminal behavior of a Data Subject to the extent that such information relates to:
  - the alleged commission by a Data Subject of any offense; or
  - any proceedings in respect of any offense allegedly committed by a Data Subject or the disposal of such proceedings.

The prohibition on processing special personal information does not apply if the:

- processing is carried out with the consent of a Data Subject;
- processing is necessary for the establishment, exercise or defense of a right or obligation in law;
- processing is necessary to comply with an obligation of international public law;
- processing is for historical, statistical or research purposes to the extent that:
  - the purpose serves a public interest and the processing is necessary for the purpose concerned; or
  - it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;
- information has deliberately been made public by the Data Subject; or
- provisions of specific sections in the Act relating to the relevant types of special personal information are complied with.

The Information Regulator may, subject to subsection 27(3), upon application by a responsible party and by notice in the Government Gazette, authorize a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the Data Subject. The Information
Regulator may impose reasonable conditions in respect of any such authorization.

f. **Employee Personal Data**

South African employment legislation requires every employer to keep a record of certain basic information on an employee, including:

- the employee’s name and occupation;
- the time worked by each employee;
- the remuneration paid to each employee;
- the date of birth of any employee under 18 years of age; and
- any other prescribed information.

The employer must keep a record for a period of three years from the date of the last entry in the record. The collection of such information from the employee may be collected without employee consent, as it is required by law, and an employer will generally be able to justify processing such information.

However, the restrictions on processing special personal information about an employee are more stringent and would need to comply with local employment legislation and the Act. For example, the record of any medical examination performed in terms of the Basic Conditions of Employment Act 1997, must be kept confidential and may be made available only:

- in accordance with the ethics of medical practice;
- if required by law or court order; or
- if the employee has, in writing, consented to the release of that information.

5. **Consent**

a. **General**

Consent of the Data Subject, though not mandatory, is listed as a justification for processing personal information under the Act. The Act defines “consent” as any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information. Under the Act and prior to the collection of the information, or as soon as possible thereafter, the responsible party must take reasonable steps to ensure that the Data Subject is aware of:
• the information being collected and, where the information is collected from the Data Subject, the source from which it is collected; the name and address of the responsible party;

• the purpose for which the information is being collected; whether or not the supply of the information by that Data Subject is voluntary or mandatory; the consequences of failure to provide the information; any particular law authorizing or requiring the collection of the information; the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organization and the level of protection afforded to the information by that third country or international organization; any further information such as the: recipient or category of recipient of the information; nature or category of the information; and

• the existence of his or her right of access to and the right to rectify the information collected; the existence of the right to object to the processing of personal information; and the existence of the right to lodge a complaint with the Information Regulator and the contact details of the Information Regulator, which are necessary, having regard to the specific circumstances in which the information is or is not to be processed to enable reasonable processing. It is anticipated that Data Subjects may exercise these rights through various forms that will be set out in the finalized regulations to the Act.

The form of consent has not been prescribed. However, in order to demonstrate consent for the purposes of the Act, the responsible party will likely need to prove compliance with the above requirements.

b. Sensitive Data
The processing of information relating to the race and ethnic origin of a Data Subject for diversity monitoring purposes would, under relevant employment equity legislation, require the written consent of the employee in the prescribed form. In addition, the collection of any health-related information requires the written “informed” consent of the patient.

The Act expressly prohibits the processing of special personal information. However, this prohibition on processing special personal information under the Act does not apply if the processing is carried out with the consent of a Data Subject. The form of consent, although not prescribed under the Act, should be explicit and clear and should include reference to the requirements listed in paragraph 5a above.

c. Minors
The Act provides that a responsible party may not process personal information concerning a child (being a natural person under the age of 18 years). However, the prohibition on processing personal information of children does not apply if:
- the processing is carried out with the prior consent of a competent person (being any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child);
- necessary for the establishment, exercise or defense of a right or obligation in law;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned;
- it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- the personal information has deliberately been made public by the child with the consent of a competent person.

The Information Regulator may, upon application by a responsible party and by notice in the Government Gazette, authorize a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child. The Information Regulator may impose reasonable conditions in respect of any authorization so granted.

d.  Employee Consent
There is no provision under the Act that specifically addresses consent requirements for employees. With reference to paragraph (4.f) above, it is noted that depending on the type of information collected, local employment legislation may require that consent be procured in writing.

e.  Online/Electronic Consent
Electronic consent is permissible and can be effective in South Africa, provided that it is properly structured and evidenced.

6.  Information/Notice Requirements
Under the Act, an organization that collects personal information must provide Data Subjects with information about:
- the organization’s identity;
- the types of personal information being collected;
- the purposes for collecting personal information;
• its privacy practices (which must be given in a clear and transparent way);
• third parties to which the organization will disclose the personal information;
• the consequences of not providing consent;
• the rights of the Data Subject;
• how the personal information is to be retained;
• where the personal information is to be transferred;
• where the personal information is to be stored;
• how to contact the privacy officer or other person accountable for the organization’s policies and practices;
• how to make an inquiry or complaint;
• how to access and/or correct the Data Subject’s personal information; and
• the duration of the proposed processing.

7. Processing Rules
Under the Act, an organization that processes personal information must limit the use of the personal information to only those activities which are necessary to fulfill the identified purpose(s) for which the personal information was collected.

8. Rights of Individuals
Under the Act, Data Subjects have the general right to:
• be informed by an organization of the personal information the organization holds about the Data Subject and how the personal information is being processed;
• access the Data Subject’s personal information subject to some restrictions and/or qualifications;
• request the correction of the Data Subject’s personal information; and
• request the deletion and/or destruction of the Data Subject’s personal information.

It is envisaged that these rights may be practically implemented by way of various forms, the precedents of which will be set out in the finalized regulations to the Act.
9. Registration/Notification Requirements
Under the Act, organizations that collect and process personal information may be required to file with and notify the appropriate data authority.

10. Data Protection Officers
Under the Act, organizations are required to register a privacy officer or other individual who will be accountable for the privacy practices of the organization with the data protection authority to be established.

11. International Data Transfers
Currently, there is nothing in South African law that expressly restricts/limits the international transfer of personal information. However, under the Act, a responsible party in South Africa may not transfer personal information about a Data Subject to a third party located in a foreign country unless:

- the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that effectively upholds the principles for reasonable processing of information which are substantively similar to the principles applicable in South Africa;

- the law, binding corporate rules or binding agreement includes provisions that are substantially similar to those in the section of the Act relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

- the Data Subject consents to the transfer;

- the transfer is necessary for the performance of a contract between the Data Subject and the responsible party; or

- the transfer is for the benefit of the Data Subject and it is not reasonably practicable to obtain the consent of the Data Subject to that transfer; and if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.

For clarification, it is noted that within the context of the above:

- "binding corporate rules" means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

- "group of undertakings" means a controlling undertaking and its controlled undertakings.
12. Security Requirements

Under the Act, organizations are required to take steps to: ensure that personal information in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organizational security safeguards to protect personal information; and ensure that the level of security is in line with the amount, nature, and sensitivity of the personal information involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose personal information to third parties may be required to use contractual or other means to protect personal information, and may be required to comply with sector specific requirements. Under the Act, organizations shall be held liable together with third-party providers in case of breach by the latter.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach

The Act provides for the notification of security compromises. Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorized person, the responsible party must notify the Information Regulator and the Data Subject, unless the identity of such Data Subject cannot be established.

The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system.

The responsible party may only delay notification of the Data Subject if a public body responsible for the prevention, detection or investigation of offenses or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to a Data Subject must be in writing and communicated to the Data Subject in at least one of the following ways:

- emailed to the Data Subject’s last known physical or postal address;
• sent by email to the Data Subject’s last known email address;
• placed in a prominent position on the website of the responsible party;
• published in the news media; or
• as may be directed by the Information Regulator.

The notification must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including:

• a description of the possible consequences of the security compromise;
• a description of the measures that the responsible party intends to take or has taken to address the security compromise;
• a recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and
• if known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information.

The Information Regulator may direct a responsible party to publicize, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a Data Subject who may be affected by the compromise.

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions.

16. Accountability

Under the Act, organizations are required to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators upon request.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in South Africa, provided that they are in compliance with local laws.

18. E-Discovery

When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of personal information is involved, and advise the employees of the implementation of such system, the monitoring of work tools and the storage of information.
19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace. They may be required to give employees the opportunity to opt out from the spam-filtering solution, and give the employees the opportunity to review the isolated emails designated as spam.

20. Cookies
The use of cookies must comply with data privacy laws. As such, the consent of Data Subjects may have to be obtained before cookies can be used and deployed. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing
Under the Act, an organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Consent of the Data Subject must be obtained for a specific activity. Bundled consent is not considered valid consent. It is envisaged that such consent will have to be obtained through the use of a form which substantially corresponds to that set out in the regulations to the Act.

Currently, responsible parties are required to afford a recipient of direct marketing communications the opportunity to opt out at no cost.
South Korea

Boseong Kim
Seoul
Tel: +82 2 721 4130
boskim@kcllaw.com

Junghwa Lee
Seoul
Tel: +82 2 721 4147
jhlee@kcllaw.com

Mike Shin
Seoul
Tel: +82 2 721 4140
mikeshin@kcllaw.com
1. Recent Privacy Developments

**Amendments to the Act on Promotion of Information and Communications Network Utilization and Information Protection**

- **Regulations on access to smart phones**

  The key amendments to the Act on Promotion of Information and Communications Network Utilization and Information Protection provide for certain regulations on the authority of access to smart phones, under which app service providers must distinguish between optional and necessary access rights for smartphone apps (i.e., what is necessary for the operation of the app), notify users of this information so that they understand it clearly, and obtain users’ consent to access Personal Data stored on their smartphones.

- **Remedy for security breach**

  If a security breach occurs as a result of the service provider’s intentional act or gross negligence, the court may award affected Data Subjects damages of up to three times the damages suffered.

**Amendments to the Personal Information Protection Act (“PIPA”)**

- **Limiting the collection, use and processing of resident registration numbers**

  Under the Amended Personal Information Protection Act (the “Amended PIPA”), public organizations and private business operators may only collect resident registration numbers in accordance with the grounds set out in applicable laws.

- **New penalty for failure to ensure security**

  Under the Amended PIPA, if an entity fails to take measures to ensure security and there is a security breach that results in a leak of resident registration numbers, such entity may be subject to a penalty of up to KRW 5 million.

- **Judicial precedent on security breach**

  Until recently, Korean courts used to be relatively reluctant to recognize the fault of companies in connection with their security breaches; however, this position has now changed. For a claim for damages resulting from a security breach filed against KT Corporation (telecom company), the Seoul Central District Court ordered KT Corporation to pay KRW 2.87 billion to the plaintiffs in the aggregate (which is KRW 100,000 for one plaintiff), finding that: (i) KT was negligent in managing the IDs, passwords and user accounts in its intranet; and (ii) it was highly likely that leaked personal information had been accessed by others and there was a possibility of additional duplication and
subsequent leakage. KT Corporation appealed this decision and the case is now being litigated in an appellate court.

**Guidelines on De-Identification of Personal Information**

The Ministry of the Interior (jointly with the Financial Services Commission and Korea Communications Commission) announced the guidelines on de-identification of personal information (the “Guidelines”) on 30 June 2016.

The Guidelines are not legally binding. However, an act of de-identification of personal information in accordance with the Guidelines may be exempt from the requirements concerning the use and provision to third parties of personal information required under the PIPA and other related laws/regulations.

The Guidelines divide the de-identification process into four stages, as follows:

**Stage 1 (Preliminary review)**

Review whether the information in question constitutes personal information. If not, determine if the information can be used without taking any action.

**Stage 2 (De-identification)**

Implement a process to prevent a person’s identity from being connected with the information in question by way of substituting, or deleting all or part of, the personal identifiers from the dataset. Strategies for de-identifying datasets include pseudonymization, aggregation, data reduction, data suppression and data masking. A single strategy or a combination of several strategies may be used.

**Stage 3 (Quality evaluation)**

The personal information manager would evaluate whether a person can be easily identified using the information in question if combined with other information through a “de-identification quality evaluation group”. An independent expert must participate in such evaluation. The “K-anonymity” (which is an objective and quantitative evaluation method) must be used in such evaluation.

**Stage 4 (Post-management)**

Implement measures necessary to prevent re-identification of de-identified information while the de-identified information is used, including safety measures, monitoring the possibility of re-identification, etc.

The protective measures necessary for safe use of de-identified information and prevention of misuse or abuse of de-identification include destruction of information when the purpose of use is accomplished, management of access
authority/access control, suspension and destruction of information processing if re-identification occurs, etc.

If you intend to provide de-identified information to a third party or outsource the processing of de-identified information to a third party, the relevant agreement with the third party must include matters concerning re-identification risk management (including prohibition of re-identification, prohibition of re-outsourcing and provision to third parties, notification requirement in the event of re-identification risk, etc.).

2. Emerging Privacy Issues and Trends

**Big data processing companies** – There have been discussions about how to regulate big data processing companies in their use of personal information. The Korea Communications Commission (KCC) is in the process of preparing relevant guidelines.

**Biometric identification** – There have been discussions about how to strengthen the security of biometric data such as fingerprint and iris scans which are used for smartphone biometric identification, since it is not possible to change such biometric data when it is leaked. The KCC is preparing guidelines which are due to be published very soon.

**Protection of personal information: new technology** – There have been discussions about how to protect personal information as new technologies are being developed, such as the “Internet of Things”, fintech, autonomous vehicles, etc. The KCC has announced it will amend applicable laws (including increasing penalties for a security breach) as these new technologies propagate and consequently the risks of a security breach increase.

**Strengthening the regulation on personal information processing and crackdown on violations** – In an effort to reduce damages resulting from security breaches, relevant regulations have been strengthened (e.g., restriction on collecting resident registration numbers), and regulatory authorities are increasingly cracking down on personal information infringers.

**Social media** – In theory, regulations concerning social media are applicable to both domestic and foreign entities, but, in practice, it is difficult to enforce them against foreign entities, which raises a concern about appropriate protection of users. Commentators are having ongoing discussions on this issue.

**Privacy breach** – As security breaches in companies have continued to occur, sanctions for such events are being strengthened. In addition, we have recently seen cases in which a privacy breach incident developed into a class action.
Employee monitoring – Commentators began a discussion about this several years ago, but it has been relatively inactive partly due to other more pressing labor and management issues.

Illegal sale of personal information – The illegal sale of customers’ personal information has become an issue, and commentators are discussing ways to regulate such illegal sale.

Other than the above, we are seeing an increasing discussion concerning personal information protection issues associated with the development of technology for the “Internet of Things” and the “right to be forgotten”.

3. Law Applicable

The applicable privacy/information laws are as follows:

The general law governing the protection of personal information is the Personal Information Protection Act or PIPA.

Information and communications service providers are regulated by the Act on Promotion of Information and Communications Network Utilization and Information Protection.

Personal credit information handled by financial institutions is governed by the Act on Use and Protection of Credit Information.

Below are hyperlinks to the applicable laws (Korean language only):

i. PIPA
   http://www.law.go.kr/lsInfoP.do?lsiSeq=195062&efYd=20170726
   Enforcement Decree of the PIPA
   http://www.law.go.kr/lsInfoP.do?lsiSeq=195569&efYd=20170726#0000
   Enforcement Rules of the PIPA
   http://www.law.go.kr/lsInfoP.do?lsiSeq=196160&efYd=20170726#0000

ii. Act on Promotion of Information and Communications Network Utilization and Information Protection
    http://www.law.go.kr/lsInfoP.do?lsiSeq=195040&efYd=20170726#0000
    Enforcement Decree of the Information and Communications Network Act
    http://www.law.go.kr/lsInfoP.do?lsiSeq=197332&efYd=20170905#0000
    Enforcement Rule of the Information and Communications Network Act
    http://www.law.go.kr/lsInfoP.do?lsiSeq=197332&efYd=20170905#0000

iii. Act on Use and Protection of Credit Information (“Credit Information Act”)
     http://www.law.go.kr/lsInfoP.do?lsiSeq=195311&efYd=20170726#0000
4. Key Privacy Concepts

a. Personal Data

Under the PDPA, “Personal Data” means data pertaining to a living person, including their name, resident registration number, images, etc., by which the individual can be identified. The PDPA provides no specific requirements in terms of the types, forms and characteristics of the data, data processing methods, or media in determining whether certain information constitutes Personal Data.

Under the Information and Communications Network Act, “Personal Data” means data in the form of code, letter, voice, sound, image, etc., that pertains to a living individual and identifies a specific person through the name, resident registration number, etc.

The definition of Personal Data under the PDPA is broader than that under the Information and Communications Network Act. Other area-specific laws that cover privacy-related issues impose requirements on other limited types of Personal Data.

b. Data Processing

Under the PDPA, processing is comprehensively defined to mean collecting, creating, recording, saving, retaining, processing, editing, searching, printing out, correcting, restoring, using, providing, disclosing and/or destroying Personal Data, and other similar acts.

c. Processing by Data Controllers

Under the PDPA, a “Personal Data processor” means a public institution, corporate body, organization, individual, etc. that processes Personal Data directly or via another person to administer Personal Data files as part of their duties. “Personal Data files” means an aggregate of Personal Data systematically arranged or organized according to specific rules in order for the Personal Data to be readily retrievable.

Under the Information and Communications Network Act, Data Controllers are limited to those who provide information and communications services.
Under the Credit Information Act, Data Controllers are limited to those who provide or use credit information.

Korean privacy law regulates Personal Data Processors, but does not distinguish between Data Controllers and Data Processors. Therefore, the most likely interpretation of the law is that both Data Controllers and Data Processors are subject to the same obligations.

d. Jurisdiction/Territoriality
The application of Korean privacy law, including the PDPA, is not limited based on where the collection or processing of Personal Data occurs. Thus, in theory, companies located overseas that collect Personal Data of users in Korea are subject to Korean privacy law. In practice, however, it is very rare for Korean judicial authorities to enforce Korean privacy law in such cases.

e. Sensitive Personal Data
The PDPA imposes additional requirements relating to the handling of (i) “sensitive data”, including ideas, belief, membership in or withdrawal from a labor union or political party, political views, health, etc., and genetic information and criminal records, and (ii) “unique identifying data”, including resident registration number, passport number, driver’s license number and alien registration number.

Processing of such sensitive data and unique identifying data is prohibited with only limited exceptions.

f. Employee Personal Data
Employee Personal Data was previously unregulated. However, since the PDPA came into force, Employee Personal Data should be treated in the same way as any other Personal Data.

As discussed in Section 5(d) below, an employer may collect and use Personal Data of an employee for the purposes of entering into and performing an employment contract. The PDPA does not, however, address the permitted scope or limitations on an employer’s collection/use of Employee Personal Data without the employee’s consent.

5. Consent

a. General
Under the PDPA, consent of the Data Subject is generally required prior to the collection, use or provision of Personal Data to third parties, subject to certain exceptions, including when it is: required or permissible by law; necessary to perform an agreement with the Data Subject; or urgently needed to protect life, body or property.
Consent must be voluntary, informed, explicit and unambiguous. Consent can be provided by way of a signature, clicking on a consent button (e.g., “I Agree” or “I Consent”), telephone, etc.

When obtaining the consent of a Data Subject, a Personal Data processor is required to notify the Data Subject of the specific matters requiring consent so that the Data Subject clearly understands what consent is being sought. Consent of the Data Subject only covers identified purposes. Fresh consent is required for purposes not previously identified and consented to.

The Data Subject can withdraw his/her consent at any time.

b. Sensitive Data
Sensitive data is recognized as a special category of Personal Data.

Under the PDPA, a Personal Data processor is required to obtain a Data Subject’s separate consent (i.e., in addition to consent obtained for processing general Personal Data) in order to process sensitive data or unique identifying data.

c. Minors
Consent cannot be obtained from minors, but can be given by a legal guardian or parent.

When a Personal Data processor obtains the consent of a legal representative of a child under the age of 14, the minimum information necessary for obtaining the consent of the legal representative (e.g., the name, contact information of the legal representative) may be collected from the relevant child without the consent of his or her legal representative.

d. Employee Consent
Since the collection/use of Personal Data is necessary for entering into and performing an employment contract with an employee, certain Personal Data of an employee may be collected/used without the employee’s consent. However, the Ministry of the Interior and Safety has made it clear that employers should notify employees of all relevant matters concerning the collection/use of their Personal Data in their employment contract.

In addition, installation of employee surveillance equipment (e.g., CCTV, GPS) in a place of business is subject to discussions with the labor-management consultation council, but there are no provisions providing for penalties for breach of this requirement.

e. Online/Electronic Consent
Electronic consent is permissible and can be effective in South Korea if it is properly structured and evidenced.
The PDPA allows for consent to be obtained from the Data Subject through a process on the Internet (e.g., clicking on a consent button), email, electronic documents, text messages, etc.

6. Information/Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; how the Personal Data is to be retained; where the Personal Data is to be transferred; how to contact the privacy officer or other person accountable for the organization’s policies and practices; how to make an inquiry or file a complaint; how to access and/or correct the Data Subject’s Personal Data; and the duration of the proposed processing.

When processing Personal Data collected from sources other than the Data Subjects, at the request of the Data Subjects, the Personal Data processor is obligated to notify the Data Subjects of the relevant sources, purpose of processing the Personal Data and the fact that the Data Subjects have the right to request suspension of the processing of Personal Data.

According to the Amended PIPA, which became effective on 30 September 2016, however, a Personal Data processor who processes sensitive data under Article 23 or unique identifying data under Article 24 of the PIPA of 50,000 or more Data Subjects or who processes Personal Data of 1 million or more Data Subjects, the Personal Data processor must comply with the above notification requirement (which may be satisfied by sending the notification via email or text message) regardless of whether or not requested by the Data Subjects.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities that are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; (iv) request the deletion and/or
destruction of the Data Subject’s Personal Data; (v) and exercise the writ of habeas data.

9. Registration/Notification Requirements

There are no requirements for organizations that collect and process Personal Data to register, file or notify the local data authority.

10. Data Protection Officers

Organizations are required to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.

The PDPA specifies the qualifications for a data protection officer, his/her duties and other related matters. The Information and Communication Network Act contains similar provisions. Depending on the size of the company, the owner or authorized representative of the company can act as the data protection officer in lieu of designating a separate data protection officer.

11. International Data Transfers

Organizations may transfer Personal Data outside of South Korea, provided that reasonable steps have been taken to safeguard such Personal Data.

The PDPA sets out the procedures that a Personal Data processor must follow in order to transfer Personal Data to third parties in other jurisdictions. The Information and Communications Network Act also provides for the procedures for transfers of Personal Data to other jurisdictions and related protective measures.

12. Security Requirements

Organizations are required to take steps to: (i) ensure that Personal Data in its possession and control is protected from unauthorized access and use; (ii) implement appropriate physical, technical and organization security safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and may be required to comply with sector-specific requirements. Organizations shall be liable together with third-party providers in case of breach by the latter.

The PDPA provides for matters concerning the scope of outsourcing, disclosure of the outsourcer, the organization’s obligation to manage and
supervise the outsourcer’s work, limitation on the scope of Personal Data processing by outsourcers, the organization’s liability for damages, etc.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, class actions, criminal proceedings, and/or private rights of action.

15. Data Security Breach
Under the PDPA, in the event of a data breach, the Personal Data processor must notify the Data Subject of such an event according to the prescribed methods of notification. In the event of large-scale security breaches, the PDPA imposes the requirement to notify the Ministry of Public Administration and Security or other specialized agencies and provides for follow-up measures.

The Information and Communications Network Act contains provisions dealing with incidents of security breaches of information and communications networks.

In addition, organizations that are involved in a data breach situation are required to: (i) gather information about the breach; (ii) assess the potential risk of harm to the Data Subject; (iii) take steps to mitigate the harm to impacted Data Subjects; (iv) take steps to contain the breach and prevent future similar breaches; (v) assist authorities with any investigation relating to the breach; (vi) and comply with data authority orders and court orders.

An organization that is involved in a data breach situation may be subject to a suspension on the processing of Personal Data, an administrative fine, penalty or sanction, civil actions and/or class actions, or a criminal prosecution.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
There are no laws/rules that regulate whistle-blower hotlines in South Korea.

18. E-Discovery
South Korea does not have a system equivalent to e-discovery under US law. An organization, however, may be required to provide Personal Data pursuant to a court order.
19. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to review the isolated emails designated as spam.

20. Cookies

The use of cookies must comply with data privacy laws. Consent of Data Subjects may have to be obtained before the use and deployment of cookies.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior consent, which may not be inferred from a Data Subject’s failure to respond.

Where consent is sought for marketing or soliciting the sale of goods or services as part of the sale of any goods or services, the Personal Data processor cannot refuse to provide such goods or services on the grounds that the Data Subject refused to consent to receive marketing or sales information.
Spain

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com

Patricia Pérez
Madrid
Tel: +34 91 436 6627
patricia.perez@bakermckenzie.com

Candelaria Canaro
Barcelona
Tel: +34 93 206 0820
cande.canaro@bakermckenzie.com
1. Recent Privacy Developments

**General Data Protection Regulation**

The European General Data Protection Regulation (“GDPR”) will start to apply as of May 2018, and it is already having a serious impact on data privacy in Spain. Once it applies, it will establish a number of new obligations and will strengthen many of the current requirements outlined in this handbook.

In June 2017, a new Spanish Data Protection Preliminary Draft Bill was issued, which included the interpretation made by the Spanish relevant actors of the requirements determined under the GDPR. In November 2017, the Council of Ministers has passed the Personal Data Protection Draft Act seeking to conform Spanish law to the GDPR, which is under parliamentary review.

Additionally, the Spanish Data Protection Authority (“SDPA”) has already issued a number of reports highlighting some of the requirements set forth by the GDPR and recommending that organizations start preparing for the new measures and obligations.

**Marketing, advertising and commercial communications can be based on the legitimate interest legal ground included by the GDPR**

In its Legal Report 0195/2017, the SDPA analyzes data processing for “marketing, advertising and commercial communication purposes in line with the development of the business carried out by the entity of its own products and/or services”.

In this respect, the SDPA states that if commercial communications are distributed via electronic channels, they are subject to both the Spanish Electronic Commerce Information Society Services Act and the GDPR. According to the Spanish E-Commerce Act, the recipient’s express consent must be obtained in advance when carrying out marketing and advertising actions, unless a previous contractual relationship exists and the commercial communications relate to products/services similar to those initially purchased by the recipient.

On the other hand, for advertising and marketing actions to be covered by the legitimate interest contained in Article 6.1. f GDPR (and not requiring the Data Subject’s express consent), the following requirements must be met:

i. advertising and marketing actions must be distributed via non-electronic channels

ii. the affected Data Subjects must remain customers of the company

iii. the products or services offered must be considered “similar” to those contracted by the customers.
**Anonymization and Pseudonymization**

In the same report, the SDPA analyses the “anonymization of transactional data, obtained through the products and/or services of financial entities, to develop new products and/or services based on anonymization and aggregated data”.

In accordance with the GDPR, anonymization and pseudonymization of Personal Data involve two types of processing: (i) the first one involves anonymization or pseudonymization of the Personal Data already held by the Data Controller; and (ii) the second refers to the processing of data after the anonymization or pseudonymization (in this case, when the data is completely anonymized, the GDPR shall not apply).

Additionally, the difference between these two types of processing assumptions will also influence the consideration required by Article 6.1. f. of the GDPR on legitimate interest, since in the first case, if it is a complete anonymization, the condition of the processing will be less than if the data is only pseudonymized.

**Profiling for specific purposes**

The same report assesses the “analysis of transactional movements and/or savings capacity of customers to make observations and offer recommendations on products and/or services of financial entities for the benefit of a better management of customers’ finances”. The report concludes that if the data that will be used for profiling, (i) is collected from the information that is available to the financial entities for the management of the already contracted services, (ii) the products and/or services that will be offered are similar to those contracted, and; (iii) the clients have been informed separately about this kind of processing, then, Article 6.1.f of the GDPR may be applicable (the data processing could be justified on the basis of legitimate interest).

However, given the high level of intrusion derived from this type of data processing, the SDPA considers that organizations must inform the Data Subject in a detailed manner about the profiling, their right to oppose to such processing, and the temporal scope of this profiling.

**Annual report 2016**

According to SDPA’s annual report 2016, there is a 24.3% increase in claims, mainly against telecoms services, financial entities and energy and water supply companies. The report also highlights the increase of granted authorizations for international transfers of data.
2. Emerging Privacy Issues and Trends

**Employee monitoring**

On 2 February 2017, the Spanish Supreme Court issued a judgment reaffirming the 2016 Constitutional Court’s set criteria, which stated that when a company suspects that irregularities are being committed, it can monitor its employees with video surveillance cameras without having to inform the employees of the specific purpose or reason why such cameras are being installed. In the particular case addressed by the Supreme Court, a company dismissed an employee for disciplinary reasons verified on videos recorded by the cameras installed in the company. The company did not previously inform its employees about the cameras. However, the cameras were installed in a visible place for employees to notice. In this regard, the Spanish Supreme Court ruled in favor of the company on the grounds that the use of the cameras in a visible position was reasonable and proportionate to its purpose without there being any risk of infringement of the right to personal privacy.

According to the recent judgement of the European Court of Human Rights regarding the Bărbulescu v. Romania case, it seems that greater information will need to be provided to employees on the scope and nature of any employee monitoring carried out, the reasons for it, as well as the possibility that the contents of employees’ communications could be accessed. The SDPA in its Guide to the protection of Personal Data in employment relationships already recommends to provide information on the purpose of monitoring and the monitoring measures adopted. Additionally, the Article 29 Working Party has published its guide on the processing of Personal Data in an employment context where it included its recommendations for the monitoring of IT tools (among others, the prohibition of continuous monitoring). Thus, employees shall be informed about:

i. the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures.

ii. the extent of the monitoring by the employer and the degree of intrusion into the employee’s privacy.

iii. the legitimate reasons for justifying monitoring the communications and accessing their actual content. Since accessing the content of communications is by nature a distinctly more invasive method, it requires weightier justification;

iv. the implementation of a monitoring system based on less intrusive methods available;

v. the consequences of the monitoring for the employee subjected to it, if any;
vi. the provision of adequate safeguards, especially when the employer’s monitoring operations were of an intrusive nature. Such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.

3. Law Applicable

- The Spanish Data Protection Act No. 15/1999 (“SDP Act”), which transposes the Data Protection Directive 95/46/EC into national law.
- The Royal Decree No. 1720/2007 (“DPAR”), which approves the regulation implementing the SDP Act.
- Instruction No. 1/2006 of the Spanish DPA on the processing of Personal Data for surveillance purposes through camera systems.
- As of 25 May 2018, the Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (“GDPR”) and the corresponding Guidelines that may be issued by the competent authorities in charge of the interpretation of this regulation.

In addition to all these applicable legislations, it is also important to mention the following Spanish DPA Guidelines:

- Guide for the fulfillment of the obligation to inform.
- Guidance and guarantees in the procedures for anonymizing Personal Data.
- Guide for the development of data processing agreements.

- Data Protection Draft Bill, which will supplement the GDPR. References to the content regulated in this document are included through this chapter, however it should be noted that this draft bill is under parliamentary review and may be subject to change.

4. Key Privacy Concepts

a. Personal Data

The SDP Act applies to the processing of any alphanumeric, graphic, photographic, acoustic or any other type of information (“Personal Data” or “Data”) relating to an identified or identifiable individual (“Data Subject”).

The GDPR defines as Personal Data, any information relating to an identified or identifiable Data Subject; which is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more
factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject.

b. Data Processing

“Processing” is broadly defined and covers any operational or technical process, whether automated or manual, performed on Personal Data that allows the collection, recording, storage, production, amendment, consultation, use, rectification, blocking and deletion, as well as the disclosure of Personal Data resulting from communications, consultations, interconnections and transfers. The SDP Act and DPAR apply to both automated and manual data processing.

Notwithstanding the foregoing, the DPAR foresees the following exemptions to the application of Spanish data protection legislation:

- Contact details of individuals providing their services within legal entities would fall out of the scope of data protection regulations, provided: (i) the categories of data processed relate only to first and last name, position, business address, email address, and phone and fax business numbers; and (ii) the purpose for processing such information shall be limited to the mere maintenance of the business relationship.

- Contact details of sole traders would fall out of the scope of data protection regulations, provided: (i) the categories of data processed refer to the sole trader exclusively with regard to its trader, industrial or ship-owner conditions; and (ii) the purpose of processing such information is of a commercial nature, (i.e., the Data Subject concerned with the data processing activities is the private entity formed by the trader, industrial or ship-owner and not said persons themselves).

Under the GDPR, “processing” is any operation performed on Personal Data, whether or not by automated means, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

c. Processing by Data Controllers

The SDP Act and DPAR apply to those entities that determine the purposes and the manner in which any Personal Data is to be processed (“Data Controller”).

The GDPR imposes obligations on both the Data Controller and the Data Processor.
d. **Jurisdiction/Territoriality**

The SDP Act and DPAR apply to:

- Data Controllers conducting their activities through an establishment in Spain. In this sense, where no Data Controller is established in Spain but data is processed by means of a Data Processor established in Spain, the Data Processor will be bound by the technical and organizational security measures set forth by Title VIII of the DPAR; or

- the processing of Personal Data taking place outside of Spain but subject to Spanish law pursuant to international public law rules; or

- Data Controllers that do not have any establishment in the EEA but that use any means located in Spain to carry out data processing activities other than merely for the purpose of transit (e.g., where Personal Data is collected by a Spanish affiliate or where a website is located in Spain). In this case, the Data Controller must designate a representative established in Spain.

“Establishment” shall be considered, irrespective of its legal structure, as any stable installation allowing the effective and real undertaking of an activity.

The GDPR will apply if Personal Data is processed in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not. It will also apply to the processing of Personal Data of Data Subjects who are in the European Union by a Controller or Processor not established in the European Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the European Union; or (b) the monitoring of their behavior as far as their behavior takes place within the European Union.

e. **Sensitive Personal Data**

The SDP Act imposes additional requirements for the processing of Sensitive Personal Data – that is, information relating to ideology, religion, beliefs, racial origin, health or sexual life, trade union membership, and criminal or administrative offenses. Data Subjects may not be compelled to disclose their ideology, beliefs or religion. Explicit and written consent to the processing of Personal Data relating to trade union membership, ideology, religion and beliefs must be obtained. Except as indicated below, the processing of Personal Data relating to health, racial origin and sexual life requires the prior express consent of the Data Subject, although it need not be given in writing. As a general rule (subject to very restrictive exceptions), Personal Data relating to criminal records and administrative sanctions may not be processed by a private Data Controller (even with the consent of the Data Subject) except by duly authorized public institutions.
Specifically, the processing of Sensitive Personal Data is prohibited unless certain conditions are met, for example:

- the Data Controller obtains the explicit (and written) consent of the Data Subject (see Section 5(b) below);
- the processing is necessary to carry out the obligations and rights of the Data Controller in the field of employment, social security and health, and safety laws;
- the processing is necessary to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent;
- the processing is carried out in the course of legitimate activities with appropriate guarantees by political parties, trade unions, churches or other religious communities, foundations, associations or any other non-profit-seeking bodies only in respect of the relevant Sensitive Personal Data (for example, political parties are exempted from consent only in respect of the processing of ideology information) and provided other conditions are met; or
- the processing is performed by a health care professional or institution under an obligation of secrecy, for the provision of medical advice or treatment.

Under the GDPR, special categories of Personal Data include any information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

As a general rule, the processing of special categories of data is prohibited under the GDPR. But the GDPR also establishes a series of exceptions such as where the Data Subject has explicitly consented.

f. Employee Personal Data

Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information) and non-Sensitive Personal Data. Sensitive Employee Personal Data may be processed in the circumstances mentioned in Section 4 (e) above and, in particular:

- where the Personal Data is health data, the employer may process the start and end date of any sickness or absence (which is considered to be processing of Personal Data by the Spanish DPA) for compliance with social security requirements – that is, in order to comply with its obligations under employment, social security and health and safety laws,
as well as the grade of disability of the employee, prior consent is not required. However, should the Data Controller wish to process any additional information (such as the reason for absence or medical certificates), the Data Controller would have to seek the prior express consent of the employee to the processing of such Personal Data and have a legitimate purpose for processing such data;

- where the Personal Data relates to the employee’s ability to perform “dangerous” or “very dangerous” activities or any activities which require a medical assessment for the prevention of “occupational risks” (as they are defined under the Spanish Labor Risks Prevention Act), this may be processed without prior consent, although this should be assessed on a case-by-case basis. However, should the Data Controller be required to conduct a medical assessment of the ability of employees to perform activities, the Spanish Labor Risks Prevention Act provides that the Data Controller may process only a “fit for work/unfit for work” result without prior consent, and may not process a description of the specific health conditions of the employee. In addition, should the Data Controller wish to conduct any other type of medical assessment (e.g., physical exams, recruitment medical exams, etc.), it should generally obtain the prior express consent of the employee and have a legitimate purpose for processing such data; and

- where the Personal Data relates to trade union membership, this may be processed to the extent necessary to comply with legal and/or collective bargaining agreement obligations, provided that other specific requirements are met.

Non-Sensitive Employee Personal Data may be processed by a Data Controller in the circumstances mentioned in Section 5 below and, in particular, for the following purposes: human resources management, payroll, management of benefit plans (life and health insurances, stock option plans, etc.), training programs, legal requirements (social security and tax withholdings), annual evaluations and when processing is necessary for the execution of an agreement to which the Data Subject is a party. A fallback justification for processing both sensitive and non-Sensitive Personal Data in the employment context may be if consent is provided by the Data Subject.

In early 2010, the Spanish DPA issued a series of guidelines which aim to gather under a single document its existing opinions and recommendations concerning the processing of data within employment relationships so as to provide both private and public organizations with a tool to make compliance with the requirements set forth by Spanish data protection regulations easier. The guidelines are split into five chapters: (i) human resources; (ii) labor risk prevention; (iii) monitoring activities conducted by employers; (iv) relationship
with trade-unions; and (v) obligations of employees when accessing Personal Data related to them.

5. Consent

a. General

Under the SDP Act, consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in certain prescribed circumstances.

Consent can be express or implied, but the appropriate form of consent will depend on the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data.

Consent of the Data Subject only covers identified purposes. Fresh consent is required for purposes not previously identified and consented to.

The Data Subject also has the right to withdraw consent at any time in given circumstances.

Similarly, under the GDPR “consent” of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

As a general rule, consent may be in writing (including in electronic form) or oral form. However, caution should be exercised when relying on oral consents as the onus for demonstrating that consent has been obtained clearly is on the controller.

A closer look at the specific requirements for consent under GDPR:

- **Unambiguous:** consent requires either a statement or clear affirmative action in order to be valid.

- **Freely given:** The GDPR now clarifies that consent will not be freely given if: (i) the Data Subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment; and/or (ii) there is a clear imbalance between the Data Subject and the controller.

- **Specific:** consent must relate to specific processing operations. Consequently, a general broad consent to unspecified processing operations as they might arise will be invalid.

- **Informed:** Data Subjects should understand the extent to which they are consenting and be aware, at least, of the identity of the controller and the purposes of the relevant processing.
• **Right to withdraw:** Data Subjects must be able to withdraw their consent at any time and be informed of their withdrawal right at the time of consenting.

**b. Sensitive Data**

Explicit and written consent to the processing of data relating to trade union membership, ideology, religion, and beliefs must be obtained. The processing of data relating to health (except in compliance with labor, social security and health, and safety regulations), racial origin and sexual life requires the prior express consent of the Data Subject, although it need not be given in writing.

Under the GDPR, the processing of sensitive data is permitted if the Data Subject has explicitly consented although it should be noted that Member States may provide that the general prohibition on processing sensitive data may not be lifted by the Data Subject.

**c. Minors**

Under the DPAR, minors over 14 years of age may give valid consent to the processing of their Personal Data, to the extent that it is accepted that such minors have, in such cases, sufficient personal capacity of judgment to provide such consent. The consent of parents or guardians is required for minors under 14 years old. Data Controllers shall guarantee that they have confirmed, through effective means, the age of children and the authenticity of the consent provided, where applicable, by parents or guardians.

The GDPR, recognizing that children deserve specific protection of their Personal Data, makes express provision for consents provided by children. Essentially, it prescribes that, in an online context, the age of consent is 16 unless Member State law provides for a younger age of consent (which must not be below 13). The new Data Protection Draft Bill sets the age for consent to 13 years.

**d. Employee Consent**

Under the SDP Act, consent must be: (i) freely given (which means that the Data Subject may not be compelled to provide his/her Personal Data, unless where expressly required by law); (ii) unequivocal (which means that no doubt exists as to the processing activities consented to by the Data Subject); (iii) specific (which means that the Data Subject must give his/her consent to each processing activity and for the purposes disclosed by the Data Controller); and (iv) informed (which means that the Data Controller has complied with its information requirements). In addition, according to general civil law principles, any consent provided by an individual by mistake, under intimidation, violence or willful misconduct will be void and null, particularly in employment relationships, where the employee is considered the weaker party. Labor courts have consistently indicated that consent provided under any of such circumstances will be void.
The GDPR expressly states that, where there is an imbalance of power between the Data Subject and the Controller, consent will not be valid (for example between employer and employee). This means that it will be difficult for employers to rely on consent to process employees’ Personal Data under the GDPR. However, consent is only one of a number of potential legal bases for processing employees’ Personal Data. As an example, processing can be lawful where it is necessary for the performance of a contract to which the Data Subject is party. An employer may legally process Personal Data about employees necessary to fulfill the employment contract.

e. Online/Electronic Consent
Under the GDPR and the SDP Act, electronic consent is permissible and can be effective in Spain if properly structured and evidenced. Specifically, the GDPR establishes that electronic requests for consents must be clear, concise and not unnecessarily disruptive to the use of the services for which they are provided.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about the organization’s identity; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; and where the Personal Data is to be transferred.

Under the GDPR notice requirements are even expanded and include, e.g., information about the legal basis for the processing, the period for which data will be stored, and, where applicable, the legitimate interests pursued by the Controller or by a third party.

The GDPR also imposes an obligation on controllers to inform Data Subjects about: (i) their right to restrict any processing concerning their Personal Data; (ii) to object to processing; (iii) the right to data portability; and (iv) the right to lodge a complaint with a supervisory authority.

In this respect, the SDPA has issued some guidelines which clarify that it is possible to provide the information in two layers: a first layer with the minimum required information and a second layer with more detailed information, which can be accessed through a link, for example.

7. Processing Rules
An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and cancel Personal Data once the stated purposes have been fulfilled. Cancelation is not equal to deletion. Cancelation implies blocking the data, which consists of
their identification and reservation in order to prevent processing except to provide them to public administrations, judges and courts for the purpose of dealing with any liability arising from processing, and only for the duration of such liability. On the expiry of such term, the data shall be deleted.

8. Rights of Individuals

Data Subjects have the right to: (i) request access to the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject's Personal Data; (iv) request the cancelation of the Data Subject’s Personal Data; and (v) object to further processing of the Personal Data.

In line with the GDPR, new rights are being recognized by the new Data Protection Draft Bill (i.e., right to data portability) and specific rights are regulated (i.e.: right to be forgotten, right of the restriction on processing and right to oppose to profiling activities).

9. Registration/Notification Requirements

Data Controllers are obliged to notify and register its Personal Data files before the Spanish DPA’s Registry. Registration must be performed prior to the use of any file or of any data processing operation. Any change of contents of the file or its use, including its cancelation, must also be notified. This obligation must be performed by means of the forms available at the Spanish DPA’s website and must be sent by the Data Controller in paper or electronically to the Spanish DPA.

Notification and registration requirements will no longer apply under GDPR. Instead of such requirements, the new Data Protection Draft Bill provides that Data Controllers and Data Processors should keep an internal, written record of their processing activities carried out unless some of the exceptions provided in the GDPR apply (i.e., companies with less than 250 employees).

10. Data Protection Officers

Under the currently applicable legislation, there is no requirement for organizations to designate a data protection officer (“DPO”) or other individual who will be accountable for the privacy practices of the organization.

According to the new Data Protection Draft Bill, companies are obliged to designate a DPO in the cases prescribed by the GDPR — when (i) the core activities of the controller consist of processing operations which require regular and systematic monitoring of Data Subjects carried out on a large scale; or (ii) the core activities of the controller consist of processing operations on a large scale of special categories of Personal Data (i.e., health
data). And the Data Protection Draft Bill provides a list of certain cases where Data Controllers and Data Processors are obliged to appoint a DPO.

11. International Data Transfers

Transfers of Personal Data from Spain to countries offering an equivalent level of protection may take place freely. Said countries are EU and EEA Member States, Argentina, Israel, Andorra, Faroe Islands, Canada, Switzerland, Guernsey, the Isle of Man, Jersey, New Zealand, Uruguay and US recipients that have signed up to the Privacy Shield arrangement, as well as any other countries which are deemed to grant an equivalent level of protection under a decision of the European Commission. International transfers to third countries not granting an equivalent level of protection, such as the US (except as indicated below), may only take place under the SDP Act where the prior authorization of the Spanish DPA has been obtained. Some exceptions to this requirement (i.e., where no authorization is required) are where:

- the Data Subject has given unequivocal consent to the transfer;
- the transfer is necessary for the performance of an agreement entered into between the Data Subject and the Data Controller or for taking pre-contractual measures at the Data Subject’s request;
- the transfer proves to be necessary for litigation purposes;
- the transfer is necessary for the conclusion or performance of a contract between the Data Controller and a third party to the benefit of the Data Subject;
- the transfer is in the public interest;
- the transfer is requested by tax and customs authorities; or
- the transfer is related to money transfers.

The transfer of Personal Data to a non-EEA country with inadequate protection levels is also permitted with the prior authorization of the Spanish DPA if a data transfer agreement is used and the agreement incorporates the EU model contractual clauses for the transfer of Personal Data to third countries adopted by the European Commission on 15 June 2001 and 27 December 2004 (Data Controller to Data Controller) or on 5 February 2010 (Data Controller to Data Processor). The applicable EU model contractual clauses duly executed by the relevant parties (Data Exporter and Data Importer) are to be submitted, together with a transfer authorization request and additional documentation, to the Spanish DPA.

In addition, the prior authorization of the Spanish DPA may also be granted if the international data transfer is held between companies of the same group
based on Binding Corporate Rules ("BCRs"). In the process of authorizing the international transfers based on BCRs, the Spanish DPA will review and comment on the BCRs.

The new Data Protection Draft Bill, in line with the GDPR provisions, introduces certain aspects that affect the whole international transfer regime.

i. The data exporter can be both a Data Controller and a Data Processor.

ii. The GDPR introduces additional legal bases, such as an approved code of conduct together with binding and enforceable commitments of the Controller or Processor in the third country, or an approved certification mechanism.

iii. A regime of prior authorization of the Spanish DPA is reduced to very few scenarios and prior notification of international transfers is introduced for other particular scenarios.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved. Current legislation lists the specific security measures to be applied which vary depending on the categories of data processed. Data Controllers must document the technical and organizational measures implemented.

To meet the new legal requirements under the GDPR, security measures will also have to take into account the current and potential risks that could affect the Data Subjects rights. Security measures will need to be detailed in the written record of the processing activities that companies will be obliged to keep and in data protection impact assessments (if any).

13. Special Rules for Outsourcing of Data Processing to Third Parties

In accordance with the current law, a services contract ("Data Processing Agreement") between a Data Controller and the service provider ("Data Processor") to process Personal Data (e.g., payroll service) must include express restrictions that the Data Processor: (i) shall process the data only in accordance with the instructions of the Data Controller; (ii) shall not apply or use the Personal Data for any purpose other than that set out in the Data Processing Agreement; and (iii) shall not disclose the Personal Data to third parties. With respect to the third requirement, the DPAR permits the Data Processor to subcontract data processing functions to a third party ("Subcontractor"), provided that the Data Processor obtains the Data
Controller’s consent to engage the Subcontractor. Alternatively, the Data Processor may engage the Subcontractor if the Data Processing Agreement: (a) already specifies particular function(s) that may be subcontracted and names a pre-approved subcontractor; (b) requires that the Subcontractor processes the Personal Data only in accordance with the Data Controller’s instructions; and (c) requires the subcontract to include terms providing for requirements (i) through (iii).

Where the Data Processor is located outside the EEA in a country not offering an equivalent level of protection, and prior authorization from the Spanish DPA is required, the Data Processing Agreement shall follow the model contractual clauses for the transfer of Personal Data to Data Processors located in third countries adopted by the European Commission.

Under the GDPR it will still be possible to outsource data processing activities to Data Processors but GDPR will impose privacy obligations directly on processors and also prescribes in detail the terms to be included in data processing agreements.

The SDPA has recently published a guideline for the drafting of Data Processing Agreements in accordance with the GDPR provisions, which contains detailed interpretations and descriptions of the applicable requirements for processing agreements.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, and/or private rights of action.

Under the GDPR, fines will be significant with maximum fines amounting to up to EUR 20,000,000 or up to 4% of the company’s total worldwide annual turnover of the preceding financial year, whichever is higher.

15. Data Security Breach

Presently, Data Controllers are not generally required either to notify the Spanish DPA or the Data Subjects upon the occurrence of a data security breach.

However, an amendment to the Spanish Telecommunications Act sets forth the obligation to notify the Spanish DPA and the Data Subjects, as applicable, of the occurrence of a data security breach where the Data Controller is an operator providing publicly available electronic communications services.

Under the GDPR, in the event of a data security breach, Data Controllers must notify the supervisory authority not later than 72 hours after having become aware of the breach. A notification is not required if the breach is
unlikely to result in a risk to the rights and freedoms of natural persons. There is also a requirement for Data Processors to notify the Data Controller without undue delay after becoming aware of a data security breach.

Data Controllers must also notify any affected individuals if (i) the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, or (ii) if the supervisory authority requires the Data Controller to do so. The Controller must communicate the Personal Data Breach to the affected individuals without undue delay.

16. Accountability

A “proactive responsibility” obligation is imposed on organizations by the GDPR and the new Data Protection Draft Bill, requiring them to implement measures in order to comply with the GDPR and the local data protection regulations. In other words, it is not enough for an organization to have the right data protection policies, but they have to demonstrate that the said policies have been duly implemented and work in practice.

Additionally, organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

Opinion 0128/2007 of the Spanish DPA (June 2007), entitled “Internal reporting schemes (whistle-blowing mechanisms)”, which is in line with Opinion 1/2006 of the Article 29 Working Party, generally foresees the establishment of whistle-blower hotlines dealing with accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime. Although the implementation of whistle-blower hotlines exceeding the scope of Opinion 0128/2007 (e.g., sexual harassment, misconduct regarding the protection of the environment, inhumane working conditions, etc.) is not prohibited, it may be harder to implement the same as it has to be accompanied with sufficient evidence to uphold the legitimacy and the need for the proposed processing.

Based on Opinion 0128/2007, it is advisable to submit specific filing requirements with the Spanish DPA as regards whistle-blower hotlines.

Data Controllers must inform employees about: the existence of the whistle-blower hotline and how it works.

Subject to certain exceptions, reported persons should be informed of the facts outlined by Opinion 1/2006 of the Article 29 Working Party, namely, among others:

- the entity responsible for the whistle-blower hotline;
• the facts surrounding the accusation;
• the departments or services which might receive the report within its own company or in other group companies; and
• how to exercise rights of access, rectification, cancelation, and objection.

Due to the novelty and complexity of a whistle-blower hotline and the sensitivity of the rights affected, there is no absolute guarantee from the Spanish DPA that even if the scheme is based on Opinion 0128/2007 of the Spanish DPA and Opinion 1/2006 of the Article 29 Working Party, it will be accepted without any further comments and/or amendments.

The Spanish DPA has traditionally required the identification of the whistle-blower, so anonymous reports were not accepted. This was contradictory with Opinion 1/2006 of Article 29 Working Party, which allows the filing of anonymous reports as an exception to the general rule (i.e., identified reports), in so far as anonymous reports are not expressly promoted. The new Data Protection Draft Bill expressly permits anonymous whistle-blower hotlines in Spain.

18. E-Discovery
When implementing an e-discover system, an organization may be required to obtain the valid consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of such system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into operations, an organization may be required to inform employees of monitoring policies being implemented in the workplace, and give employees the opportunity to review isolated emails designated as spam.

20. Cookies
On 29 April 2013, the Spanish DPA, together with industry representatives Adigital, Autocontrol, and IAB, published the Guide for the Use of Cookies in Spain (the “Guide”). The document provides guidance for compliance with the general rule on installing and/or using cookies, which requires foremost informing and obtaining the consent of the user.

The Guide identifies cookies that are exempt from compliance with the general rule. These are cookies used: (i) only to allow communication between the user and the network; or (ii) to provide strictly a service explicitly requested by the user, as well as “user-input” cookies, user authentication or identification cookies (for one session only) and security cookies, as well as
other technical cookies used by plugins, provided that these are the sole purposes of the use of such cookies.

Thus, the installation and use of any other types of cookies remain subject to the general rule of informing and obtaining the user’s consent. The Guide seeks to facilitate compliance with that rule by providing for the:

- **Duty to inform**: This entails providing clear and complete information regarding the use of cookies and their purposes/uses and how to revoke consent and remove cookies, making all this information available to users permanently (e.g., through a hyperlink to the Cookies Policy).

- **Duty to obtain consent**: This is the most controversial requirement since the legislation on cookies does not indicate whether the consent must be express or implied. The Guide states that it is always advisable to require users to mark a checkbox or click on an “I agree” button, since this can ensure that consent is properly obtained and will guarantee the provider’s ability to prove its compliance with the regulations on cookies. However, users will also be deemed to have provided their implicit consent if they keep browsing the website, provided that:
  
  i. users have performed a conscious and affirmative action;
  
  ii. users have been previously informed in an explicit, clear and unequivocal way as to the existence and purposes of the cookies used in the website; and
  
  iii. users are able to object to the use of cookies regardless of the potentially negative effects this may have on the browsing experience.

Therefore, owners of websites aimed at the Spanish market who have not already done so, should carry out a process for adopting these regulations by using this Guide as a reference. In this regard, we recommend from a practical point of view considering the implementation of the following measures:

- reviewing and classifying the different cookies used by the organization under the new rules provided for in this Guide, and determining the information and consent requirements applicable to each type of cookie used;

- modifying the information practices (entry page, banners, etc.) as well as the content of the information provided to the user (cookies notice, privacy policy, etc.); and

- modifying, if necessary, methods and procedures for obtaining consent for the use of cookies.
21. Direct Marketing

Spanish law allows marketing communications to be sent through the use of the Internet or other electronic means as long as said communications can be easily identified by the recipient as such and the person or company in whose name they are sent can be easily identified.

As a general rule, online marketing communications can only be sent to those recipients who have authorized it expressly. However, Spanish law also allows companies to send marketing communications to those clients with whom there is a previous contractual relationship, in which case the company may send advertising messages regarding products or services similar to those contracted by the client.

In any case, the provider must offer the recipient the possibility of opposing to the processing of their Personal Data for promotional purposes, both at the time of collection of the data and in each of the commercial communications addressed to the recipient.

Spanish law also obliges service providers to provide simple and free procedures so that recipients can revoke the consent they have previously provided. These rules are also applicable to the sending of marketing communications by means other than email (e.g.: mobile phone messaging service, apps, etc.).

Additionally, as mentioned in Section 1, in a recent report issued by the SDPA (Legal Report 0195/2017) it is considered that the data processing behind a marketing communication could be based on the legitimate interest of the controller when the actions are carried out by non-electronic means, the affected Data Subject is client of the entity and the products or services offered can be considered “similar” to those contracted by the client, under the upcoming GDPR scenario.
Sweden

Sten Bauer
Stockholm
Tel: +46 8 566 177 16
sten.bauer@bakermckenzie.com

Peder Oxhammar
Stockholm
Tel: +46 8 566 177 25
peder.oxhammar@bakermckenzie.com
1. Recent Privacy Developments

**Processing of crime-related Personal Data**

On 16 February 2016, the Supreme Administrative Court issued a judgment regarding the use of a technical solution intended to prevent persons from fueling cars at petrol stations without paying. Cars suspected of fueling without paying would be registered in a central database used by several companies to prevent such cars from fueling on credit at other petrol stations. As a general rule, only public authorities may process Personal Data relating to crime, suspicion of crime and criminal judgments. The representatives from the petrol industry who wanted to implement the technical solution had therefore applied to the Swedish Data Inspection Board (the “Board”) for an exemption from this prohibition. The Board did not grant an exemption and the case was challenged in courts until it was finally decided by the Supreme Administrative Court.

The Supreme Administrative Court found that the intended purpose of the technical solution did not justify the violation of privacy of the processing of Personal Data and that there were no legal grounds to grant an exemption from the general prohibition on processing of Personal Data related to crime. The Supreme Administrative Court stated that the privacy risks of a central database used by several companies were significant.

This is the first case where the Supreme Administrative Court has considered the possibility for an exemption from the prohibition to process Personal Data relating to crime. The case shows that even if there is a legitimate purpose for processing Personal Data relating to crime, the Supreme Administrative Court is likely to be restrictive when assessing whether or not an exemption should be granted.

**Decision Regarding Recording of Customer Service Telephone Calls**

On 10 May 2016, the Board issued decisions against telecom operators regarding the processing of Personal Data collected when recording calls made to the customer service department of the respective telecom operator. In both decisions the Board stated that the collection and processing of Personal Data in connection with customer service calls could be based on a weighing of the telecom operators’ interest against the privacy interests of the callers and that consent was not required. In both instances, however, the telecom operators did not provide sufficient information regarding the rights of the individual callers prior to the recording of the calls.

The Board ordered the telecom operators to provide information on the right to receive, once a year and free of charge, information about the Personal Data being processed by the telecom operators, the right to request correction of Personal Data and information about the applicable retention period for the Personal Data.
These decisions show that the Board is able to accept that calls are recorded for the purpose of internal training of customer service employees and for evidencing agreements entered into by telephone, provided that callers are provided with sufficient information about the Personal Data processing and the callers’ rights.

2. Emerging Privacy Issues and Trends

EU General Data Protection Regulation

The new EU General Data Protection Regulation (“GDPR”) will apply in Sweden from 25 May 2018. The Swedish Government has appointed a committee to assess and report on the changes required to current Swedish laws. The committee has issued its findings in a report. The report will be used as a basis for the changes required to be made to Swedish data protection law following the GDPR. In addition, the Board has issued general information regarding the GDPR.

3. Scope of the Law


Camera Monitoring Act (2013:460) ("CMA"), governing privacy and use of camera monitoring.


Credit Information Act (1973:1173), which contains privacy regulations in relation to credit information.


Patients’ Personal Data Act (2008:355), which governs the processing of Personal Data in the healthcare sector.

EU General Data Protection Regulation 2016/679 ("GDPR").

4. Key Privacy Concepts

a. Personal Data

The PDA and the GDPR apply to the processing of “Personal Data” being any information relating to an identified or identifiable living individual ("Data Subject"). The GDPR also applies to the free movement of Personal Data.
b. Data Processing

“Processing” is widely defined and covers any operation or set of operations performed on Personal Data, including, inter alia, collection, recording, organization, storage, transfer and deletion. The PDA applies to both manual and automated data processing. However, the processing of Personal Data in non-structured formats (e.g., in running text or the use of ordinary email programs), is subject to exemptions from many of the rules under the PDA, including the requirements set out with respect to the processing of Sensitive Personal Data and transfer of Personal Data to a country located outside of the EEA. Notwithstanding, the exceptions only apply if the processing does not give rise to any violation of the Data Subject's personal integrity.

Under the GDPR, the processing of Personal Data in non-structured formats will no longer be subject to any exemptions, as it is under the PDA. However, there are still certain specific situations when processing of Personal Data is subject to exemptions from the regulation.

c. Processing by Data Controllers and by Processors

The PDA and the GDPR apply to those persons who, alone or together with others, determine the purposes for which and the manner in which any Personal Data is processed (“Data Controller”).

The GDPR also applies to those persons who process Personal Data on behalf of the Controller (“Data Processor”).

d. Jurisdiction/Territoriality

The PDA applies to data processing activities carried out by Data Controllers established in Sweden as well as Data Controllers that are not established in the EEA but use equipment based in Sweden to carry out data processing activities (other than merely for the purpose of transit).

The GDPR applies to the processing activities of an establishment of a Controller or a Processor in the Union, regardless of whether the processing takes place in the Union or not. The GDPR also applies to the Processing of Personal Data of Data Subjects who are in the Union by a Controller or Processor not established in the Union, if the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the European Union; or (b) the monitoring of their behavior as far as their behavior takes place within the European Union.

e. Sensitive Personal Data or Special Categories of Personal Data

The PDA imposes additional requirements on the processing of Sensitive Personal Data – that is, Personal Data relating to race or ethnic origin, political opinions, health or sex life, religious or philosophical beliefs and membership
of a trade union. Specifically, the processing of Sensitive Personal Data is prohibited, unless certain conditions are met, including:

- the Personal Data has been made public by the Data Subject or the Data Controller obtains the explicit consent of the Data Subject (see Section 5(b));
- the processing is necessary to carry out the obligations and rights of the Data Controller in the field of employment law;
- the processing is necessary to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent;
- the processing is carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade union aim and provided certain conditions are met;
- the processing is necessary for the establishment, exercise or defense of legal claims;
- the processing is performed by a health care professional for certain purposes or under an obligation of secrecy within the medical advice or treatment area; or
- the processing is performed for research and statistical purposes, provided the public interest in the research or statistical project clearly outweighs the risk of undue violation of the Data Subjects’ integrity.

The PDA imposes additional requirements on the processing of personal identification numbers as well as Personal Data concerning violations of the law. In principle, it is, with a few exemptions, prohibited for any entity other than government authorities to process Personal Data relating to crime, suspicion of crime and criminal judgments. Personal identification numbers may be processed only when it is clearly necessary having regard to the purpose of the processing; the importance of a certain identification; or any other considerable reason.

Under the GDPR, the general rule is that processing of special categories of Personal Data ("Sensitive Data") is prohibited. This includes the same categories of Personal Data as the PDA as well as sexual orientation, genetic data and biometric data for the purpose of uniquely identifying a natural person.

Under the GDPR, the processing of such Personal Data is allowed under certain circumstances. These exemptions from the general rule include but are not limited to, processing that is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of
the Data Subject in the field of employment and social security and social protection law, or if the Data Subject has given explicit consent (provided Member State law does not exclude such consent). Member States may also maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

f. Employee Personal Data
Employee Personal Data is likely to include both non-Sensitive Personal Data and Sensitive Personal Data (e.g., health-related information). Sensitive Employee Personal Data may be processed under the circumstances mentioned in Section 4(e) above, commonly for the purpose of carrying out the Data Controller’s obligations in the field of employment law. Non-sensitive Employee Personal Data may be processed by a Data Controller for purposes that are necessary in order to maintain and administer the employment relationship (e.g., performing a contract to which the Data Subject is a party, or carrying out the Data Controller’s legal obligations). Other justifications for processing non-Sensitive Employee Personal Data may include purposes which are of legitimate interest of the Data Controller and which are considered to be of greater weight than the Data Subject’s interest in his or her protection of the personal integrity. A fallback justification for processing both sensitive and non-Sensitive Personal Data in the employment context may be if consent is provided by the Data Subject. However, there are limitations on what is considered to constitute valid consent in the employment context (see Section 5(d) below).

Under the GDPR, Member States may, by law or by collective agreements, provide for specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ Personal Data in the employment context, inter alia for the purposes of the recruitment, the performance of the contract of employment, management, equality and diversity in the workplace, health and safety at work, and for the purpose of the termination of the employment relationship. Those rules shall include suitable and specific measures to safeguard the Data Subject’s human dignity, legitimate interests and fundamental rights.

5. Consent
a. General
As a general rule, Personal Data may be processed only if the Data Subject gives consent. There are a number of exceptions to this requirement, which legitimize processing without the consent of the Data Subject. Nevertheless, consent is, in practice, often one of the more straightforward ways of justifying processing. Written consent is not required. However, it is worth noting that, when in dispute, it is the Data Controller that is required to demonstrate that consent has been obtained. There is no language requirement set out in the PDA. However, the Board requires that all information provided to Data
Subjects regarding consent of processing Personal Data shall be translated into Swedish. If the Data Subject is proficient in the alternative language, it could nevertheless be argued that a translation is unnecessary. Under the GDPR the request for consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. The Data Subject's consent must also be freely given, specific, informed and an unambiguous indication, stated or given by a clear affirmative action, that signifies the Data Subject agreement to the processing of Personal Data relating to him or her.

b. Sensitive Data
Where consent is relied upon to justify the processing of Sensitive Data, it must be explicit. Written consent is not expressly required but may be preferable in order to prove that consent has in fact been obtained.

c. Minors
Although the PDA does not expressly regulate the Data Subject’s right to consent to the processing of his or her Personal Data, it is generally accepted that persons having reached the age of 15 years normally can provide valid consent. However, the situation must be assessed on a case-by-case basis. Valid consent is usually determined based on whether or not the Data Subject is capable of understanding the implications and effects of the consent, depending on, inter alia, the Data Subject’s age, the purpose of the processing and the Personal Data to be processed. If a Data Subject who is a minor is not considered to be able to give valid consent, a parent or legal guardian must provide consent on the Data Subject's behalf.

Under the GDPR, in relation to the offer of information society services directly to a child, consent given by the child to the processing of its Personal Data shall be valid only where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The Controller must make “reasonable efforts” to verify that a parent or guardian has provided the appropriate consent. Member States may set a lower age for those purposes, but not lower than 13 years. It is not yet decided what age will be set for Sweden, but the committee has suggested the stipulated minimum of 13 years.

d. Employee Consent
The Board has produced an opinion on the processing of Personal Data in the employment context. The Board's view is that consent is not freely given where there is a real or a potential prejudice arising from not consenting or where there is no real possibility for the employee to refuse to give his or her consent. The Board goes on to state that if an employee is genuinely able to withdraw his or her consent at any time without suffering any detriment, this is an indication that the consent is freely given.
The GDPR expressly states that, where there is an imbalance of power between the Data Subject and the Controller, consent will not be valid (for example between employer and employee). This means that it will be difficult for employers to rely on consent to process employees’ Personal Data under the GDPR. However, consent is only one of a number of potential legal bases for processing employees’ Personal Data. As an example, processing can be lawful where it is necessary for the performance of a contract to which the Data Subject is party. An employer may legally process Personal Data about employees necessary to fulfill the employment contract.

e. Online/Electronic Consent

Consent may be given electronically and will be considered to have been sufficiently demonstrated where it can be shown that the Data Subject had sufficient notice of the requisite information forming the basis of consent (e.g., inclusion of a hyperlink to a notice or policy directly above a consent button) and steps have been taken to prevent consent from being mistakenly given (e.g., a double click acceptance process). Note that guidance has not been issued on the interrelated issue of how to verify that it is the correct Data Subject who consents to the processing. The GDPR presents examples of how consent may be given by electronic means. This could include, inter alia, ticking a box when visiting a website or another statement or conduct which clearly indicates the Data Subject’s acceptance of the proposed processing. Pre-ticked boxes should not therefore constitute consent. If the Data Subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity, the purposes for collecting Personal Data, its privacy practices (which must be given in a clear and transparent way), third parties to which the organization will disclose the Personal Data, the consequences of not providing consent, the rights of the Data Subject, where the Personal Data is to be transferred and stored, how to contact the privacy officer or other individual who is accountable for the organization’s policies and practices, how to make an inquiry or file a complaint, and how to access/and or correct the Data Subject’s Personal Data.

The GDPR states that the Controller also shall provide the Data Subject with specific types of information when Personal Data is obtained, such as the contact details of the Controller and, where applicable, of the Controller’s representative and of the Data Protection Officer (see Section 10), the purpose and legal basis for the processing, the recipients of the Personal Data, if the Controller intends to transfer Personal Data to a third country or
international organization, the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period and where applicable, the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability and other rights of the Data Subject, as well as the right to lodge a complaint with a supervisory authority.

7. Processing Rules

An organization that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize personal information once the stated purposes have been fulfilled and legal obligations met.

The GDPR also regulates that processing shall be done in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. Rights of Individuals

Data Subjects have the general right to: be informed by an organization of the Personal Data the organization holds about the Data Subject, be informed by an organization of how the Data Subject’s Personal Data is being processed, request the correction of the Data Subject’s Personal Data, and request the deletion and/or destruction of the Data Subject’s Personal Data.

In comparison to the PDA, the rights of the Data Subjects are strengthened, enhanced and specified under the GDPR. The regulation gives Data Subjects among other rights, the right to information, access, rectification and erasure, restriction of processing, data portability, as well as the right to object.

9. Registration/Notification Requirements

Under the PDA, the Controller is subject to a general notification duty to the Board regarding the Personal Data processing activities performed by the Controller. The notification shall be made on a special form in Swedish, but the information to be provided is not very detailed. There are certain exemptions from the notification duty, i.e., (i) valid consent to the processing is obtained; (ii) a Data Protection Officer has been duly appointed (see Section 10); or a certain record on the Personal Data processing activities is held by the Controller (not applicable to Sensitive Personal Data).

The GDPR does not contain a general notification duty. Such a duty has instead been replaced by procedures and mechanisms which focus on those
types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes.

10. Data Protection Officers

Under the PDA, it is not mandatory to appoint a Data Protection Officer (“DPO”), but some Controllers do so in lieu of notifying the Board (see Section 9) and/or to get some support and point of contact with respect to the Personal Data activities. The DPO shall be (i) sufficiently familiar with Swedish data privacy laws; and (ii) independent of management. It is recommended by the Board (but not legally required) that the DPO speaks Swedish and lives in Sweden. The DPO does not need to be employed by the Controller. The Controller shall notify the Board of the DPO appointment on a specific form in Swedish.

Under the GDPR, the Controller and the Processor shall appoint a Data Protection Officer in any case where (i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity, (ii) the core activities of the Controller or the Processor consist of processing operations which require regular and systematic monitoring of Data Subjects on a large scale; or (iii) the core activities consist of processing on a large scale of Sensitive Personal Data and Personal Data relating to criminal convictions and offenses. The GDPR lists the minimum requirement of tasks that a DPO should have. The DPO shall directly report to the highest management level of the Controller or the Processor and should also be provided with the resources necessary to carry out the tasks of the DPO as well as be provided access to Personal Data and processing operations, and to maintain his or her expert knowledge.

11. International Data Transfers

Subject to the specific exceptional authorizations below, Personal Data may not be transferred to third countries (i.e., countries outside the EEA) unless the destination country provides for “adequate protection” of the Personal Data and only if the Controller or Processor has provided appropriate safeguards, and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available, or pursuant to one of the following exceptions:

- the Data Subject has given his or her express consent to the transfer;
- the transfer is for the performance of a contract between the Data Subject and the Data Controller of Personal Data or the implementation of pre-contractual measures taken due to a request of the Data Subject;
• the transfer is for the conclusion or performance of a contract between the Data Controller and a third party which is in the interest of the Data Subject;

• the transfer is for the establishment, exercise or defense of legal claims; or

• the transfer is for the protection of vital interests of the Data Subject

The GDPR has the same exceptions as the PDA, but adds the following exceptions:

• the transfer is necessary for important reasons of public interest;

• the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;

• the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Transfers of Personal Data from Sweden to recipients in the United States that are certified under the EU-US Privacy Shield arrangement are generally permitted, since these recipients are considered as providing adequate protection. Moreover, the use of a data transfer agreement incorporating the model clauses adopted by the European Commission will legitimize a transfer of Personal Data to non-EEA countries without adequate protection. Prior notification of the agreement to the Board is not required. Another alternative which will legitimate a transfer of Personal Data is if binding corporate rules are implemented. However, this alternative is normally fairly time consuming.

12. Security Requirements

Organizations are required to: take steps to ensure that Personal Data in its possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

The GDPR lists measures that shall be taken to ensure a level of security, including inter alia as appropriate:

• the pseudonymization and encryption of Personal Data;
• the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
• the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
• a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13. Special Rules for Outsourcing of Data Processing to Third Parties

A transfer of Personal Data must as a general rule be necessary for the purpose of the processing. Organizational, cost efficiency, and security reasons are normally viewed as acceptable reasons for a transfer of Personal Data due to outsourcing. Although the Personal Data processing is outsourced, the Controller remains responsible for the processing activities. Consequently, the Controller must make sure that the provisions under the DPA and other related regulations are complied with, both by the Controller but also by the third-party service provider. The third-party service provider and its sub-processors (if any) are viewed as Processors, implying that the written processor agreement obligation would be triggered (see Section 7). Moreover, should Personal Data be transferred to a country located outside of the EEA, the Controller must make sure that any of the exceptions to the general prohibition on transferring Personal Data to a third country applies or that another acceptable measure for the transfer has been taken (see Section 11). The Controller may be obliged to provide the Data Subjects with information about the transfer of their Personal Data.

The GDPR imposes direct compliance obligations on both Data Controllers and Data Processors, and both will face direct enforcement and penalties if they do not comply with the GDPR.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

Under the GDPR, fines will be significant with maximum fines amounting to up to EUR 20,000,000 or up to 4% of the company’s total worldwide annual turnover of the preceding financial year, whichever is higher.

15. Data Security Breach

The PDA is somewhat unclear in this respect and there are no specific statutory provisions regulating the subject matter, but according to the Board,
the Controller shall normally inform Data Subjects of the breach. The information shall, inter alia, include details about the anticipated effects of the breach. Moreover, the Controller shall inform other institutions that might be affected, (e.g., banks). There is no obligation to notify the Board. However, if large numbers of people are affected, it might be advisable to contact the authority.

An organization that is involved in a data breach situation may be subject to closure or cancellation of the file, register or database; an administrative fine, penalty or sanction; civil actions and/or class actions; and/or criminal prosecution.

Under the GDPR, in the event of a Personal Data breach, Controllers must notify the supervisory authority of the Member State where the Controller or the Processor has its main establishment or only establishment not later than 72 hours after having become aware of the breach. A notification is not required if the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. There is also a requirement for Processors to notify the Controller without undue delay after becoming aware of a Personal Data breach.

Controllers must also notify any affected individuals if (i) the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons or (ii) if the supervisory authority requires the Controller to do so.

The Controller must communicate the Personal Data Breach to the affected individuals without undue delay.

16. Accountability

Organizations are required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data, and, upon request, furnish the results of the privacy impact assessments and/or evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data. A single assessment may address a set of similar processing operations that present similar high risks.

17. Whistle-Blower Hotline

There is no filing requirement for the introduction of a whistle-blower hotline, but certain limitations with respect to the use of the whistleblower hotline apply. Moreover, the ordinary notification duty according to PDA applicable
with respect to the normal course of processing of Personal Data will still apply (see Section 9).

18. E-Discovery

It is generally permissible to process Personal Data for the individual control of employees’ use of email and Internet for the purposes of litigation or regulatory requests, provided that the Controller complies with the rules of the PDA or the GDPR. Further, employers must provide employees with detailed information about: the implementation of the e-discovery system, the purpose of the processing, the monitoring of work tools (e.g., email, Internet), and the storage of inter alia emails. In general, employers are not entitled to review and process any of the employees’ private information. According to the Board, it is advisable to implement an Internet-policy that contains guidelines for the employee use of Internet and email.

19. Anti-Spam Filtering

Generally, the introduction of a spam filtering solution in an organization does not raise privacy issues provided the employees have agreed to the spam filtering solution or have the possibility to access the emails that have been filtered. However, the individual control of such a spam filtering system will raise privacy issues (see Section 17).

20. Cookies

There are specific laws/rules that regulate the deployment of cookies, and hence, the use of cookies must comply with data privacy laws. Consent of Data Subjects must be obtained before cookies can be used. Further guidance regarding the requirement for consent and information requirements in connection with the use of cookies is expected to be issued by the Swedish Post and Telecom Authority by the end of 2016 or beginning of 2017.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond.

Under the GDPR, where Personal Data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to processing of Personal Data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.
Switzerland

Alessandro Celli
Zurich
Tel: +41 44 384 13 66
alessandro.celli@bakermckenzie.com

Muriel Binder
Zurich
Tel: +41 44 384 14 27
muriel.binder@bakermckenzie.com

Markus Winkler
Zurich
Tel: +41 44 384 13 01
markus.winkler@bakermckenzie.com
1. Recent Privacy Developments

Data protection and privacy is increasingly becoming the subject of litigation in Switzerland. In the past year, Swiss courts have seen quite a few cases on the subject of data protection and privacy.

As in previous years, several lower courts, as well as the Federal Supreme Court, have had to deal with cases involving Swiss banks aiming to disclose Personal Data to the US Department of Justice in connection with tax investigations pending in the US. The Zurich High Court, for example, ruled that Personal Data disclosures to governmental authorities in the US could not be justified by an overriding public interest unless the bank desiring to disclose the data is systemically relevant to the Swiss banking system. This decision was now confirmed by the Federal Supreme Court.

In another case the Federal Supreme Court had to deal with a large online Data Processor. The platform in question is gathering and publicizing Personal Data on its website and runs creditworthiness checks for registered users. The Court ruled that it is reasonable, when a large number of personal profiles are processed, to verify the accuracy of its data in a ratio of 5% of the queries made on the platform. In order to insure the safety of the processed data they may not simply rely on the reasons brought forward by the person submitting a request for credit analysis, but have to properly verify the legitimacy of his or her interests in a ratio of 3% to the queries made on the platform concerned. Furthermore, the Court decided, that if the platform cannot answer information requests regarding its data processing itself, it must forward such requests to its business partner concerned in the matter.

In a further case, the Federal Supreme Court ruled that the commercial collection and transmission of private addresses (being Personal Data) to third parties qualifies as data processing. Such a data processing must be registered with the Federal Data Protection and Information Commissioner. The Data Controller is further obliged to implement a process to inform, adjust and delete such Information on request by a Data Subject.

In the last case discussed here, the Court reviewed the legality of an internal “watchlist” kept by the Swiss financial market regulator FINMA as an inventory of persons who may not be deemed adequate to serve on executive positions of FINMA supervised entities. The Court qualified data in this watchlist as personality profiles, the processing of which requires a formal legal basis. The Court found such legal basis in the Federal Act on the Swiss Financial Market Supervisory Authority and ruled that the watchlist was in principle compatible with the law. However, in this case, the collected Information was found not to be sufficiently reliable.
2. Emerging Privacy Issues and Trends

In September 2017, the new draft for a completely revised Federal Law on Data Protection ("FLDP") was published together with the explanatory message by the Federal Council. The revision is triggered by EU General Data Protection Regulation ("GDPR"), the pending amendment of the Convention 108 of the Council of Europe as well as the technological and social progress.

The new FLDP incorporates privacy by design as well as privacy by default concepts. The static notion of a "data file" will be replaced by the dynamic concept of profiling, in line with the GDPR concept. The obligation to register certain critical data files with the Federal Commissioner for Data Protection and Information will be removed. Instead, Data Processors may appoint a data processing officer who has to maintain a directory of data processing activities. This draft also introduces the concept of an impact assessment which has to be conducted when data processing may involve a high risk for the personality or fundamental rights of the Data Subjects concerned. In cases of data security breaches the draft proposes a notification obligation. Lastly, the Swiss particularity of extending the notion of Data Subject to legal entities will be abolished. Many of these concepts reflect changes being introduced by the GDPR in Europe.

On 10 January 2018, the Federal Council adopted a phased approach for introducing the new FLDP. In a first phase, the act shall be amended to the extent necessary to allow for an adequacy decision the by European Commission in view of the GDPR, in order to safeguard the Swiss economy’s competitiveness in its dealings with the EU. The second phase will look at additional improvements. At this point in time it is not clear yet when the new act will come into force.

3. Law Applicable

The Federal Law on Data Protection of 14 June 1993 ("FLDP") together with its implementing ordinance ("Ordinance").

The FLDP and the implementing Ordinance were substantially revised in 2007. The revised provisions entered into force on 1 January 2008. Besides delivering greater transparency through stricter information obligations regarding Sensitive Personal Data and Personality Profiles, the revision resolves some existing contradictions in the language and also introduces some incentives for self-regulation. Switzerland is not subject to the European Union’s General Data Protection Regulation ("GDPR"). The GDPR may still apply to certain specific situations where Swiss entities are involved in processing data of Data Subjects domiciled in a EU member state.
4. Key Privacy Concepts

a. Personal Data
The FLDP applies to the processing of any information (“Personal Data”) relating to an identified or identifiable legal person or natural person (“Data Subject”).

b. Data Processing
“Processing” is broadly defined in the FLDP and includes all acts relating to Personal Data, regardless of the equipment and procedures used, in particular, the collection, storage, use, modification, disclosure, archiving or destruction of Personal Data. The FLDP applies to both automated and manual data processing.

c. Processing by Data Controllers
The FLDP applies to those persons who determine the purposes for which and the manner in which any Personal Data is, or is to be, processed (“Data Controller”).

d. Jurisdiction/Territoriality
The FLDP applies to Data Controllers domiciled in Switzerland, and the processing of Personal Data pertaining to Data Subjects domiciled in Switzerland.

e. Sensitive Personal Data
The FLDP imposes additional requirements for the processing of Sensitive Personal Data – that is, Personal Data concerning religious, philosophical, political or union opinions or activities; health, sexuality or racial origin; social security files; and criminal or administrative proceedings and sanctions. In addition, special rules apply to “personality profiles”. A personality profile is a collection of Personal Data that allows for the appraisal of the essential characteristics of an individual's personality (“Personality Profile”).

The amended FLDP provides an obligation to register data collections with the Data Protection Commissioner if (i) the Data Controller regularly processes Sensitive Personal Data or Personality Profiles, or (ii) it regularly discloses Personal Data to third parties (including other group companies). By way of exception, the Data Controller will not have to register if (among other things) it has appointed an internal data protection commissioner who independently supervises the compliance with the data protection legislation and who keeps a register of all data collections. Therefore, by appointing an internal data protection commissioner, the Data Controller can avoid having to register under the amended laws.

The processing of Sensitive Personal Data is prohibited unless justified by the consent of the Data Subject, an overriding public or private interest, or the law
(see Section 7 below). These criteria will be applied in a stricter manner if there are Sensitive Personal Data or Personality Profiles involved. The revised law introduces the obligation of the Data Controller to actively inform Data Subjects about the collection of Sensitive Personal Data or Personality Profiles. This information must at least cover the identity of the Data Controller, the purpose of the processing, and the categories of recipients of the Personal Data (if it is intended to disclose the Personal Data to third parties).

f. Employee Personal Data
Employee Personal Data is likely to include Sensitive Personal Data (e.g., health-related information) and non-Sensitive Personal Data. The processing of Employee Personal Data, whether sensitive or non-sensitive, will be justified if required to implement an employment agreement. Other justifications may be invoked under certain circumstances.

5. Consent Requirements

a. General
The consent of the Data Subject is not mandatory, although it is contemplated as a justification for the processing (see Section 7 below) as well as cross-border transfers (see Section 11 below) of Personal Data. In practice, it is often one of the more reliable ways to justify any data processing. Written consent is not required but is recommended for evidential purposes.

b. Sensitive Data
The FLDP does not distinguish between Sensitive and non-Sensitive Personal Data as regards consent requirements. However, a court may in practice apply stricter criteria to the consent language required for the processing of Sensitive Personal Data than for the processing of non-Sensitive Personal Data. The revised law requires the explicit consent of the Data Subject if the processing involves Sensitive Personal Data or Personality Profiles.

c. Minors
Persons under the age of 18 cannot give valid consent. A parent or legal guardian must give consent on their behalf.

d. Employee Consent
An employee’s consent will be valid only if it is freely given prior to the processing of the Personal Data. This requirement will not be fulfilled if consent is given by the employee to avoid a real or potential prejudice which could arise from not consenting, where there is no real possibility of the employee refusing to consent, or where the consequence of refusal is that a candidate will not be offered employment. Where the employee or the candidate is entitled to withdraw its consent at any time without suffering any detriment, this is an indication that consent is freely given. An employee’s
consent can be given explicitly or tacitly. A tacit consent will not suffice if the processing involves Sensitive Personal Data or Personality Profiles. The majority of the Swiss doctrine sees a consent given by an employee to his employer to collect and work with data which is not strictly relevant for the employment relationship as not freely given and therefore as invalid.

e. **Online/Electronic Consent**
Consent may be given electronically, and will be considered to have been sufficiently demonstrated where it can be shown that the Data Subject had sufficient notice of the requisite information forming the basis of consent (e.g., inclusion of a hyperlink to a notice or policy directly above a consent button) and steps have been taken to prevent consent from being given mistakenly (e.g., a double click acceptance process).

6. **Information/Notice Requirements**
An organization that collects Personal Data must provide Data Subjects with information about: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) its privacy policies (which must be given in a clear and transparent way); (v) third parties to which the organization will disclose Personal Data; (vi) where the Personal Data is to be transferred; (vii) how to contact the privacy officer or other person who is accountable for the organization’s policies and practices; (viii) how to make an inquiry or file a complaint; (ix) and how to access and/or correct the Data Subject’s Personal Data.

7. **Processing Rules**
An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected; and delete/anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

8. **Rights of Individuals**
Data Subjects have the general right to: (i) access the Data Subject’s Personal Data, subject to some restrictions and/or qualifications; (ii) request the correction of the Data Subject’s Personal Data; and (iii) request the deletion and/or destruction of the Data Subject’s Personal Data.

9. **Registration/Notification Requirements**
An organization that collects and processes Personal Data may be required to register, and notify the appropriate data authority. See Section 4(e) for the obligation to register data collections with the Data Protection Commissioner under certain circumstances.
10. Data Protection Officers

In Switzerland, there is no requirement to appoint or designate a data protection officer or other individual who will be accountable for the privacy practices of the organization.

11. International Data Transfers

Personal Data may not be transferred abroad if such transfer could put Data Subjects at risk. The reputation of the persons affected will be particularly put at risk if the data is transferred to countries that fail to provide a level of protection equivalent to the level provided under Swiss law. The Swiss Federal Data Protection and Information Commissioner keeps a list of countries deemed to provide an equivalent level of protection. The EU member states are included in this list. The revised law introduces a catalogue of reasons which justify the transfer of Personal Data to countries that lack an adequate level of data protection. This catalogue is exhaustive, i.e., the transfer of Personal Data to such countries is only lawful if one of the reasons for justification is fulfilled. In order to prevent putting the persons concerned at risk, the Data Controller can, for instance, require the data recipient to sign a data transfer agreement or obtain the Data Subject’s consent to the transfer.

An organization may transfer Personal Data outside of the jurisdiction, provided that: appropriate data transfer agreements (i.e., Model Contractual Clauses) or other prescribed measures are put in place; binding corporate rules (“BCRs”) are implemented to secure international data transfers; or recipients in the US are registered under the Swiss-US Privacy Shield established in 2017.

12. Security Requirements

Organizations are required to: (i) take steps to ensure that Personal Data in its possession and control is protected from unauthorized access and use; (ii) implement appropriate physical, technical and organization security safeguards to protect Personal Data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties may potentially be required to use contractual or other means to protect the Personal Data. There may be additional obligations for specific sectors. In case of the occurrence of a data breach, the outsourcing organization will be held liable together with the third-party provider.
14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

There is currently no explicit general provision in the FLDP that would require a Data Controller to notify a data security breach to Data Subjects or the Federal Commissioner for Data Protection and Information. The proposed draft new FLDP now includes such an obligation dependent on the likely risks involved for the Data Subject.

Under current law, organizations that have suffered a data security breach must determine on their own whether and what kind of action to take in response to the breach. The organization must, therefore, decide on a case-by-case basis whether to voluntarily notify in the event of a data security breach. To that end, the organization may seek guidance from the competent authorities on an informal basis. There is no formal procedure for informal consultations with the authorities.

This decision on whether or not to notify may depend on the nature of the data concerned. While Swiss laws do not formally distinguish between sensitive and non-sensitive information in connection with data security breaches, it is important to highlight that statutory requirements are applied more strictly if sensitive data is involved. A notification is more likely to be recommended if sensitive data is affected by the data security breach.

The organizational impact of a data security breach that becomes public can be manifold. The security breach can trigger an investigation by the Federal Data Protection and Information Commissioner. Violating data protection obligations may also result in civil liability. The Data Subject may sue the organization for correction, cease and desist, deletion, and damages covering financial losses or lost profits incurred by the Data Subject. The damages depend on the actual losses and lost profits proved by the Data Subject. In very exceptional cases, the Data Controller may be obliged to pay a satisfaction amount to the Data Subject to compensate immaterial damages. Finally, data security breaches and investigations frequently entail a lot of negative publicity and, therefore, cause reputational harm.

16. Accountability

There is no existing law in Switzerland that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. However, the new draft FLDP requires organisations to conduct an impact assessment
in cases where data processing may involve a high risk for the personality or fundamental rights of the Data Subjects concerned. So, impact assessments may well be required in Switzerland in the near future. It is also not a requirement to furnish evidence relating to the effectiveness of the organization’s privacy management program to privacy regulators.

17. Whistle-Blower Hotline

No filing requirement is required other than the regular data protection filings, provided that the criteria for such filing are met.

18. E-Discovery system

There are no requirements that apply other than the general legal requirements under the Swiss data protection law and, potentially, labor law.

19. Anti-Spam filter

There are no requirements that apply other than the general legal requirements under the Swiss data protection law and, potentially, labor law.

20. Cookies

The use of cookies must comply with data privacy laws. Some types of cookies that track or monitor the user may not be permitted.

21. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject's failure to respond. The organization may be required to obtain consent for a specific activity as bundled consent may not be considered valid consent.
Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang@bakermckenzie.com

Chris Tsai
Taipei
Tel: +886 2 2715 7310
chris.tsai@bakermckenzie.com

Louis Hsieh
Taipei
Tel: +886 2 2715 7308
louis.hsieh@bakermckenzie.com
1. Recent Privacy Developments

The Personal Data Protection Act (the “PDPA”) of 2010, which replaced the previous Computer-Processed Personal Data Protection Law of 1995 and became fully effective in 2012, has redefined the landscape of data protection regulations in Taiwan. The PDPA applies to both public and non-public institutions. Regulated institutions are required to notify and obtain the Data Subject’s prior consent in order to process Personal Data, subject to the exemptions provided by law. In addition, these institutions must have a predefined purpose for collecting such data.

An amendment to the PDPA, which involves 12 existing articles, was published on 30 December 2015 and became effective on 15 March 2016 (the “Amendment”). The main purpose of the Amendment is to relax certain regulations relating to a Data Subject’s consent based on recent law practices. There is also an increasing trend of non-public institutions implementing the “Personal Data File Security Maintenance Plan” as an internal regulation subject to the guidelines provided by the competent authorities.

2. Emerging Privacy Issues and Trends

Overhaul of Taiwan’s Data Protection Law

Compared to its predecessor, the PDPA of 2010 has significantly strengthened the Personal Data protection laws in Taiwan and has already changed the ways in which Personal Data can be collected, processed, stored, used and transmitted.

Under the PDPA, Data Collectors are required to give affirmative notice to the Data Subjects whose Personal Data they collect and must advise them of the purposes for which their Personal Data is being collected or used, as well as the sources from which the data is derived.

The PDPA also provides for civil and administrative liabilities and even criminal liabilities if individuals or enterprises misuse and profit from the collection, processing or use of Personal Data.

As the PDPA had been criticized for being too strict in terms of obtaining written consents, the Amendment allows consent to be given not only in writing (except for Sensitive Personal Data) but also electronically or orally. It also allows consent to be presumed under specific conditions. Unlike the previous version of the PDPA, Sensitive Personal Data is now subject to the Data Subject’s self-autonomy so that its collection, processing and use can be authorized by the Data Subject’s prior written consent. Furthermore, the Amendment also extends the scope of exemptions for both public and non-public institutions in terms of prior notification requirements and use of Personal Data outside the designated scope.
Personal Information File Security Maintenance Plan for Non-Public Institutions

Article 27 of the PDPA requires non-public institutions to adopt proper security measures in retaining Personal Data. Competent authorities are also encouraged to provide the “Personal Data File Security Maintenance Plan” (“Maintenance Plan”) and the “Rule for Management of Personal Data after the Completion of the Business” as guidelines for respective industries. Since the implementation of the PDPA, various institutions have already implemented their respective rules for the Maintenance Plan, including those in the following industries: multi-level marketing, human resources, real estate, water corporations, hotel and tourism, and financial institutions regulated by the Financial Supervisory Commission (the “FSC”) (including financial holding companies, the banking industry, securities industry, futures industry, insurance industry, institutions that engage in electronic stored value cards, or foundations that are under the FSC regulations). Each enterprise under the respective industries shall adopt the proper security measures in retaining the collected Personal Data and report to the competent authorities for record. It is foreseeable that it will become a common practice for companies to implement such a Maintenance Plan.

Data Protection Enforcement

Since the implementation of the PDPA on 1 October 2012, we have seen a number of cases resolved against public and non-public institutions which resulted in the imposition of civil liabilities, administrative penalties and even criminal responsibilities pursuant to the PDPA. Meanwhile, the FSC has imposed fines on various financial institutions, including banks and insurance companies for violating the data protection requirements pursuant to their respective regulations, such as the Banking Act and the Insurance Act. Given that the financial industry is a highly regulated industry, the penalties set forth in those applicable regulations are much higher than those in the PDPA. In addition, when it comes to data protection, finance-related statutes and regulations are special laws and thus prevail over the application of the PDPA as a general rule.

Anti-Spam Legislation

In February 2009, the government introduced an anti-spam bill called the Commercial Electronic Mail Management Act (the “Bill”). The Bill, which is still in the legislative process, defines unsolicited email or spam as email intended to market commercial products or services which are not based on an existing relationship between the sender and the recipient. The Bill seeks to reduce the burden of commercial emails by (i) introducing consumer consent and other requirements with which commercial email senders must comply, and (ii) giving spam recipients the right to recover damages.
Under this Bill, spam will be considered legitimate only if the recipient consents to receiving it. The law will authorize a sender (a legal entity, group or individual who initiates a commercial email) to send an initial unsolicited commercial email, provided the email is clearly marked as a commercial advertisement, contains the sender's name and business address, and gives the recipient an opt-in option to receive subsequent messages from the sender. The recipient’s failure to respond to the sender’s initial email constitutes the recipient’s refusal to receive the sender’s subsequent messages. The Bill will also prohibit most forms of randomly generated spam, including those that harvest email addresses derived from alpha-numeric searches.

If passed and promulgated as expected, the Bill will give spam recipients a right to recover NTD 500 to NTD 2,000 (approximately USD 17 to USD 69) from the sender for each unauthorized commercial email. It will also authorize class action lawsuits by authorized organizations on behalf of at least 20 persons. An early version of Taiwan’s proposed anti-spam legislation was criticized because it imposed heavy obligations on internet service providers by requiring them to implement specific measures to prevent commercial email abuses.

As of October 2018, this Bill is still under review by the commission of the Legislative Yuan. There are no new developments on the Bill or its proposed amendments.

3. Law Applicable

Specific data protection rules can be found in: (i) the constitutional right to privacy recognized by the Justices of the Constitutional Court, which protects an individual’s ability to control his or her own Personal Data, including control over whether to disclose Personal Data, the time, manner and scope of disclosure and the right to correct such information when it is wrongly stated; (ii) the PDPA, which, as a general rule, regulates all individuals and legal entities that collect, use or process Personal Data; and (iii) ancillary regulations under the PDPA, such as its Enforcement Rules, and other internal rules regarding personal information security promulgated by each government department.

The right of privacy or Personal Data protection is also represented in various laws and regulations in Taiwan, including:

- the Civil Code of Taiwan, which provides a private right of action for the tortious infringement of privacy;
- the Criminal Code, which penalizes certain types of privacy infringements, including eavesdropping, illegally opening sealed envelopes, and the unauthorized release of privileged medical, financial or legal information;
• the Freedom of Government Information Law, which prohibits the release of government information which would result in an invasion of personal privacy; and

• the Guidelines for Consumer Protection in E-Commerce, which apply to business operators in electronic commerce. While the Guidelines are not formal law, they may be legally enforced under the provisions of Taiwan’s Consumer Protection Law. They include guidelines for collecting, using and protecting consumers’ Personal Data.

4. Key Privacy Concepts

a. Personal Data
Under the PDPA, “Personal Data” means a natural person’s name, date of birth, national identification number, passport number, special features, fingerprints, marriage, family, education, occupation, medical records, medical history, genetic information, sex life, health examinations, criminal records, contact information, financial status, social activities, and other data sufficient to directly or indirectly identify that person.

b. Data Processing
The PDPA defines data processing as recording, inputting, storing, editing, amending, correcting, copying, retrieving, deleting, outputting, or transmitting Personal Data collected in order to create or use the personal profile of a Data Subject.

c. Processing by Data Controllers
The PDPA applies to public and non-public institutions, including all individuals, legal entities and enterprises that collect, use or process Personal Data.

d. Jurisdiction/Territoriality
The PDPA extends to:

• the collection, use or processing of Personal Data in Taiwan by all individuals, legal entities and enterprises (including Taiwanese and foreign individuals, legal entities and enterprises);

• the collection, use or processing of Personal Data of Taiwanese citizens by all individuals, legal entities and enterprises outside of Taiwan; and

• the international transmission of Personal Data by all individuals, legal entities and enterprises.

e. Sensitive Personal Data
The PDPA imposes stricter requirements for Sensitive Personal Data, including medical records and relevant information, genetic information, sex
life, health examinations and criminal records with a higher level of protection. These kinds of Personal Data are banned from being collected, processed or used, except under limited circumstances with security measures imposed both before and afterwards. Nevertheless, the Amendment has slightly relaxed the restrictions on the Data Subject’s written consent (please see 5(b) below).

f. Employee Personal Data
The PDPA treats Employee Personal Data the same way as other Personal Data. Labor laws also do not address Employee Personal Data.

5. Consent
a. General
Under the PDPA, public institutions may, but are not required to, obtain the Data Subject’s consent when they act within the scope of their official responsibility or when there is no likelihood of injury to the Data Subject’s rights and interests.

Under the PDPA, in principle and subject to certain exceptions, non-public institutions must (i) have a predefined purpose, and (ii) meet certain requirements prescribed by the law in order to process Personal Data.

With respect to the Guidelines for Consumer Protection in E-Commerce, business operators engaged in electronic commerce should obtain consumers’ consent before collecting or processing their Personal Data. Note that businesses should obtain parental consent before collecting, using or revealing to a third party any information containing the Personal Data of children under 12 or their family members.

b. Sensitive Data
Sensitive Personal Data, including medical records and relevant information, genetic information, sex life, health examinations and criminal records, is subject to a higher level of protection. These items of Personal Data are banned from being collected, processed or used except under limited circumstances with security measures imposed both before and afterwards. Nevertheless, the Amendment has slightly relaxed the restrictions by granting the Data Subject a right to, after being duly notified, authorize the collection, process or use of the Sensitive Personal Data by a prior written consent at his/her sole discretion.

c. Minors
Minors under the age of 20 cannot give valid consent, except with respect to normal routine matters within the everyday life of a minor. The parent or legal guardian of a minor may consent on behalf of the minor. A parent or legal
guardian may validate a contract made by a minor who has reached the age of seven but is under the age of 20.

d. **Employee Consent**
No special rules apply for employee consent. It is understood that employee consent is not required to carry out an employment contract or administer an employment relationship.

e. **Online/Electronic Consent**
Under the Amendment, Data Subjects’ consent is no longer limited to being in writing, except where a written consent is still necessary for the use of Sensitive Personal Data. Consent may be given electronically or even orally, while it is the data collector’s responsibility to take the burden of proof evidencing that the consent has been obtained in case of any dispute raised.

6. **Notice Requirements**
An institution that collects Personal Data must provide Data Subjects with information about the institution’s identity, the purposes for collecting Personal Data, third parties to which the institution will disclose the Personal Data, the consequences of not providing consent, the rights of the Data Subject, how to make an inquiry or file a complaint, how to access/and or correct the Data Subject’s Personal Data, and the duration of the proposed processing.

7. **Processing Rules**
An institution that processes Personal Data must limit the use of the Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected, and delete/anonymize personal information once the stated purposes have been fulfilled and legal obligations have been met.

8. **Rights of Individuals**
Data Subjects have the general right to access their Personal Data, subject to some restrictions and/or qualifications, request the correction of their Personal Data, and request the deletion and/or destruction of their Personal Data.

9. **Registration/Notification Requirements**
There is no registration requirement under the PDPA. When Personal Data is stolen, disclosed, altered or infringed as a result of a violation of the PDPA, the collector should notify the Data Subject.

10. **Data Protection Officers**
Under the PDPA, public institutions must designate personnel who are exclusively responsible for data protection. Non-public institutions must take
appropriate measures to prevent Personal Data from being stolen, amended, destroyed or disclosed.

11. International Data Transfers
Under the PDPA, the central competent authority may restrict international transmission of Personal Data by non-public institutions if:

- such transmission involves major national interest;
- such transmission is subject to special provisions of an international treaty or agreement;
- the receiving country lacks proper laws and regulations that adequately protect Personal Data, and the rights and interests of a Data Subject are likely to be injured/damaged; or
- the Personal Data is indirectly transmitted to a third country (area) to evade the application of the PDPA.

12. Security Requirements
Institutions are required to take steps to ensure that Personal Data in its possession and control is protected from unauthorized access and use, to implement appropriate physical, technical and institutional security safeguards to protect Personal Data, and to ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Institutions that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and comply with specific requirements subject to their business types. Institutions that outsource to third parties will be held liable together with the third parties in case of any breach by the latter.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach
Under the PDPA, public institutions and non-public institutions are obliged to notify the affected individuals by appropriate means in the event of a data security breach. Under the Enforcement Rules for the PDPA, “appropriate means” shall mean any method which can deliver the message to the affected
individuals, including written notice, telephone, facsimile, or electronic transmission. However, in the event that the costs may be substantial, public notice is allowed. The notice should contain how the data security was breached and the remedy already adopted.

An institution involved in a data breach situation may be subject to closure or cancellation of the file, register or database, an administrative fine, penalty or sanction, civil actions and/or class actions, or criminal prosecution.

16. Accountability
There is no requirement under the PDPA for institutions to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
Except for general complaints/petitions to the competent authority, Taiwan does not have any particular whistle-blower legislation.

18. E-Discovery
Taiwan does not have common law pre-trial discovery procedures (including e-discovery). There are requirements that evidence can be introduced at a certain stage of the trial process, but the e-discovery system is still in an experimental stage and is not widely used. Therefore, it would be prudent to obtain consent in advance or to specify in the employee’s handbook that the company may access Personal Data in the e-discovery process.

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, it is advisable for a company to provide in the employee’s handbook that company email accounts are for business purposes only and that the company may process or use the company email accounts for business-related purposes, including implementing a spam-filtering solution.

20. Cookies
There are no specific laws/rules that regulate the deployment of cookies in Taiwan.

21. Direct Marketing
An institution that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent, which cannot be inferred from a Data Subject’s failure to respond. Institutions must also provide a mechanism for the Data Subject to “opt out” of the marketing activities.
Thailand

Dhiraphol Suwanprateep
Bangkok
Tel: +66 02 636 2000 Ext. 4950
dhiraphol.suwanprateep@bakermckenzie.com

Pattaraphan Paiboon
Bangkok
Tel: +66 02 636 2000 Ext. 4568
pattaraphan.paiboon@bakermckenzie.com

Kritiyanee Buranatrevedhya
Bangkok
Tel: +66 02 636 2000 Ext. 4592
kritiyanee.buranatrevedhya@bakermckenzie.com
1. Recent Privacy Developments

Thailand does not yet have a consolidated general data privacy law, but is currently taking steps to enact one in the form of the Personal Data Protection Bill ("PDPB"). The PDPB, if passed, will be the first general data protection law in Thailand and, in its current draft form, a Data Subject’s consent is required before or at the moment of collection, use and disclosure of his/her Personal Data.

The background to the PDPB is that the Thai government initiated a digital economy plan to promote IT business and the digital environment in Thailand (the “Plan”). Pursuant to the Plan, the Thai Cabinet approved amendments to existing laws and new bills “in principle” between December 2014 and January 2015. The PDPB is part of the set of laws under the Plan.

Current laws and bills under the Plan are set out below:

- **Laws**
  - The Ministry, Department, and Bureau Reform Act (No. 17) B.E. 2559 (2016). This act reforms the Ministry of Information and Communications Technology into the Ministry of Digital Economy and Society, (“MDES”), which will be responsible for developments related to the digital economy.
  - The Digital Development for Economy and Society Act B.E. 2560 (2017). This act establishes the Committee for Digital Economy and Society, Digital Development Fund, and the Digital Economy Promotion Office to support and promote the Plan.
  - The Amendment to the Computer Crime Act (No. 2) B.E. 2560 (2017). This act revises the criteria for computer crimes and the power of the relevant officials under the Computer Crime Act.
  - The Amendment to the Organization to Assign Radio Frequencies and to Regulate Broadcasting and Telecommunications Businesses Act (No. 2) B.E. 2560 (2017). This act revises and supplements the licensing criteria for the allocation of radio frequencies. It also revises the power and duties of the National Broadcasting and Telecommunications Commission.

- **Bills**
  - The Draft Amendment to the Electronic Transactions Act. This act revises the criteria for conducting electronic transactions and revises the structure, power, and duties of the Electronic Transactions Commission.
o **The National Cybersecurity Bill.** This bill provides the criteria for ensuring cyber security and establishes a National Cybersecurity Committee (“NCSC”).

o **The Draft Amendment to the Royal Decree Establishing the Electronic Transactions Development Agency (Public Organization).** This amendment revises and supplements the powers and duties of the Office of Electronic Transactions Development Agency.

o **The PDPB.** Currently, the PDPB is being considered by the MDES. In January 2018, the MDES issued a new version of the PDPB and opened a public hearing. After the public hearing process is complete, the new PDPB will be forwarded to the Cabinet for approval before its submission to the National Legislative Assembly (the “NLA”) for further consideration. Once the NLA endorses the draft law, it will be sent to His Majesty the King for final approval before being published in the Government Gazette. There is no specific timeline indicating when the PDPB will be passed.

2. Emerging Privacy Issues and Trends

- **Mandatory Breach Notification**

Currently, there is no general requirement to notify any specific authorities of data breaches.

If the PDPB is passed in its current form, there will be requirements for breach notification imposed upon the Data Controller and Data Processor.

The Data Controller is required to notify the Data Subject of the breach incident immediately. If the breach affects a number of Data Subjects in excess of what is prescribed by the Personal Data Protection Committee, the Data Controller must also report the breach incident and remedial plan to the Personal Data Protection Committee immediately.

The Data Processor is required to notify the Data Controller of the breach incident.

In addition, there are requirements for specific industries. Under the Telecommunications Business Act B.E. 2544 (2001), telecommunications operators must notify affected users without delay in case of a breach of the Data Subject’s rights in relation to personal information, privacy, or the right to communicate through telecommunications.

- **Anti-spam Legislation**

the source or with a falsified source of origin which disrupts the peaceful use of the computer system (spamming).

The Computer Crime Act further prohibits sending computer data or emails to other persons in a manner that causes a disturbance to the recipient without allowing the recipient to easily opt out from receiving such data/emails (an opt-out option). A sub-regulation under the Computer Crime Act further prescribes the circumstances which are not deemed to cause a disturbance to recipients and where an opt-out option is required.

- **Cloud Computing**

There is no general legislation governing data privacy for cloud computing services at the moment, except for certain specific sectors.

- **Electronic Contracting**

The Draft Amendment to the Electronic Transactions Act, if passed in the current form, specifically prescribes the validity or enforceability of a contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems.

- **Electronic Signatures**

The Draft Amendment to the Electronic Transactions Act, if passed in the current form, will change the criteria of electronic signatures to be broader and focus on the intention of the electronic signature owner.

- **Cybersecurity**

The National Cybersecurity Bill will establish the NCSC as a central command center focusing on cyber terrorists and cyber attacks in Thailand and maintaining national security, military security, and economic stability in the cyber world.

Under the bill, the NCSC is entitled to request private entities to act or not to act, and notify the NCSC if there is a cyber attack that may affect the financial stability, commerce, or national security. Furthermore, it empowers the NCSC, with a court order, to access any communications information or proceed with any proper measures for the benefit of national cybersecurity, and to suppress any future damage. However, in the event of an emergency, the official, with approval of the NCSC, can request any data from private entities without a court order.

Currently, in the absence of cybersecurity law, the Office of the Prime Minister Regulations Re: the National Cybersecurity Preparation Committee B.E. 2560 (2017) has been issued as temporary guidance to prepare the necessary infrastructure for the development of cybersecurity. It will automatically be repealed once the National Cybersecurity Bill becomes effective.
3. Law Applicable

The right to privacy has long been recognized in the Thai legal system. As such, a person shall have the right to be afforded protection against undue exploitation of his or her Personal Data, as provided by law. In the absence of a general data protection law in Thailand, the most relevant law relating to data privacy available at the moment would be the law of wrongful act (tort).

Theoretically, any violation of the Constitution that results in damage to others may constitute a wrongful act (a tort) under the Thai Civil and Commercial Code. However, to date, no court decision that interprets the provisions of the Constitution in this light has been issued.

In addition to the above, the use and/or transfer of certain types of Personal Data is restricted in specific sectors, which include the following sectors:

- Telecommunications – The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications prescribes requirements on telecommunications license holders to collect, process, and maintain the Personal Data of their telecommunications users.

- Credit bureau – The Credit Bureau Act B.E. 2545 (2002) was enacted with the following objectives: (i) to control the credit bureau company and credit information transactions; (ii) to protect the rights of the Data Subject; and (iii) to ensure that reliable information is given to the processor of credit information.


- Public health – The National Health Act B.E. 2550 (2007) provides protection on personal health information. No one shall disclose it in a manner that causes damages to the Data Subjects, unless the consent is obtained or other exceptions apply.

- Banking and e-payment – Electronic payment service providers are subject to the Royal Decree Regulation on Electronic Payment Services B.E. 2551 (2008) and its related sub-regulations. There are requirements for service providers to protect their customers’ Personal Data. At present, a Payment System Act B.E. 2560 (2017) (the “Payment System Act”) has been issued to unify existing payment laws and regulations. Once the Payment System Act becomes effective in April 2018, certain current e-payment laws and regulations will be revoked.
Government agencies – The Official Information Act B.E. 2540 (1997) provides protection for Personal Data of individuals which is in the possession or control of a state agency.

As there is currently no general data projection law, in this handbook, we will focus on the requirements under the current draft version of the PDPB.

4. Key Privacy Concepts

a. Personal Data

Personal Data under the PDPB could be classified into two main categories as follows:

i. General Personal Data

The PDPB defines “Personal Data” as data relevant to a person that can identify the person directly or indirectly, excluding only names, titles, workplaces, or business addresses, and particular information of a deceased person.

ii. Sensitive Personal Data

According to the PDPB, certain Personal Data (e.g., race, ethnicity, political opinion, religious beliefs, sexual behavior, criminal history and medical history) is deemed Sensitive Personal Data.

b. Data Processing

The PDPB provides a definition for the term “Data Processor” as “a person or entity who conducts activities related to [the] collection, use, or disclosure of Personal Data under the instructions or under the name of the Data Controller”.

Data Processors are subject to various obligations, including implementing appropriate security measures, notifying the Data Controller of data breach incidents, and establishing and maintaining records of processing activities. Failure to comply would result in fines.

c. Processing by Data Controllers

Please see our response in (b) above regarding data processing and Data Processor.

For your reference, although there is no definition of “processing” under the PDPB, the PDPB prohibits Data Controllers from collecting, using or disclosing Personal Data without a Data Subject’s consent. However, there are certain exemptions to the consent requirements, such as (1) for the purpose of research and statistics, provided it is in the public interest and the Personal Data is kept confidential, (2) for the purpose of a legitimate interest
pursued by the Data Controller or by a third party, or (3) for the public interest or in the exercise of official authority vested in the Data Controller.

d. **Jurisdiction/Territoriality**
   Thailand.

e. **Sensitive Personal Data**
   Please see our response in (a).

f. **Employee Personal Data**
   No specific requirements apply under the PDPB.

5. **Consent**
   a. **General**
      The PDPB generally requires consent for collection, use, disclosure, or international transfer of Personal Data with exemptions.

   b. **Sensitive Data**
      Sensitive Personal Data cannot be collected without the Data Subject’s consent, with a few exemptions.

   c. **Minors**
      There are no specific requirements under the PDPB. However, when applying the legitimate interest exemption to consent requirements, special consideration must be taken into account if the Data Subject is a minor. Generally, consent cannot be obtained from minors. It can be given by a legal guardian or parent on behalf of the minor, or from the minor himself/herself depending on the circumstances.

   d. **Employee Consent**
      There are no specific requirements applicable to an employee under the PDPB.

   e. **Online/Electronic Consent**
      The PDPB prescribes the form of consent to be in writing or given via an electronic system, unless consent cannot be obtained by such methods.

6. **Notice Requirements**
   According to the PDPB, Data Controllers will be required to notify Data Subjects of certain details before or at the moment of collecting Personal Data, e.g., the purposes of collection, types of persons or organizations that Personal Data might be disclosed to, rights of the Data Subject, etc.

7. **Processing Rules**
   Please see our response in 4(b) above regarding data processing.
8. Rights of Individuals
The PDPB sets out rights of Data Subjects, e.g., right to access the Data Subject’s data, or right to access such data obtained without the Data Subject’s consent.

9. Registration/Notification Requirements
Currently, there are no requirements for an organization that collects and uses Personal Data to register with the local data protection authority, or file with and notify the appropriate data protection authority.

10. Data Protection Officers
According to the PDPB, the Personal Data Protection Committee, the Expert Committee, and the Supervisory Committee will be set up and will be in charge of Personal Data. The Personal Data Protection Committee has the power and duty, among other things, to issue guidelines/notifications/rules for Personal Data protection. The Expert Committee will deal with complaints from Data Subjects who suffer damage caused by Data Controllers who violate or fail to comply with the PDPB.

11. International Data Transfers
The PDPB requires that the transfer of Personal Data to other countries must comply with a sub-regulation, to be issued by the Personal Data Protection Committee, with certain exceptions (consent, prior agreement, etc.).

12. Security Requirements
Under the PDPB, Data Controllers and Data Processors must provide security methods to prevent loss, access, use, change, alteration, or disclosure of Personal Data without the authority to do so, etc.

13. Special Rules for Outsourcing of Data Processing to Third Parties
Under the PDPB, if Personal Data is granted to third parties, Data Controllers must take measures to prevent third parties from using or disclosing Personal Data without authority.

14. Enforcement and Sanctions
Failure to comply with data privacy laws can result in complaints, data protection authority investigations or audits, data protection authority orders, administrative fines, penalties or sanctions, civil actions, and private rights of action.
15. Data Security Breach
Under the PDPB, if a breach happens, the Data Controller is required to notify the Data Subject of the breach immediately. If the breach affects a large number of people (the number is to be prescribed by the Personal Data Protection Committee), the Data Controller must also report the breach incident and the remedial plan to the Personal Data Protection Committee immediately. In addition to the abovementioned requirements, the Data Processor must also notify the Data Controller of the breach incident.

16. Accountability
Under the PDPB, the Data Controller is obligated to regularly conduct a Data Protection Impact Assessment of the Data Subject.

17. Whistle-Blower hotline
There are no specific laws/rules in Thailand that govern the establishment of a whistle-blower hotline.

18. E-Discovery
Thailand currently does not have an e-discovery system.

19. Anti-Spam Filtering
There are no specific laws or regulations restricting the installation of spam filtering within organizations in Thailand.

20. Cookies
There are no specific laws or rules in Thailand that regulate the use and deployment of cookies.

21. Direct Marketing
Sending promotional direct marketing message for business purposes is subject to the Computer Crime Act. Under a sub-regulation of the Computer Crime Act, consent and an opt-out option are required to send commercial messages.
Turkey

Can Sozer
Istanbul
Tel: +90 212 376 64 43
can.sozer@esin.av.tr

Hilal Temel
Istanbul
Tel: +90 212 376 64 17
hilal.temel@bakermckenzie.com
1. Law on the Protection of Personal Data

After almost a decade of legislative struggles, on 7 April 2016, the Law on the Protection of Personal Data (the “Data Protection Law”) entered into force, effective as of 7 October 2016. The Data Protection Law aims to harmonize Turkish data protection laws with the European Data Protection Directive No. 1995/46/EC (the “Directive”) and Council of Europe’s Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (the “Strasbourg Convention”), which Turkey ratified on 18 February 2016.

2. Transitional Periods

The Data Protection Law envisages a gradual entry into force and establishes transitional period obligations.

7 April 2017

The provisions that entered into force within one year after the publication of the Data Protection Law are as follows:

- The Authority was to issue secondary legislation based on the Data Protection Law within one year, namely before 7 April 2017. The Authority issued the below draft regulations and opinions to date:
  - the Draft Regulation on Data Controllers’ Registry (5 May 2017),
  - the Draft Regulation on Personal Data Deletion, Destruction and Anonymization (29 May 2017), and
  - opinions (12 July 2017), which shed light on how the Authority will interpret rules surrounding explicit consent, exceptions to process data in the absence of explicit consent, and cross-border data transfers.

- Explicit consents lawfully given before 7 April 2016 will be deemed compliant with the Data Protection Law, unless the relevant Data Subject expresses his/her declaration of intent to the contrary within one year (i.e., before 7 April 2017). Any data for which the Data Subject raised an objection must, therefore, be deleted, anonymized or destructed.

7 April 2018

In addition, Personal Data processed before 7 April 2016 must be aligned with the requirements introduced by the Data Protection Law within two years (i.e., before 7 April 2018). Non-compliant Personal Data must immediately be deleted, destroyed or anonymized.
3. Before the Data Protection Law

In the absence of the Data Protection Law, general provisions of Turkish law (especially the Turkish Constitution, Criminal Code, Labor Law, Code of Obligations, Civil Code and E-Commerce Law) and sector-specific rules (such as rules under the Banking Law, Payment Systems Law and Electronic Communications Law) applied to data protection matters. As such, processing or transfer of Personal Data were somewhat protected under general Turkish laws even before the Data Protection Law.

According to Article 20/3 of the Turkish Constitution, Personal Data can only be processed if designated by law or upon the Data Subject’s explicit consent. All Data Subjects are can request (i) information about their processed Personal Data, (ii) access to such data, (iii) their data to be edited or deleted, and (iv) information on whether their Personal Data has been processed in line with the purpose of collection.

The following are important general and sector-specific privacy provisions under Turkish law, which are applicable to date. Sector-specific rules, mainly, are of crucial significance if/when the provisions contain stricter requirements than the Data Protection Law.

**General Provisions**

**Turkish Constitution.** In addition to Article 20 above, Article 17(I) of the Constitution provides that “*every individual is entitled to rights of living, protection and improvement of his material and spiritual being*.”

**Turkish Civil Code.** Articles 23, 24 and 25 of the Turkish Civil Code safeguard personal rights. Article 23 sets out that “*no individual may waive his/her freedom or restrict his/her freedom contrary to morality and law*”. Furthermore, Article 24 provides legal remedies, stating that “*violation of personal rights is unlawful unless justified by the consent of the person whose rights have been violated, superior private or public benefit, or authority granted by law*”. Article 25 also sets out certain civil remedies in case of infringement of personal rights.

**Turkish Code of Obligations.** Pursuant to Article 27 of the Turkish Code of Obligations, an agreement contrary to personal rights is invalid. Furthermore, under Article 58, a person whose personal rights have been violated may seek damages against the person who has violated those rights. Additionally, Article 419 imposes a duty on an employer in relation to Employee Personal Data. Pursuant to this provision, an employer may only use Employee Personal Data where it is related to the employee’s qualifications or if it is required to perform a service.

**The Turkish Labor Law.** Article 75 of the Turkish Labor Law states that “*the employer shall arrange a personnel file for each employee working in its*
establishment. In addition to the information about the employee’s identity, the employer is obligated to keep all the documents and records in its possession in accordance with this Act and other legislation and to show them to authorized persons and authorities when requested. The employer is obligated to use information obtained about the employee consistent with the principles of honesty and law and not to disclose information which the employee has a justifiable interest in keeping secret”.

In Turkey, employers generally receive the following from employees: employee application forms, copies of identification cards, certificates of residence, copies of diplomas, certificates of proficiency (if any), employment contracts, health reports, original disability reports (for disabled employees), warning letters regarding employment health and security, and conviction records. To the extent that Article 75 is applicable, the employers are only permitted to use such data according to this provision.

Under certain circumstances, an employee may terminate his or her employment contract for cause under the Labor Law in the event of an invasion of privacy.

Turkish Criminal Code. Personal Data and privacy are also safeguarded under the Turkish Criminal Code. For instance, under Article 134 of this Code, a person who violates the secrecy of a person’s private life may be fined or imprisoned for one to three years. According to Article 135 of the Turkish Criminal Code, illegally recording Personal Data, violating the data recording prohibition or data recording without consent of the relevant person, and illegally recording data relating to the political, philosophical or religious views, or ethnic origins of individuals or moral inclinations, sex lives, health conditions or trade union affiliations may subject the offender to six months’ to three years’ imprisonment. Similarly, under Article 136 of this Code, the illegal transfer, dissemination and collection of Personal Data is punishable by imprisonment of one to four years.

Pursuant to Article 138 of the Turkish Criminal Code, if a person whose responsibility is to delete Personal Data at the end of the retention period fails to do so, that person may be imprisoned for six months to one year. Nevertheless, the sanction of imprisonment only applies to natural persons; the Turkish Criminal Code also sets forth security measures applicable to legal entities.

Sector-Specific Provisions

Electronic Communications Act. Article 51 of the Electronic Communications Act contains detailed rules on the protection and management of Personal Data in the electronic communications sector. These rules include, but are not limited to, the new rule allowing international transfer of Personal Data with explicit consent. According to Article 51, Personal Data may only be
processed when explicitly permitted by law and in line with the principles of good faith. Additionally, electronic communications and traffic data are deemed private; therefore, the recording, retention, interception or tracking of electronic communications, in the absence of another legal basis or the consent of the Data Subject (i.e., parties to the communication), is prohibited. Moreover, retaining and accessing data in users’ terminal equipment for purposes other than those related to the provision of electronic communications services, are permitted only after obtaining the users’ informed consent. Electronic communications operators are obligated to take administrative and technical measures to ensure the security of their users’ Personal Data.

**Banking Act.** Article 73 of the Banking Act states that the council operating within the organization of Banking Regulation and Supervision Agency and the relevant chairman, member and officers are obliged to keep confidential the information collected during the exercise of their duties, and information belonging to the banks, their subsidiaries, affiliates, and jointly controlled entities and customers of those, except as provided under this Article 73. In addition, those who obtain confidential information by virtue of their duties must not disclose this information. Banking Act and its secondary regulations also require banks to keep their primary servers and backups of primary servers in Turkey.

**The Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions** (the “Payment Systems Law”). Article 32 of the Payment Systems Law requires payment system operator, payment institution and electronic money institutions not to disclose confidential information obtained by them during their duties. Payment Systems Law and its secondary regulations also require regulated entities to keep their primary servers and back-ups of primary servers in Turkey.

**Electronic Communications Act** (the “Electronic Communications Act” or “ECA”). Article 51 of the ECA addresses many issues regarding data protection in the electronic communications sector. Under Article 51, Personal Data may only be processed when explicitly permitted by law and in line with the principles of good faith. Also, retaining and accessing data in users’ terminal equipment for purposes other than those related to the provision of electronic communications services is only permitted after obtaining the users’ consent. Subject to other laws governing the transfer of Personal Data abroad, such as the Data Protection Law, the transfer of traffic and location data abroad is also only permitted with the Data Subjects’ explicit consent.
4. Key Privacy Concepts

a. Personal Data
Personal Data is all kinds of data related to an identified or identifiable real person.

b. Data Processing
Data processing means any operation performed upon Personal Data, whether by automatic means or not by automatic means on the condition that is a part of any data filing system, such as collection, recording, storage, conservation, modification, rearrangement, disclosure, transmission, taking over, making available, classification or blocking of use.

c. Data Controllers
Data Controller is defined under the Data Protection Law as the natural or legal person who determines the purposes and means of processing Personal Data and also is responsible for the establishment and administration of a data filing system.

d. Data Protection Authority
The Data Protection Law envisages the establishment of the Data Protection Authority (the “Authority”), as an administratively and financially independent public entity. The Authority was established on January 2017.

The Authority has investigative powers and powers of intervention. The Authority also has the power to engage in legal proceedings as it has six staff lawyers.

e. Data Controllers Registry
The Authority will run a Data Controllers Registry, and all Data Controllers will have to register themselves with this registry before data processing.

The Draft Regulation on Data Controllers Registry requires all Data Controllers to register before initiating processing activities. Upon registering, the regulation will require controllers to provide their identity and address information, along with information for any representatives; the purposes of processing data; an explanation of the categories of Data Subjects as well as the categories of data being processed; recipients of any data transfers; any Personal Data which might be transferred to third countries; and security measures taken to ensure information security.

f. Jurisdiction/Territoriality
Article 35 of the Law on International Private Law and Procedure Law No. 5718 provides that “claims arising from the violation of personal rights through the media, such as radio, press, television, the Internet or any other mass media will be governed by, at the discretion of the aggrieved party (i) the law
of the aggrieved party’s habitual residence, provided the injurer is in a position to be aware that damage could occur in that jurisdiction, (ii) the law of the injurer’s place of business or habitual residence, (iii) the law of the jurisdiction where the damage occurred, provided that the injurer is in a position to be aware that the damage could occur in that jurisdiction”. It further sets forth that “[t]he first clause of this article is also applicable to claims arising from violation of personal rights by processing Personal Data or restricting right to demand information regarding Personal Data”.

Moreover, the Data Protection Law applies to legal entities and individuals that process Personal Data in Turkey through automatic means or as part of a data filing system. The Data Protection Law, however, is silent on whether or not its application will extend to the processors of data that are based outside of Turkey. At the initial stage, it would be the safest option to adopt a broad interpretation of the Data Protection Law and consider any processing activity, which concerns Turkish citizens or residents of Turkey and which show their effect in Turkey, as captured by the Data Protection Law. In the future, the Authority is expected to issue a regulation and/or give guidance on its jurisdictional powers.

g. **Sensitive Personal Data**
The Personal Data revealing race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, foundation or trade union membership, health, sexual life, data on penal convictions or security measures, as well as biometric and genetic data of a person.

h. **Explicit Consent**
Informed consent given with free will for a specific subject.

i. **Anonymizing**
Processing Personal Data in such a way to render it impossible, under any circumstances, to link such data with an identified or identifiable person, including doing so by pairing the relevant dataset with another.

j. **Employee Personal Data**
Turkish law does not separately address Employee Personal Data. If it is deemed Personal Data, the above-mentioned legal framework applies. According to the opinions published by the Authority, it is controversial whether an employee may be deemed to have given his/her explicit consent as employee cannot always act upon his/her free will against the employer in case of a contractual employment relationship.
5. Consent

a. General
Explicit consent of the Data Subject is required prior to the collection, processing and disclosure of Personal Data. Explicit consent by the Data Subject must always be voluntary, informed, explicit and unambiguous, though it is not required in the following circumstances:

- it is specifically designated by laws;
- processing is necessary in order to protect the vital interests of third parties or the Data Subject whose consent cannot be obtained due to physical impossibilities or would not normally be valid and binding;
- processing of Personal Data with respect to parties to a contract provided that the data is directly relating to the formation or performance of the contract;
- processing is necessary for compliance with a legal obligation to which the Data Controller is subject;
- data to be processed has been made public by the Data Subject;
- processing is necessary for the establishment, performance or protection of a right; or
- processing is mandatory for the Data Controller’s legitimate interest, on the condition that it does not harm the Data Subject’s fundamental rights and freedoms.

b. Sensitive Personal Data
Under Article 6 of the Data Protection Law, Personal Data relating to race, ethnicities, political, philosophical, religious, sectarian views or other beliefs, clothes and appearances, association, foundation and trade union affiliations, health conditions, sexual life, convictions and safety precautions, and biometric and genetic data is classified as Sensitive Personal Data.

As a general rule, Sensitive Personal Data may be processed only if the Data Subject has unambiguously given his/her explicit consent. Except for Personal Data related to individuals’ health conditions and sexual lives, it is possible to process Sensitive Personal Data without the Data Subject’s explicit consent where processing has been specifically designated by laws.

Data related to health conditions and sexual life may be processed without the Data Subject’s explicit consent solely by the persons or authorized institutions and organizations who are under a confidentiality obligation, and for the purposes of protecting public health, preventive medicine, medical diagnosis,
medical treatment and care, or for planning, management or financing of health services.

Under the Data Protection Law, Sensitive Personal Data may not be processed unless adequate measures determined by the Data Protection Authority are taken.

c. Employee Consent

Article 75 of the Turkish Labor Law states, “[t]he employer shall arrange a personnel file for each employee working in its establishment. In addition to the information about the employee’s identity, the employer is obligated to keep all the documents and records in its possession in accordance with this Act and other legislation and to show them to authorized persons and authorities when requested. The employer is obligated to use information obtained about the employee consistent with the principles of honesty and law and not to disclose information which the employee has a justifiable interest in keeping secret”.

Additionally, Article 419 of the Code of Obligations imposes a duty on an employer in relation to Employee Personal Data. Pursuant to this provision, an employer may only use employee personal information where it is related to the employee’s qualifications or if it is required to perform a service.

On 24 March 2016, the Turkish Supreme Court concluded that once the employees sign and initial the policies stating that the communication conducted via corporate computer, email address, phone or other IT device of the company will be subject to review by employers at any time, and that the relevant communication records may at any time be stored, reported, and appropriated by the employer, employers cannot be expected to have a reasonable expectation for privacy of their personal correspondences over these devices. Upon this assessment, the Supreme Court found the employer rightful, who terminated the employment contract on justifiable grounds by asserting employees’ personal emails communicated through company email address as evidence of decrease of performance in the workplace.

6. Information/Notice Requirements

The Data Protection Law provides for certain obligations to ensure transparency when data is processed. Accordingly, while collecting Personal Data, the Data Controller is obligated to inform the Data Subject of the following information:

- the identity of the Data Controller, or, if available, its representative;
- the purposes for which Personal Data will be processed;
- the persons to whom Personal Data might be transferred and the purposes for such transfer;
• the method and legal cause of collection of Personal Data; and
• the rights of the Data Subject.

The Data Controllers are also required to register with a publicly available Data Controllers Registry before they start processing Personal Data.

7. Processing Rules

Under the Data Protection Law, data processing must be conducted in line with the principles below:
• data processing must be in accordance with the law and good faith;
• data processed must be accurate and up-to-date;
• data must be processed for specific, clear and legitimate purposes;
• data processing must be conducted in connection with, limited to and appropriate for the purpose of processing; and
• data must be retained only limited to the period prescribed by the law or necessary for the purpose of processing.

8. Rights of Data Subjects

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access the Data Subject's personal Data, subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject's Personal Data; (iv) request the deletion and/or destruction of the Data Subject's Personal Data; and (v) exercise the writ of habeas data. More specifically, Data Subjects have the right to:
• learn whether or not Personal Data relating to him/her is being processed;
• if it is processed, request information with regard to the processing;
• learn the purposes of the processing and whether the data is used for such purposes or not;
• know the third persons within or outside the country to whom the Personal Data is transferred;
• request correction of the Personal Data if the data is processed incompletely or inaccurately;
• request deletion or destruction of the Personal Data on procedures concerning anonymizing, deleting or removing Personal Data;
• request notifying third persons to whom the Personal Data is transferred, about the processes made within the scope of correction and deletion of Personal Data;

• object to negative consequences about him/her that are concluded as a result of analysis of the processed Personal Data by solely automatic means; and

• request for indemnification if the Data Subject suffered damage because of illegal processing of his/her Personal Data.

9. Anonymizing, Deleting or Removing Personal Data

If the purposes of processing Personal Data no longer exist, Personal Data must be deleted, destructed or anonymized by the Data Controller either through its own act or upon the Data Subject’s request. The principles and procedures on deleting, removing or anonymizing Personal Data will be determined through secondary legislation, to be issued by the Authority.

The Draft Regulation on Personal Data Deletion, Destruction and Anonymization mainly sets out grounds for deletion of Personal Data, principles of Personal Data deletion, anonymization and scope of Personal Data retention and deletion policy.

10. Registration/Notification Requirements

The Data Controllers will need to be registered before the Data Controllers Registry in order to perform the data processing. The Data Controllers Registry will be kept and maintained under the supervision of the Authority.

11. Data Protection Officers

There is no requirement for private organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization. A Data Controller, however, is obliged to conduct the necessary audits to ensure that the provisions of the Data Protection Law are applied in its institution or entity.

12. International Data Transfers

In principal, Personal Data cannot be transferred to foreign countries without the Data Subject’s explicit consent.

Personal Data shall be transferred without the Data Subject’s explicit consent on the condition that the conditions for exceptions on processing of Personal Data without Data Subject’s explicit consent exists, and either (i) there is adequate level of protection in the relevant foreign country, or (ii) there is no adequate level of protection in the country of transfer, however, the Data Controllers and Processors located both in Turkey and in the relevant country
undertake to provide adequate protection in writing and the approval of the Authority is obtained.

Once established and operative, the Authority will determine the jurisdictions with and without adequate level of protection for Personal Data. The below measures will be taken into account during such determination:

- international treaties to which Turkey is a party;
- reciprocity with respect to data transfer between Turkey and the country requesting the Personal Data;
- data quality, purpose and period of the processing, specific to each and every Personal Data transfer;
- relevant legislation of the country to which Personal Data will be transferred; and
- measures undertaken by the Data Controller residing in the country where the Personal Data will be transferred.

13. Security Requirements
A Data Controller shall take all necessary technical and administrative measures to ensure appropriate security level to ensure the following:

- prevention of illegal processing of the Personal Data;
- prevention of illegal access to the Personal Data; and
- preservation of the Personal Data

In addition, the Data Controller is obligated to make either internal or external audits to ensure that it complies with the security requirements.

14. Special Rules for Outsourcing of Data Processing to Third Parties
If the data is processed by a third party on behalf of the Data Controller, the controller will be jointly responsible to ensure the security measure provided in the Data Protection Law, and listed in section 13 above.

15. Enforcement and Sanctions
The Authority will be entitled to impose administrative fines on those who infringe the provisions of the Data Protection Law, as follows:

- infringement of obligation to inform the Data Subject will be subject to an administrative fine of TRY 5,000 to TRY 100,000;
infringement of obligations in relation to data security will be subject to an administrative fine of TRY 15,000 to TRY 1,000,000;

non-compliance with the Board decisions of the Data Protection Authority as a result of an inspection will be subject to an administrative fine of TRY 25,000 to TRY 1,000,000; and

infringement of obligation to register with the Data Processors Registry will be subject to an administrative fine of TRY 20,000 to TRY 1,000,000.

In addition, the below provisions of the Criminal Code will be applicable for infringements:

unlawful collection of Personal Data is subject to imprisonment of one year to three years;

unlawful transfer, acquisition or distribution of Personal Data is subject to imprisonment of two to four years; and

infringement of obligation to delete or anonymize Personal Data under the Data Protection Law will also be subject to the Criminal Code (imprisonment of one year to two years).

Failure to comply with data privacy laws can result in complaints, administrative fines, penalties or sanctions, civil actions, criminal proceedings, and/or private rights of action.

16. Data Security Breach

If third parties unlawfully obtain Personal Data, the Data Controller must immediately inform the Data Subject and the Authority. If it deems necessary, the Authority may announce the incident on its website or through other means.

17. Accountability

Personal Data processed before 7 April 2016 must be aligned with the requirements introduced by the Data Protection Law within two years (i.e., until 7 April 2018). Non-compliant Personal Data must immediately be deleted, destructed or anonymized. Otherwise, Data Controllers will face legal consequences provided in the Data Protection Law, under Section 15 above.

18. Whistle-Blower Hotline

There is no specific law/rule that governs whistle-blower hotlines in Turkey.

19. E-Discovery

When implementing an e-discovery system, an organization may be required to obtain the consent of employees if the collection of Personal Data is
involved, and appropriately inform employees of the implementation of the system, the monitoring of work tools and the storage of information.

20. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to inform employees of monitoring policies being implemented in the workplace.

21. Cookies
There are no specific laws/rules in Turkey that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws. To the extent cookies collect Personal Data, consent of Data Subjects must be obtained at the time of collection of Personal Data by cookies.

22. Direct Marketing
On 1 May 2015, the Law on Regulation of Electronic Commerce (the “E-Commerce Law”) entered into force. The E-Commerce Law bans commercial messages by email, text messaging (SMS), fax, and autodial machines (robocalls) to consumers without their prior approval. Previously, it was permitted to send unsolicited messages if consumers were provided with an easy and free-of-charge opportunity to opt out. Under the E-Commerce Law, commercial messages can be sent to a consumer electronically only if the consumer has given prior approval. Approval must be obtained either electronically or in writing.

The content of the commercial message must be in line with the approval given. The message also must include: (i) sender identity; (ii) sender phone number/fax number/SMS number/email, depending on the electronic means used; (iii) subject and purpose of the message; and (iv) information on the actual sender, if the message is sent on behalf of another entity.

As consumers always have the right to opt out of receiving commercial messages, the sender must provide them an easy and free-of-charge opportunity to revoke their prior approval; details of this opportunity must be contained in the message.

The opt-in system will not apply to B2B relationships and commercial messages can still be sent to businesses without their prior approval.

The service provider will be responsible for storing and securing the Personal Data obtained from the online agreement. The service provider will not be able to transfer the Personal Data to third parties without the buyer’s consent, or use the data for other purposes.
Ukraine

Oleksiy Stolyarenko
Kyiv
Tel: +380 44 590 0101
oleksiy.stolyarenko@bakermckenzie.com
1. Recent Privacy Developments

Reforming the administration of Personal Data protection

In July 2013, the Ukrainian government adopted a draft law that introduced amendments to the Personal Data Protection Law in Ukraine. As a result, all Personal Data protection functions were transferred from the State Service of Personal Data Protection to the Ukrainian Parliament Commissioner for Human Rights (“Commissioner”) effective 1 January 2014.

As such, the Commissioner was tasked with developing all Personal Data protection procedures, recommendations and enforcement practices that regulate matters related to Personal Data protection. To date, the Commissioner has drafted and approved: Model Rules on Personal Data Processing; Rules on Exercising Control by the Ukrainian Parliament Commissioner for Human Rights over Compliance With Laws on Personal Data Protection; Procedure of Notification of the Ukrainian Parliament’s Commissioner for Human Rights on the Processing of Personal Data, which is of Particular Risk to the Rights and Freedoms of Personal Data Subjects, on the Structural Unit or Responsible Person that Organizes the Work Related to Protection of Personal Data During Processing Thereof.

In addition, registration of databases containing Personal Data is no longer required; instead, Data Controllers must notify the Commissioner of the processing of certain types of sensitive information.

2. Emerging Privacy Issues and Trends

Ukraine follows the EU data protection trends at its own pace.

Regulation (EU) 2016/679 (the “GDPR”) and Directive 2009/136/EC are due to be adopted by the Ukrainian government, as part of the process of implementing EU law in Ukraine.

In its annual report, the Commissioner highlighted the need for Ukraine to adopt not only the GDPR, but also Directive 2016/680 dated 27 April 2016.

In addition, the Supreme Court of Ukraine published, as part of a joint program with the Council of Europe and the European Union, “Strengthening the Information Society in Ukraine”, a collection of decisions of the European Court of Human Rights on the protection of Personal Data.

However, it is likely that after the GDPR enters into force in May 2018, the process of implementing the EU Personal Data regulations in Ukraine will be expedited, driven by the export-oriented IT outsourcing industry.

It should also be noted that the EU–Ukraine Association Agreement fully came into force in September 2017. Under this agreement, the parties have agreed to cooperate on the introduction of the highest European and
international data protection standards, including ones included in the Conventions of the Council of Europe. When the agreement was signed in 2014, it was unclear what the wording “the highest European data protection standards” entailed. But with the introduction of the GDPR, it is now clear what this phrasing means. As a prospective member of the European Union, Ukraine is obligated to harmonize its legislation with the legislation of the European Union. Taking into account the current pace of EU integration processes in Ukraine, the adoption of the GDPR in Ukraine will likely happen during the next two to four years.

3. Law Applicable

The Law of Ukraine On Personal Data Protection, adopted in 2010 ("PDP"),\(^1\) outlines the general requirements and obligations related to the collection, processing and use of Personal Data by private bodies and by the government of Ukraine.

Under the PDP, the processing of Personal Data is not restricted under the following circumstances: (i) individuals processing Personal Data for their own personal or domestic activities; and (ii) Personal Data processed solely for journalistic and artistic purposes, provided the balance between the right to respect for private life and the right to freedom of expression is secured. In addition, the PDP does not apply to archived information from repressive totalitarian organizations within the territory of Ukraine from the period between 1917 and 1991.

In addition, the main sources of Personal Data protection in Ukraine are: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol ratified by Ukraine in 2010; a number of regulations approved by the Commissioner; respective provisions of the Code of Ukraine on Administrative Offenses; and the provisions of the Criminal Code establishing liability for Personal Data offenses.

4. Key Privacy Concepts

a. Personal Data

The PDP applies to the “processing” of “Personal Data”, i.e., any information about an individual who is identified or can be specifically identified ("Data Subject").

The Constitutional Court of Ukraine, in its Decision No. 2-rp/2012 dated 20 January 2012, held that “Personal Data” constitutes confidential personal information, access to which is limited by a person himself/herself. Such confidential personal information may include data about the individual’s

nationality, education, marital status, religious beliefs, health, current address, date and place of birth, and property status. The list of confidential personal information is not exhaustive.

b. Data Processing
“Processing of Personal Data” is defined as any action performed manually or through the means of automated systems including, but not limited to, the acquisition, registration, accumulation, storage, adaptation, modification, restoration, use and distribution (dissemination, sale, transfer), depersonalization and destruction of Personal Data.

c. Processing by Data Controllers
The PDP applies to any person or legal entity which processes Personal Data on his, her or its own behalf (“Data Controller”).

“Data Controller” is defined by the PDP as a person or a legal entity that establishes the purpose of processing Personal Data, and sets the scope and procedures of the data processing.

d. Jurisdiction/Territoriality
The PDP applies to all Personal Data processing (i.e., acquisition, registration, accumulation, storage, adaptation, modification, restoration, use and distribution (dissemination, sale, transfer), depersonalization and destruction) within the territory of Ukraine. However, enforcement of the PDP against legal entities and individuals without a legal presence in Ukraine is not yet established.

e. Sensitive Personal Data
Ukrainian data protection law recognizes the concept of sensitive data (direct translation: “special categories of Personal Data that constitute special risks to rights and freedoms of Data Subjects”). Data protection rules for sensitive data are more stringent.

Sensitive Data includes Personal Data on: racial or ethnic origin, national origin, political, religious or philosophical beliefs, membership in political parties and/or organizations, trade unions, religious organizations or community organizations with an ideological orientation, health, sex life, biometric data, genetic data, location and or methods of transportation, facts related to administrative or criminal liability, criminal investigation measures related to a preliminary investigation and the measures envisaged by the Law of Ukraine “On investigating activity”, and instances of violence against a person.
The PDP prohibits processing of Sensitive Personal Data unless certain conditions are met, including:

- valid express consent has been obtained by the Data Collector from the Data Subject;
- an employer-employee relationship exists between the Data Collector and Data Subject;
- the data processing is necessary to protect the life of the Data Subject or of a third party where the Data Subject is physically or legally incapable of giving consent;
- the data has evidently been made public by the Data Subject;
- the data is necessary to assert, exercise or defend legal claims;
- the data is processed by a religious organization, NGO, political party or trade union with respect to their members in the course of regular activities and such data would not be transferred to third parties;
- the data processing is necessary to establish a medical diagnosis or to provide healthcare services or medical treatment, under the condition that the data processed is protected by medical confidentiality rules; and
- the data processing is conducted by law enforcement agencies and is related to criminal convictions, criminal investigations or counterterrorism activities.

The PDP requires legal entities and individuals processing Sensitive Data to file a respective notification to the Commissioner and appoint a Personal Data officer or establish a specific division responsible for Personal Data Protection.

f. Employee Personal Data

The PDP permits the collection and processing of Employee Personal Data, including sensitive data, by an employer within the course of an employer-employee relationship. However, the PDP views the employer rather narrowly as the legal entity that concludes the employment agreement with an employee. Accordingly, the transfer and processing of Employee Personal Data within a group of companies is not justified. Therefore, and for such purposes, Employee Personal Data may only be processed upon obtaining consent from the employee.

5. Consent

a. General

Consent is an appropriate way to justify the collection, processing and use (including transfer) of Personal Data.
The Ukrainian Personal Data regulations define consent as the “voluntary act of the individual (duly informed) to permit the processing of Personal Data in accordance with the objectives set out for processing expressed in written or electronic form”.

Informed consent is understood to constitute the “voluntary, competent decision of a person on the processing of his/her Personal Data that is based on receipt by this person in an objective manner and with full information with respect to future Personal Data processing”.

In order to make a voluntary and informed decision, a person, according to the Ukrainian Personal Data protection regulations, should be provided with responses to the following questions:

- Who will process his/her Personal Data? (Name of the processor of Personal Data, address, contact numbers, etc.)
- For what purpose will the Personal Data be processed? (The goal of processing must be formulated clearly.)
- What Personal Data will be processed? (Specific exhaustive list of Personal Data to be processed.)
- What specific actions will be performed on the Personal Data? (Collection, storage, transmission, publication, depersonalization, etc.)
- Who is the controller of the Personal Data? What are the rights and obligations of the Data Controller?
- To whom and where will the Personal Data be transferred? For what purpose? On what grounds?
- How long will the Personal Data be stored by the controller?
- Under what conditions can a person withdraw consent to the processing of Personal Data and what are the consequences of such action?

The Data Subject has a right to revoke his/her consent at any time. After revocation, the Data Controller and Data Processor must suspend the processing of Personal Data and destroy all of the Personal Data related to such Data Subject.

b. Sensitive Data

Ukrainian law recognizes Sensitive Data as a special category of Personal Data. It may be collected and processed with the express consent of the Data Subject. However, in certain prescribed circumstances, Sensitive Data may be processed without obtaining such consent.
c. Minors
The PDP does not provide clear guidance on the age requirements for minors to be legally capable of consenting to Personal Data processing.

The Civil Code of Ukraine stipulates that minors from the age of 14 are capable of concluding small value contracts that correspond to the minor’s moral, social and physical level. They can also manage their own independent income and IP rights, have a right to become a shareholder/founder of a legal entity, and open a bank account. All other legally binding actions by minors shall be approved by their parents or guardians.

Whether the minors can consent, and the extent of such consent to the processing of their Personal Data, remains to be decided by the Ukrainian authorities.

d. Employee Consent
Employee consent is not necessary to collect and process Employee Personal Data, including sensitive data, by an employer within the course of the employer-employee relationship. However, any transfer or processing of Employee Personal Data by third parties, even affiliated, requires consent on a general basis.

e. Online/Electronic Consent
Consent may be: (i) given in writing, i.e., ink signature or electronically; (ii) included as one of the conditions of a contract; or (iii) provided in any other form which leads to the conclusion that consent has been provided (written application, questionnaire, etc.). However, it is important to ensure that:

- the Data Subject has consented deliberately and unequivocally;
- consent is properly recorded and documented (for this purpose, the Data Subject should have to engage in traceable activity, such as checking a box and then pressing a button);
- the Data Subject can access the consent wording at any time; and
- the Data Subject must be able to withdraw consent at any time.

6. Information/Notice Requirements
An organization that collects Personal Data must provide Data Subjects with information about: the organization’s identity; the types of Personal Data being collected; the purposes for collecting Personal Data; its privacy practices (which must be given in a clear and transparent way); third parties to which the organization will disclose the Personal Data; the consequences of not providing consent; the rights of the Data Subject; and where the Personal Data is to be transferred.
7. Processing Rules
An organization that processes Personal Data must limit the use of Personal Data to only those activities which are necessary to fulfill the identified purpose(s) for which the Personal Data was collected and to the period necessary to fulfil said purpose(s), but no longer than the period prescribed by the archive legislation or bookkeeping. If, during processing, it becomes evident that Personal Data contains incorrect information, such data should be amended immediately or destroyed.

The Data Controller needs to obtain new consent from the Data Subject if the identified purpose of the Personal Data processing has changed based on the new identified purpose and scope.

8. Rights of Individuals
Data Subjects have a number of rights in Ukraine, including to be informed on sources of Personal Data collection, the location of their Personal Data, the purpose of processing, and the location of the Data Controller. In addition, Data Subjects have a right to access their Personal Data and request modification of their Personal Data in case it is outdated, or elimination if such data has been collected illegally. Data Subjects can apply for protection from illegal Personal Data processing to the Commissioner, police or to the courts.

9. Registration/Notification Requirements
Any person or organization that processes Sensitive Personal Data is required by the PDP to send a proper notification to the Commissioner, which should include the following information:

- types of Personal Data processed;
- purpose of Personal Data processing;
- category or categories of Data Subjects whose Personal Data is processed;
- identities of third-party recipients of Personal Data;
- cross-border transfers of Personal Data;
- place (actual address) of data processing; and
- general description of the technical and organizational measures taken by the Data Controller of Personal Data to ensure its protection.

The PDP provides exceptions to the above requirement. As such, notification is not necessary in the following cases:

- Sensitive Personal Data is processed in order to be included in a database or registry that is open to the general public;
• Sensitive Personal Data is processed by public associations, political parties and/or organizations, trade unions, employers' associations, religious organizations or NGOs with an ideological orientation, provided the processing of Personal Data relates exclusively to members of these associations and is not transferred without their consent; and

• Sensitive Personal Data is processed within an employee-employer relationship.

10. Data Protection Officers

The PDP requires legal entities and individuals processing Sensitive Personal Data to appoint an individual or establish a separate division responsible for Personal Data Protection.

The Data Officer/Designated Unit is responsible for consultations with the Data Controller/Processor on matters relating to compliance with Personal Data protection legislation and for interactions with the Commissioner on matters related to the prevention and elimination of data protection violations. The Data Officer/Designated Unit oversees compliance with the rights of Data Subjects with respect to Personal Data, analysis of security threats, and will have access to all facilities and computer systems where Personal Data is processed. Upon identification of a Personal Data violation, the Data Officer/Designated Unit must report the matter to the Data Controller/Processor.

11. International Data Transfers

International transfers of Personal Data are allowed from Ukraine in the following cases:

• unequivocal consent for international transfer has been obtained from the Data Subject;

• it is necessary to conclude or perform a transaction between the Controller of Personal Data and a third party – for the benefit of the Data Subject;

• it is necessary to protect the vital interests of Data Subjects;

• it is necessary to protect the public interest, or to establish, secure and enforce legal demands; and

• the Controller of Personal Data has provided appropriate safeguards to ensure the confidentiality of the private and family life of the Data Subject.

Under the PDP, international data transfers are allowed to countries that provide adequate state protection of Personal Data. Under the PDP, members of the EU/EEA and countries that ratified the Convention for the Protection of
Individuals with regard to Automatic Processing of Personal Data are deemed to provide adequate state protection of Personal Data. However, Personal Data shall not be transferred and shared internationally for any other purpose than that for which it was collected.

12. Security Requirements

Personal Data must be processed in a manner that prevents unauthorized access. The Data Controller/Processor must independently design special technical protection measures to prevent unauthorized access to Personal Data and to technical and software systems through which any access to Personal Data is controlled, logged and secured.

13. Special Rules for the Outsourcing of Data Processing to Third Parties

The transfer of Personal Data from the Data Controller to the Data Processor is only allowed on the basis of an agreement in writing where the parties agree on the scope and purpose of the Personal Data processing as well as other respective security measures.

14. Enforcement and Sanctions

The requirements of the PDP are enforced in Ukraine by the Commissioner, the police and the courts, through the respective administrative, criminal and civil actions, which may result in administrative fines, penalties or sanctions, civil actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

Ukrainian privacy regulations do not contain any specific rules related to Data Security breaches. Therefore, the Data Controllers/Processors as well as infringers may be found liable for violating the PDP on a general basis.

16. Accountability

Ukrainian privacy regulations do not contain any specific rules related to privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in Ukraine, provided they are in compliance with local laws. There is no specific regulation from the Personal Data protection standpoint. However, all collection of Personal Data through such hotlines should comply with the PDP and respective rules.
18. E-Discovery

Ukrainian privacy regulations do not contain any specific rules related to E-Discovery systems. Therefore, the general provisions of the privacy law/regulations should apply.

19. Anti-Spam Filtering

Ukrainian privacy regulations do not contain any specific rules related to Anti-Spam Filtering. Therefore, the general provisions of the privacy law/regulations should apply.

20. Cookies

There are no specific laws/rules that regulate the deployment of cookies. Hence, the general Ukrainian laws apply.

21. Direct Marketing

Direct Marketing activities require prior (opt-in) consent from the Data Subject, who must have the opportunity to unsubscribe from Direct Marketing (opt-out) at anytime.
Robbie Downing  
London  
Tel: +44 20 7919 1161  
robbie.downing@bakermckenzie.com  

Harry Small  
London  
Tel: +44 (0)20 7919 1914  
harry.small@bakermckenzie.com  

Ian Walden  
London  
Tel: +44 20 7919 1247  
ian.walden@bakermckenzie.com  

Benjamin Slinn  
London  
Tel: +44 20 7919 1783  
benjamin.slinn@bakermckenzie.com
1. Recent Privacy Developments

**The UK Data Protection Bill**

On 13 September 2017, the UK government introduced a Data Protection Bill (the “Bill”) in the context of Brexit and the EU General Data Protection Regulation (“GDPR”). The Bill is currently before the UK Parliament. The Bill will replace the current UK Data Protection Act (the “DP Act”) and supplements the GDPR by including certain derogations and options from the GDPR which are left to the authority of individual EU member states (for instance, the Bill confirms most of the current DPA exceptions to Data Subject rights and the current conditions for processing sensitive and criminal data). The Bill also implements the EU Law Enforcement Directive.

As long as the UK continues to be an EU member state, the GDPR and the Bill (which will become the new Data Protection Act) together form the statutory framework for UK data protection law. The UK government’s stated intention is to maintain the GDPR provisions following the UK’s exit from the EU. In order to do this, the provisions of the GDPR will be transposed into domestic law by means of the future European Union (Withdrawal) Bill currently before the UK Parliament.

**Data transfers between the UK and the EU after Brexit**

On 24 August 2017, the UK government published “The exchange and protection of Personal Data – A future partnership paper” which sets out the government’s vision for a future partnership with the EU regarding Personal Data flows between the UK and the EU following Brexit. In particular, the UK government intends to seek mutual recognition of adequacy status between the UK and the EU in order to enable the free flowing of Personal Data between the UK and the EU countries following the UK’s exit from the EU. This means that no cross-border data transfer mechanisms (such as model contractual clauses or binding corporate rules) would be required to legitimize UK-EU cross-border transfers. The outcome of the ongoing Brexit negotiations will determine whether and in which way an arrangement between the UK and the EU will be reached with respect to data flows.

**New ICO guidance**

In the course of 2017, the ICO has developed its general guide to the GDPR. This is considered to be an ongoing work and the ICO will continue expanding this guide over time, in particular as new guidance is issued by the Article 29 Working Party (future European Data Protection Board).

In 2017, the ICO also issued the following draft guidance under GDPR:

- Draft GDPR consent guidance (subject to public consultation from 2 March 2017 to 31 March 2017);
Draft GDPR guidance on contracts and liabilities between controllers and processors (subject to public consultation from 13 September 2017 to 10 October 2017); and

Children and GDPR guidance (subject to public consultation from 21 December 2017 to 28 February 2018).

The above guidance is currently in draft form. The ICO has been awaiting for definitive guidance from the Article 29 Working Party on the topics above before finalizing its guidance.

In the course of 2017, the ICO took a number of additional initiatives oriented to provide GDPR interpretation and clarification and assist businesses with GDPR implementation. In particular:

- On 6 April 2017, the ICO published a feedback request on profiling and automated decision-making to gather views from the public and feed them to the sub-working group of the Article 29 Working Party charged with preparing guidelines on automated individual decision-making and profiling (such guidance was issued by the Article 29 Working Party on 3 October 2017 and is currently in draft form);
- The ICO has launched a dedicated advice service telephone line for small organisations;
- The ICO has provided a number of online self-help resources on GDPR (e.g., GDPR checklist and GDPR self-assessment toolkit);
- The Information Commissioner has created a GDPR myth busting blog with a view to clarify key concepts and obligations under the GDPR.

2. Emerging Privacy Issues and Trends

**ICO Enforcement Action**

In the period between December 2016 and November 2017, the ICO has issued 53 monetary penalties for serious breaches of the ePrivacy Regulations or the DP Act.

a. **Direct Marketing**

The ICO is particularly focused on enforcing the electronic direct marketing rules under the ePrivacy Regulations especially in relation to telephone calls, text messages and emails, which is driven by the number of complaints that the ICO receives. In the period between December 2016 and November 2017 the ICO issued 30 monetary penalties for breaches of the ePrivacy Regulations, the total of these monetary penalties together being GBP 2,967,500. Of the 30 monetary penalties for breaches of the ePrivacy Regulations, 13 of these related to nuisance telephone calls, and the fines
ranged from GBP 40,000 to the highest monetary penalty to date issued by the ICO for breach of the ePrivacy Regulations, which was GBP 4,000,000 which related to 99.5 million nuisance calls by a marketing company. In addition, eight monetary penalties were issued during this period for breaches related to text messages which ranged from GBP 40,000 to GBP 140,000. The ICO is particularly focused on enforcing the electronic direct marketing rules under the ePrivacy Regulations especially in relation to telephone calls, text messages and emails, which is driven by the number of complaints that the ICO receives. In addition, the ICO has imposed eight monetary penalties in relation to direct marketing emails which ranged from GBP 10,500 to GBP 80,000. In at least four of these eight cases, the breach of the ePrivacy Regulations consisted in sending emails to individuals who had previously opted out from direct marketing emails, to ask for a renewal or update of their direct marketing/privacy preferences. The ICO has judged these type of communications to be direct marketing communications (which are therefore prevented in relation to individuals who have opted out).

b. DP Act

As in previous years, the ICO has continued to issue monetary penalties for serious breaches of the DP Act, the majority of which relate to (i) data security breaches or, in any case, violations of the information security principle; or (ii) violations of the transparency and fair processing principles in the charity sector (in particular, with respect to wealth screening/individual profiling for fundraising purposes). The ICO issued 23 monetary penalties between December 2016 and November 2017 for breaches of the DP Act, the total of these monetary penalties together being GBP 1,037,000. The monetary penalties issued ranged from GBP 1,000 to GBP 150,000. However, in January 2017, the ICO issued a fine of GBP 400,000 against a large mobile phone retailer in relation to an external cyber attack leading to the organization’s computer systems losing significant amounts of Personal Data including customer and employee records as well as historic transaction details. This is the equal highest monetary penalty issued by the ICO to date in relation to a breach of the DP Act (a penalty of the same amount had been imposed in 2016 on a TV, broadband, mobile and phone provider, which was subject to a cyber attack which exploited vulnerabilities on webpages by using an SQL injection attack). The ICO focused on what it saw as a series of basic errors which a large company should not have allowed to happen. Notably, even though there was no evidence of actual harm caused by this particular attack, the ICO focused on the absence of measures and the resulting risk of actual (and substantial) harm.

**Recent case law**

In 2017, there have been some significant data protection case-law developments in the UK. Notably, in *Various Claimants vs WM Morrisons*
Supermarket PLC\(^1\) the English High Court found the employer (Morrisons) vicariously liable for a significant data breach caused by a rogue employee which affected Personal Data (including payroll data) of almost 100,000 employees. This is one of the first class-action type claims for data protection law breaches in the UK (5,518 employees joined this claim). As the claimants were successful, this judgment opens the door to potentially very significant liabilities of employers (Data Controllers), even where each individual loss is small. Morrisons was also held vicariously liable for the criminal actions of its rogue employee. The Court did acknowledge that this is a difficult issue, and gave leave to appeal. Importantly though, other than breach of the seventh data protection principle (see below) Morrisons did not have primary liability for breach of the DP Act or breach of confidence – that would only be the case if Morrisons authorised or permitted the misconduct. Employees claimed Morrisons was liable for breaches of several of the DP Act’s principles. The only principle Morrisons was found to have breached was the seventh principle, i.e., the requirement to ensure appropriate technical and organization security measures to protect the data. Retention of the data, and a lack of clear procedure to address data deletion in this case, was a significant issue and Morrisons should have addressed it. On the facts, however, it was found not to have caused the unauthorized disclosure.

In Dawson-Damer & Others vs Taylor Wessing LLP ("Dawson-Damer")\(^2\) the Court of Appeal decided on a the validity of a Data Subject access request. In particular, this judgment has established that (i) there is no requirement in the DP Act that a Data Subject access request must have no other purpose other than accessing and verifying the accuracy of Personal Data. In other terms, the fact that the requester acts for a collateral purpose (e.g., for disclosure of information for litigation purposes) does not per se affect the validity of the access request; and (ii) the “disproportionate effort” exemption to the Data Subject access right in the DP Act is not to be construed narrowly and it is for the Data Controller to prove that the production of the relevant data by finding it and supplying it will be disproportionate. The ICO has updated its guidance on the issue as a result.

3. Law Applicable


The Privacy and Electronic Communications Regulations 2003 effective 11 December 2003 (as amended), implementing the ePrivacy Directive (2002/58/EC) (as amended) ("ePrivacy Regulations").

---

\(^1\) [2017] EWHC3113 (QB).
\(^2\) [2017] EWCA Civ 74.
4. Key Privacy Concepts

a. Personal Data
The DP Act applies to the processing of any data ("Personal Data") relating to an identified or identifiable living individual ("Data Subject"). The ICO has issued guidance on the classification of data as Personal Data. In general, the guidance suggests that in most cases it will be obvious whether or not data will be considered Personal Data. The primary question to consider is “Can a living individual be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the Data Controller?”

The ICO has also issued guidance with a view to clarifying what is “data” for the purposes of the DP Act. The guidance aims to help organizations determine whether information falls within any of the five categories of data covered by the DP Act, including automatically processed data; data forming part of a relevant filing system; data forming part of an accessible record; and data recorded by a public authority.

The concept of Personal Data remains unchanged under the GDPR. In addition, the GDPR specifies that online identifiers such as (at least static) IP addresses and cookie identifiers are Personal Data (to the extent they can be associated with an individual through other available data).

b. Data Processing
“Processing” is extremely widely defined and covers any operation or set of operations performed on Personal Data including collection, recording, organization and deletion. The DP Act applies to both manual and automated data processing.

The concept of data processing remains unchanged under the GDPR.

c. Processing by Data Controllers
The DP Act applies to those persons who determine the purposes for which and the manner in which any Personal Data is, or is to be, processed ("Data Controller").

The GDPR introduces the concept of Joint Controllers (as previously developed in regulatory guidance). Joint Controllers are two or more persons who jointly determine the purposes and means of data processing. The GDPR also introduces obligations which apply directly to Data Processors (and direct liability of Data Processors for breaches of those obligations), i.e., persons who process Personal Data on behalf of a Data Controller.
d. Jurisdiction/Territoriality
The DP Act applies to data processing activities carried out by:

- Data Controllers established in the UK; and
- Data Controllers that are not established in the EEA but that use equipment located in the UK to carry out data processing activities (other than merely for the purpose of transit).

The ICO has indicated that “use of equipment” may include, for example, the hosting of a website within the UK or the use of cookies (i.e., if cookies are placed on the computers of internet users within the UK).

Under certain circumstances, the GDPR extends its applicability to Data Controllers and Data Processors which are established outside of the UK and EU (e.g., when offering goods or services to individuals in the EU). What precisely “in the EU” means will need to be explained through case law and experience: it does not relate simply to citizenship of or residence in an EU Member State.

e. Sensitive Personal Data
The DP Act imposes additional requirements for the processing of Sensitive Personal Data – that is, Personal Data relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offense, or criminal proceedings. Specifically, the processing of Sensitive Personal Data is prohibited unless one of a number of stated conditions is met. These include:

- the Data Controller obtains the explicit consent of the Data Subject (see Section 5(b) below);
- the processing is necessary to carry out the obligations or rights of the Data Controller in connection with employment;
- the processing is necessary to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent or the Data Controller cannot reasonably be expected to obtain consent;
- the processing is carried out in the course of legitimate activities by any body or association which is not established or conducted for profit and which exists for political, philosophical, religious or trade union purposes and provided other specific conditions of processing are met;
- the information contained in the Personal Data has been made public as a result of steps deliberately taken by the Data Subject;
• the processing is necessary for the purpose of legal proceedings, obtaining legal advice or for establishing, exercising or defending legal rights;

• the processing is necessary for the administration of justice, for the functions of Parliament, for the exercise of powers conferred on a person under an enactment or for the exercise of functions of the Crown, a Minister or of a government department;

• the processing is necessary for medical purposes and is undertaken by a health professional or person with the equivalent duty of confidentiality as a health professional;

• the processing is of Sensitive Personal Data consisting of information on racial or ethnic origin and is necessary for reviewing and ensuring equality of opportunity and treatment between different racial or ethnic origins and provided appropriate safeguards for the rights and freedoms of Data Subjects are in place; or

• the information is about a criminal conviction or caution, and the processing is necessary for the purpose of administering an account relating to a payment card (or for cancelling the payment card) used in the commission of one of certain listed offenses relating to indecent images of children and for which the Data Subject has been convicted or cautioned under the relevant legislation in England and Wales, Scotland or Northern Ireland.

The conditions for processing Sensitive Personal Data remain broadly unchanged under the GDPR. The GDPR expands the definition of Sensitive Personal Data to include biometric data and genetic data.

f. Employee Personal Data

Employers inevitably have to process both sensitive and non-Sensitive Personal Data about their employees. Sensitive data in the employment context typically consists of information relating to employees' physical or mental health, sexual life, religion, racial or ethnic origin, and trade union membership, etc.

The ICO has published a detailed Employment Practices Code, which is a practical guide to how the ICO considers employers can comply with the DP Act in relation to employee data. The Code is not legally enforceable, but is likely to be taken into account by courts when enforcing the DP Act and, therefore, compliance with it is very much recommended. In addition, in June 2017, the Article 29 Working Party issued Opinion 2/2017 on Data Processing at Work (which takes into account the GDPR).

Provided that an employer is careful about the type of data that it obtains from employees and complies with the data protection principles set out in the DP
Act (e.g., the data collected is adequate, relevant and not excessive and is processed for limited purposes), the employer is generally able to justify processing non-Sensitive Employee Personal Data without the need to obtain employee consent (consent of the Data Subject is one of the conditions for processing non-Sensitive Personal Data set out in the DP Act). It can do so if one of the other processing conditions set out in the DP Act are met, for example, if: (i) it is necessary to perform the employment contract; (ii) it is necessary to comply with a legal obligation to which the employer is subject; or (iii) it is in the employer’s legitimate interests and does not unduly prejudice the employee’s right to privacy or other rights.

The restrictions on processing Sensitive Employee Personal Data are more stringent. In order to do so, additional processing conditions must be met. For example, the employer can process sensitive Personal Data where it is necessary: (i) to perform or exercise any right or obligation imposed by law in connection with their employment; (ii) for the purpose of or in connection with legal proceedings or to obtain legal advice; or (iii) to establish, exercise or defend legal rights. For example, health information can be processed for the purposes of ensuring the employee is kept safe at work and appropriate adjustments are made to their working environment, and information about an employee’s ethnic or racial origin may be processed for the purpose of meaningful equal opportunities monitoring, although typically that should be done in an anonymized form whenever practicable.

Where the other processing conditions cannot be met, a fallback justification for processing both sensitive and non-Sensitive Employee Personal Data is obtaining employee consent (or “explicit” consent in the case of Sensitive Personal Data). However, this is not recommended, partly because of the difficulties of obtaining every employee’s consent, and also because the ICO has expressed significant doubts about the validity of consent in the employment context, because of the inequality of bargaining power (as confirmed in the ICO draft GDPR consent guidance, adopted on 2 March 2017).

In addition to the above, employers should ensure that all employee personal and Sensitive Personal Data is accurate and up to date, is kept securely, and is not retained for longer than is necessary (see Sections 8 and 12 below).

5. **Consent**

a. **General**

Consent of the Data Subject is not mandatory although it is contemplated as a justification for processing, and in practice can be one of the more straightforward ways to justify processing. Written consent is not required. Consent is not defined in the DP Act. However, the ICO’s Legal Guidance on the DP Act explains that:
• in order for the Data Subject to signify his/her agreement to Personal Data relating to him/her being processed, there must be some active communication between the parties;

• the adequacy of any consent or purported consent must be evaluated; and

• consent must be appropriate to the particular circumstances.

The GDPR significantly strengthens the requirements for obtaining valid consent (e.g., implied consent is no longer accepted as valid consent). Draft guidance on GDPR consent requirements has been issued by the Article 29 Working Party (draft guidelines on consent under GDPR, adopted on 28 November 2017) and ICO (draft GDPR consent guidance, adopted on 2 March 2017). It must not be assumed that valid consent under the DP Act is valid consent under the GDPR: all DP Act consents should be reviewed.

b. Sensitive Data

Where consent is relied upon to justify the processing of Sensitive Personal Data, it must be explicit. The ICO’s Legal Guidance on the DP Act explains that “explicit consent” must be absolutely clear and should cover the specific detail of the processing, the particular type of Personal Data to be processed (or even the specific information in question), the purposes of the processing and any special aspects of the processing which may affect the individual. (See Section 4(e))

The requirement that consent which justifies the processing of Sensitive Personal Data must be explicit remains unchanged under the GDPR and has been interpreted by the Article 29 Working Party as meaning an “express statement of consent” (draft guidelines on consent under GDPR, adopted on 28 November 2017).

c. Minors

The DP Act does not specify a minimum age at which a child can provide valid consent. The ICO has, moreover, taken the view that to attempt to do so would not be advisable, as much will depend on the capacity of the child and the complexity of the proposition that is being put to him. On this point (and specifically in the context of the online processing of Personal Data), the ICO has stated that “assessing understanding, rather than merely determining age, is the key to ensuring that Personal Data about children is collected and used fairly”. There is a distinction drawn, however, between children under the age of 12, who are considered incapable of providing valid consent to the processing of their Personal Data (and in respect of whom the explicit and verifiable consent of a parent or guardian should be obtained), and children between the ages of 12 and 16. In the case of the latter, the ICO considers that such a child may be capable of providing valid consent if the information collected is restricted to that necessary to enable the child to be sent further
but limited communications and it is clear that the child understands what is involved. That said, the position for children between 12 and 16 is recognized as a “grey area” and the above is offered as guidance only and should not be assumed to apply in all cases. For example, the ICO has stated (again in the context of the online processing of Personal Data) that organizations may decide to obtain parental consent for children aged over 12 where there is a greater risk. In the case of children over 16, there is a presumption that they are capable of providing valid consent.

The GDPR requires that where data processing for the offer of information society services is based on consent, consent should be obtained from the holder of parental responsibility for children below a certain age (to be set by Member States between 16 and 13). The current draft of the UK Data Protection Bill sets the age at 13 years but it is uncertain, at the time of writing, whether this will remain or be subject to additional conditions.

d. Employee Consent

In the UK, there are doubts as to whether consent given in the context of an employment relationship can be considered valid. It is questionable whether consent would qualify as “freely given”, as the employee may feel forced to consent due to the subordinate nature of their relationship with their employer.

An employer can process Personal Data without employee consent if one of the other processing conditions set out in the DP Act are met, for example, if: (i) it is necessary to perform the employment contract; (ii) it is necessary to comply with a legal obligation to which the employer is subject; or (iii) it is in the employer’s legitimate interests and does not unduly prejudice the employee’s right to privacy or other rights. However, there are stricter requirements when employers are processing employee’s Sensitive Personal Data (see Section 4(f)).

These requirements and approach to consent in the employment context remain unchanged under the GDPR.

e. Online/Electronic Consent

In the UK, online or electronic consent is permissible and deemed effective if properly structured and evidenced. Guidance on online/electronic consent under the GDPR has been provided by Article 29 Working Party (draft guidelines on consent under GDPR, adopted on 28 November 2017) and ICO (draft GDPR consent guidance, adopted on 2 March 2017)

6. Notice Requirements

An organization that collects Personal Data must provide Data Subjects with information on: the name of the Data Controller; the purposes for which the data is intended to be processed; and any additional information which is necessary to ensure that the processing is fair in the circumstances (this
might include the identity of any third parties to whom the Personal Data may be transferred). Where data is obtained from a third party, the Data Controller will not have to provide this information where to do so would involve “disproportionate effort” or where collection or disclosure of the data is necessary for the Data Controller’s compliance with a legal obligation. The ICO has issued a code of practice which provides guidance on privacy notice requirements for Data Controllers.

The GDPR has significantly strengthened notice requirements and, in particular, requirements around information to be provided with the privacy notice (content of the privacy notice). The Article 29 Working Party has issued draft guidelines on transparency under GDPR.

7. Processing Rules

A Data Controller is required to process Personal Data fairly and lawfully. Personal Data can only be obtained for one or more identified purpose(s) and must not be further processed in any manner which is incompatible with those purposes. Data Controllers must ensure that Personal Data is adequate, relevant and not excessive in relation to the purposes for which it is processed. Data Controllers must not keep Personal Data for longer than is necessary for the purpose for which it is processed. Data Controllers must ensure that Personal Data is accurate and where necessary kept up to date. In addition, Data Controllers must adopt appropriate technical and organizational security measures (see Section 12), comply with the rules regarding international data transfers (see Section 11) and respect the rights of Data Subjects (see Section 8).

These principles and requirements of data processing remain unchanged under the GDPR.

8. Rights of Individuals

Data Subjects have the right to: be informed by a Data Controller upon written request of the Personal Data which the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; request the correction of the Data Subject’s Personal Data; request the deletion and/or destruction of the Data Subject’s Personal Data in certain limited circumstances.

The GDPR strengthens these Data Subject rights and it introduces new rights such as the right to data portability and the right to restriction of processing.
9. Registration/Notification Requirements

Data Controllers are required to file a notification with the ICO, which maintains a public register of Data Controllers. There are exemptions from notification for certain types of processing.

The GDPR has abolished the general requirement for organisations to register with their supervisory authority.

10. Data Protection Officers

In the UK, there is no requirement to appoint or designate a data privacy officer (“DPO”) or other individual who will be accountable for the privacy practices of the organization.

The GDPR introduces the obligation to appoint a DPO under certain circumstances, although the requirements in the UK are unlikely to be as prescriptive as in other EU Member States. The Article 29 Working Party has issued guidelines on DPOs (adopted on 5 April 2017).

11. International Data Transfers

Transfers of Personal Data from the UK to EEA Member States are generally permitted without the need for further approval. Transfers are also permitted to Canada, Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Andorra, Israel, Switzerland, New Zealand and Uruguay, which are the subject of the European Commission’s findings of adequacy (subject to the fulfillment of certain pre-conditions) in relation to their data protection laws. As of 1 August 2016, transfer to the US is permitted where the recipient has signed up to the EU-US Privacy Shield arrangement.

Subject to the specific authorizations mentioned above, Personal Data may not be transferred to countries outside the EEA, unless the destination country provides adequate protection of the Personal Data, which is determined by the Data Controller in the first instance. Exceptions to this general prohibition are, however, expressly contemplated under the DP Act, including where:

- the Data Subject has consented to the transfer;
- the transfer is necessary to perform a contract with the Data Subject, or to take steps at his request with a view to entering into a contract with him;
- the transfer is necessary for the conclusion or performance of a contract entered into between the Data Controller and third parties in the interests of, or at the request of, the Data Subject;
- the transfer is necessary to protect the vital interests of the individual, or for reasons of public interest, or in connection with legal proceedings, or
for the purpose of obtaining legal advice or establishing, exercising or defending legal rights; or

- the transfer has been specifically authorized by the ICO, or is made on terms which are of a kind approved by the ICO. This is the language in the DP Act itself. In practice, however, the ICO has indicated it does not propose to approve any forms of terms for the transfer of Personal Data.

The adoption of model contractual clauses approved by the European Commission will also provide an adequate level of protection to justify the transfer. (Note that the Data Controller must in any event justify all of its data processing under the DP Act; justification of any transfers is an additional compliance requirement.) Unlike many other EU Member States, if a transfer contract is used it will not need to be filed or approved by the ICO, whether before or after any transfers take place.

Where multinational organizations are transferring personal information outside the EEA, but within their group of companies, they may also adopt BCR as a means of justifying such intra-group transfers. Acceptable BCR may include intra-group agreements, policies or procedures, and special arrangements among the group of companies that afford the requisite protection. The ICO, along with twenty other DPAs across the EEA have agreed to mutually recognize BCRs approved by one of these 21 DPAs. For BCR to enable the transfer of personal information freely within a corporate group, they must be approved by at least one DPA that has agreed to mutually recognize BCR applications, and by any remaining DPAs in EEA countries from which the organization transfers Personal Data and which have not agreed to mutual recognition of BCR applications. The Article 29 Working Party has adopted a model checklist and table setting out the required contents of an application to a data protection authority for approval of proposed BCR. As at 9 February 2018, a total of 33 BCR authorizations had been granted by the ICO.

The GDPR maintains the previous data transfer mechanisms (with appropriate safeguards). In particular, under the GDPR new model contractual clauses could be issued by the EU Commission (which would replace the current model contract clause based on Directive 95/46/EC); and for the first time BCRs are formally recognized by law.

Furthermore, the GDPR introduces new data transfer mechanisms (with appropriate safeguards), e.g., adherence to an approved code of conduct or approved certification mechanism.

With respect to UK-EU data transfers after the UK exits the EU, the UK government has announced its intention to seek mutual recognition of adequacy status between the UK and the EU (meaning that free data flows between the UK and EU states will be allowed, with no need to put in place a
data transfer mechanism), as noted at section 1. Such an arrangement between the UK and the EU will depend, among other things, on the outcome of the Brexit negotiations.

12. Security Requirements

Data Controllers are required to take steps to ensure that Personal Data in its possession and control (and where processed by a Data Processor on the Data Controller’s behalf) are protected from unauthorized or unlawful access and use and accidental loss, destruction or damage; implement appropriate physical, technical and organization security safeguards to protect Personal Data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved and the harm that may result from unauthorized or unlawful access and use and accidental loss, destruction or damage. The ICO considers encryption as an important security measure (although not expressly required) and it has issued guidance on encryption.

Under the GDPR, Data Processors can be directly liable for breaches of the information security obligation (in addition to Data Controllers). The GDPR also provides some examples of possible security safeguards, e.g., encryption and introduces the concepts of data protection by design and data protection by default.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Where Personal Data is processed on behalf of a Data Controller, the Data Controller is under an obligation to: (a) ensure that it has chosen a Data Processor which provides sufficient guarantees in respect of the technical and organization security measures governing the relevant processing; (b) take reasonable steps to ensure compliance by the Data Processor with those measures; and (c) enter into a written contract with the Data Processor which requires the Data Processor to act only on instructions from the Data Controller, and to comply with obligations equivalent to those imposed on the Data Controller with regard to adopting appropriate technical and organization measures against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data (including taking reasonable steps to ensure the reliability of any employees who have access to the Personal Data). In addition, if the Data Processor is located outside the EEA the contract with the Data Processor will need to address the issues outlined in Section 11 above.

Also, guidance from the ICO emphasizes the importance of the Data Controller’s due diligence and ongoing monitoring (e.g., regular reports or inspections) of the Data Controller’s chosen Data Processor.
The GDPR mandates specific requirements that the processing agreement between the Data Controller and the Data Processor must address. In September 2017, the ICO has issued draft guidance on contracts and liabilities between Controllers and Processors under the GDPR.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in civil actions or criminal proceedings being brought by the ICO and/or private rights of action by Data Subjects.

The GDPR strengthens the remedies available to Data Subjects against Data Controllers’ breaches and extends such remedies against Data Processors’ breaches. The GDPR also establishes the maximum amount of administrative fines that national supervisory authorities can issue (although the determination of the amount of fines remains in the discretion of national supervisory authorities). On 3 October 2017, the Article 29 Working Party issued Guidelines on the application and setting of administrative fines for the purposes of GDPR.

15. Data Security Breach

The ePrivacy Regulations require providers of public communications services (e.g., telecoms operators and internet service providers) to notify the ICO of security breaches which lead to the loss or disclosure of Personal Data and also to notify the relevant individuals if the breach is likely to affect their privacy. This notification obligation applies to all security breaches, and not just serious breaches. As a result of the Commission Regulation (EU) 611/2013 (“Notification Regulation”), such security breaches must be notified to the ICO within 24 hours of detecting a breach, along with information about the breach (where feasible). In addition, full details of the security breach need to be provided to the ICO within three days but where this is not possible a justification for the delay must be provided to the ICO with full details to follow without undue delay. In addition, although not required by the ePrivacy Regulations, the ICO has stated that organizations should also submit the log of breaches (required to be maintained under the ePrivacy Regulations) to the ICO on a monthly basis. The ICO has published guidance in relation to the notification of security breaches required under the ePrivacy Regulations as a result of Commission’s Notification Regulation.

Other than the obligations on telecoms operators and internet service providers, until 25 May 2018 (when the GDPR starts applying) there is no other general obligation on Data Controllers to notify either individual Data Subjects or the ICO in the event of a data security breach. However, the ICO has issued guidance which sets out the circumstances in which serious data security breaches should be notified to the ICO. In addition, specific sectors may be subject to specific legal or regulatory requirements or codes of
practice which in some circumstances require notification of security breaches.

Under the GDPR, every Data Controller which suffers a data security breach is under an obligation to notify the breach to the competent supervisory authority within 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the Data Subjects. Data Controllers must also communicate the breach to the Data Subjects concerned without undue delay if the breach is likely to result in a high risk to the Data Subjects. Data Controllers are required to maintain internal records of every data security breach they suffer. Data Processors are required to notify every data security breach to the Data Controller(s) without undue delay after becoming aware of the breach. On 3 October 2017, the Article 29 Working Party issued draft guidelines on Personal Data breach notification under GDPR.

Once the Network and Information Security Directive (EU/2016/1148) (“NIS Directive”) is implemented in the UK, Operators of Essential Services and Digital Service Providers will be required to adopt appropriate and proportionate security measures to protect and ensure the continuity of the services they provide while managing security risks and be required to notify the competent authority of incidents that have a significant (for Operators of Essential Services) or substantial (for Digital Service Providers) impact on the services they provide.

16. Accountability

Until 25 May 2018 (when the GDPR takes effect), there is no law in the UK that requires organizations to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data. However, the ICO has published a code of practice on conducting privacy impact assessments which sets out the basic steps an organization should carry out during the assessment process and includes a template that can be used to help produce a privacy impact assessment report.

The GDPR introduces the accountability principle. This requires Data Controllers to be able to demonstrate compliance with the GDPR obligations by, e.g., developing and maintaining records of processing activities and carrying out (and documenting) a data protection impact assessment where a data processing activity, in particular using new technologies, is likely to result in a high risk to Data Subjects.

17. Whistle-Blower Hotline

Whistle-blower hotlines may be established in the UK.
18. E-Discovery
When implementing an e-discovery system, an organization is required to advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information. Guidelines and recommendations on data processing at work (including, e.g., monitoring activities) have been provided by the Article 29 Working Party in its opinion 2/2017 of 8 June 2017 (taking into account GDPR obligations).

19. Anti-Spam Filtering
When implementing an anti-spam filter solution into its operations, an organization is required to ensure that any interception is proportionate (i.e., does not entail blanket monitoring), is for a legitimate business purpose and that notice is provided to all users. Guidelines and recommendations on data processing at work (including, e.g., monitoring activities) have been provided by the Article 29 Working Party in its opinion 2/2017 of 8 June 2017 (taking into account GDPR obligations).

20. Cookies
There are specific rules that regulate the deployment of cookies under the ePrivacy Regulations (which implement the ePrivacy Directive). Consent must be obtained before cookies can be used, other than for cookies which are strictly necessary for the service requested by the user. The ICO had stated in its guidance that implied consent could be relied upon in certain circumstances. However, under the GDPR implied consent is no longer deemed as valid consent (as it must be expressed unambiguously by a statement or a clear affirmative action). In general, the GDPR has strengthened the requirements for the validity of consent. The GDPR consent requirements also apply to cookie consent.

A draft ePrivacy regulation is currently pending and subject to the legislative process at EU level. Once adopted, this regulation will replace the current ePrivacy Directive (which sets out the current regime on cookie consent).

21. Direct Marketing
Both the DP Act and ePrivacy Regulations contain rules on direct marketing and the ICO has also published guidance on these rules. The ICO indicates that where consent is required for direct marketing, organizations must be able to demonstrate that consent was knowingly given, clear and specific, and organizations should keep clear records of such consent. The ICO recommends that organizations should use opt-in boxes if possible. The ICO also highlights that the rules on calls, texts and emails are stricter than the rules on mail marketing, and consent in relation to marketing via calls, texts and emails must be more specific. The ICO discourages organizations from taking a one-size-fits all approach in relation to direct marketing. The ICO
emphasizes the importance of carrying out rigorous checks before relying on indirect consent (e.g., consent originally given to a third party) and that indirect consent is unlikely to be sufficient for direct marketing via calls, texts or emails, particularly if the consent is generic or non-specific. In addition, the ICO states that organizations must not carry out automated pre-recorded marketing calls without specific prior consent and must not send marketing texts or emails to individuals without their specific prior consent (with the limited exception for existing customers for similar services).

As noted above, the GDPR has strengthened the requirements for the validity of consent. The GDPR consent requirements also apply to direct marketing consent. Do not rely on pre-GDPR consents for post-GDPR processing without reviewing them to ensure they comply with the GDPR.

A draft ePrivacy regulation is currently pending and subject to the legislative process at EU level. Once adopted, this regulation will replace the current ePrivacy directive (which sets out the current regime on direct marketing).
United States

Amy de La Lama
Chicago
Tel: +1 312 861 2923
amy.delalama@bakermckenzie.com

Lothar Determann
Palo Alto
Tel: +1 650 856 5533
lothar.determann@bakermckenzie.com

Michael Egan
Washington, D.C.
Tel: +1 202 452 7022
michael.egan@bakermckenzie.com

Helena Engfeldt
San Francisco
Tel: +1 415 984 3842
helena.engfeldt@bakermckenzie.com

Heather Mantegna Fitzwater
Chicago
Tel: +1 312 861 8808
heather.mantegna@bakermckenzie.com

Brian Hengesbaugh
Chicago
Tel: +1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Lindsay Martin
Chicago
Tel: +1 312 861 2949
lindsay.martin@bakermckenzie.com

Brandon Moseberry
Chicago
Tel: +1 312 861 8265
brandon.moseberry@bakermckenzie.com

Michael Stoker
Chicago
Tel: +1 312 861 2870
michael.stoker@bakermckenzie.com

Harry Valetk
New York
Tel: +1 212 626 4285
harry.valetk@bakermckenzie.com
The United States has enacted numerous privacy laws at the federal and state levels to address data privacy and security, specifically with respect to different industries, Data Subjects, activities and data categories. These privacy laws are continuously updated and refined to cover new technologies, business models, threats and other factors. The United States opted for specific legislation in lieu of one omnibus data protection law, as is the case in Europe.

Every business in the United States is subject to privacy laws at the federal and state levels. California in particular has been very active in passing new privacy laws as described further in our separate chapter on California privacy laws in this Handbook.

Many federal and state privacy laws also apply to companies that are based in other countries and collect Personal Data from people in the United States, for example, via the Internet or mobile apps. US federal and state privacy laws and other privacy requirements are actively enforced by federal and state authorities, and are aggressively enforced via class action lawsuits and privacy-related litigation.

1. A Multitude of Federal and State Privacy Laws

The first challenge that any business faces in the United States is to identify the privacy laws that apply to its business operations. There are a multitude of federal and state privacy laws. Some privacy laws focus on particular industries, such as: (i) health care privacy rules under the Health Insurance Portability and Accountability Act and comparable state laws; (ii) financial services privacy rules under the Gramm-Leach-Bliley Act and comparable state laws; and (iii) telecommunications privacy rules for customer proprietary network information under the Telecommunications Act of 1996.

Some privacy laws focus on particular activities, such as:

- the Fair Credit Reporting Act, which applies to companies that gather and share certain data about consumers for credit, employment and other specified purposes (“consumer reporting agencies”), as well as companies that use consumer reports (“users”), companies that furnish data to consumer reporting agencies (“furnishers”), employers who use consumer reports for background check purposes and other businesses that engage in certain activities (such as printing consumer credit card numbers on receipts); and

- the Electronic Communications Privacy Act and comparable state laws, which generally apply to, among other activities, the interception of wire, oral, or electronic communications, and access to certain stored communications.
Other privacy laws specifically protect certain **Data Subjects**, for example the Children’s Online Privacy Protection Act, which protects children under 13 with respect to online collection of personal information.

Some privacy laws focus on particular **data categories**, such as certain laws in California and Massachusetts, and a large number of other state data security and breach notification requirements, which apply to social security numbers, bank account numbers, credit card numbers, health information, and a broad range of other sensitive data fields.

### 2. Federal Trade Commission and State Attorneys General

Beyond the specific privacy laws and regulations, the Federal Trade Commission (“FTC”) has broad authority pursuant to Section 5 of the FTC Act to take action against businesses that engage in certain “unfair or deceptive” trade practices. The FTC has traditionally used this authority to pursue companies that engage in “deceptive” practices, such as violating consumer privacy policies. The FTC has expanded the use of its authority to take actions against companies that engage in “unfair” practices, meaning practices that are disclosed in a privacy policy, but nevertheless are deemed by the FTC to be contrary to consumer expectations or otherwise harmful. The trend toward more robust enforcement that moves beyond merely enforcing the company’s privacy policy is continuing. In *FTC v Wyndham Hotels*, the FTC prevailed in federal courts against complaints that it is exceeding its authority by creating federal privacy law without a legislative mandate to do so. The outcome of the case has encouraged the FTC’s ability to continue and expand its efforts, and to even more aggressively exercise its fairness enforcement power in privacy and security cases.

For these reasons, businesses must address requirements established by the FTC regarding complaints and consent decrees, as well as follow the FTC’s guidance on privacy matters available here ([https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business](https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business)). In 2016, the FTC released new guidance for developers of mobile health apps and recommendations to businesses on the growing use of big data. In 2015, the FTC issued a report on the “Internet of Things” and urged companies to adopt best practices to address consumer privacy and security risks. In 2014, the FTC issued guidance on privacy protection for children online, which affirmatively states that the US Federal Children Online Privacy Protection Act applies to foreign companies that collect Personal Data from children in the United States, US companies that collect Personal Data from children abroad, and companies that act as mere Data Processors or collect data about children under 13 via cookies on third-party websites.

Beyond the FTC actions, many State Attorneys General also have broad authority to pursue unfair or deceptive practices pursuant to state powers (often called “Mini-FTC Acts”). An important recent trend has involved greater
collaboration between and among State Attorneys General to pursue actions against companies that experience data security breaches or other privacy issues. Such coordinated actions can often exact greater penalties and impose increased demands on companies than what would otherwise be required by the FTC.

3. US Law Enforcement and Other Legal Demands

Beyond federal and state privacy laws, there are various related federal and state requirements to produce information to law enforcement and regulatory authorities, to gather data for purposes of global internal investigations, and to respond to e-discovery and other demands for data in civil litigation. By way of a few examples, companies may be ordered to produce information pursuant to: (i) a search warrant executed by federal or state criminal authorities; (ii) an order for the interception of electronic communications by criminal authorities pursuant to federal or state wiretap acts; (iii) a grand jury subpoena issued by federal or state criminal authorities; (iv) a trial subpoena issued by federal or state criminal authorities; (v) an administrative subpoena issued by federal or state regulatory authorities; and (vi) a civil subpoena seeking the production of documents in connection with civil litigation.

Some of these US legal demands, including orders under the USA Patriot Act (which was superseded by the USA Freedom Act in 2015), have attracted considerable attention in non-US jurisdictions and such attention has increased dramatically in the wake of the publicity around surveillance programs by the US NSA and cooperating intelligence agencies in Australia, Canada, New Zealand and the UK (part of the “Five Eye” alliance) and other US allies, including Germany (Bundesnachrichtendienst). Compared to other jurisdictions, US laws protecting data privacy in connection with government surveillance actually fare quite well, as demonstrated by Baker McKenzie’s 2017 Global Surveillance Survey, which includes heat maps and a country-by-country comparison, available here: (http://globalitc.bakermckenzie.com/surveillance/).

As a reaction to international and domestic criticism, the US government enacted the USA Freedom Act (restoring, modifying and repealing provisions of the USA Patriot Act) and the US Judicial Redress Act (extending the reach of certain US privacy law provisions to citizens in the EU and other allied nations) and created various new administrative safeguards, including appointing privacy officers at the agencies and creating a privacy oversight board that has published a scathing report, declaring some of the existing programs that are unconstitutional and illegal under US law. A number of lawsuits against these and other programs are working themselves through the US court system with wins for plaintiffs, which include the American Civil Liberties Union and the Electronic Frontier Foundation and support their efforts in reigning in the activities of the US intelligence agencies. These US
government measures and court cases will help reduce the risk of potential conflicts with non-US data protection, privacy, bank secrecy, confidentiality, anti-investigatory or “blocking” statutes, and other data restrictions. In practice, companies need to be mindful of these potential conflicts when structuring their global privacy compliance programs. Also, when any such demand is received, the company should carefully assess options and approaches to help address the US and non-US requirements. For example, can the law enforcement authority at issue utilize any Mutual Legal Assistance Treaties to obtain the data directly from its counterparts in a foreign jurisdiction? Can the company assert that the data at issue is not within the company’s lawful control and therefore cannot be produced? Can the company persuasively argue against production of the data on the grounds that it may violate non-US privacy or other laws? These are a few examples, and each situation requires a careful assessment of the specific facts and the applicable US and non-US legal requirements.

4. Summaries of Key Privacy Laws

An exhaustive review of US privacy laws is outside the scope of this handbook. Instead, the following sections summarize key aspects of some key federal and state laws relating to data privacy. The federal laws covered are the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act. In addition, the handbook covers the data security regulations published by the Massachusetts Office of Consumer Affairs and Business Regulation and the security breach laws that have been enacted in most states, as illustrated by key provisions of California’s statute. As noted above, these examples do not represent an exhaustive list of applicable restrictions, but are intended as illustrations of the laws and regulations that are currently in place in the United States.
United States
California Privacy Laws

1. Recent Privacy Developments
In the last few years, California has enacted more than 50 new privacy laws and updates to existing privacy laws, including:

- CalECPA, an electronic communications privacy law that requires California law enforcement agencies to obtain a warrant before they can compel access to emails;
- data security and breach notification requirements regarding data collected through automated license plate recognition systems;
- privacy protections for connected television voice recognition features;
- privacy rules for drones to protect airspace from invasion of privacy;
- laws to penalize the offering of hacking services;
- requirements on operators of websites (within or outside the United States) that collect Personal Data from California consumers to disclose how they respond to “Do Not Track” signals and details on third-party data collection;
- a limited “right to be forgotten” for minors, requiring platform operators to enable minors to remove their own posts (but not posts reproduced by third parties);
- an extension of existing health information privacy laws to companies that offer software, hardware or online services to consumers for purposes of maintaining medical information;
- an expansion of the California data security breach notification law (covered in a separate chapter of this handbook); and
- laws intended to reign in revenge porn.

At the same time, plaintiffs' law firms have increased privacy-related class action lawsuits in California courts based on California privacy laws, including laws:

- requiring consent from all parties before calls, emails or other communications involving persons in California can be monitored, filtered or recorded;
• prohibiting retailers from collecting any Personal Data from credit card holders, even with consent, except as necessary to process credit card transactions (California Song-Beverly Credit Card Act);

• requiring companies to disclose sharing of personal information with third parties (including affiliated companies operating under different brands) for their direct marketing purposes; and

• general unfair competition laws in the context of alleged misrepresentations in privacy policies, particularly representations regarding “reasonable data security measures” in the aftermath of data security breaches.

2. Emerging Privacy Issues and Trends

Within the United States, California is usually the first to enact new legislation in the areas of data privacy and security and consumer protection more generally. California is world-renowned for innovation in the data processing and information technology fields as well as in the data privacy legislation arena. The state has successfully implemented various pieces of legislation requiring disclosures and transparency, such as California’s data security breach notification law and California’s Online Privacy Protection Act that requires companies to post privacy policies for online consumer services. Both laws were firsts worldwide and successfully copied around the world. Nearly all US states and many foreign countries have data breach notification laws now.

Less successful and burdening businesses with a flurry of painful lawsuits have been some of California’s absolute prohibitions, like the California Song-Beverly Credit Card Act, and detailed prescriptions like the “Shine the Light” law that requires companies to post a text link with “Your California Privacy Rights” on their home pages under certain circumstances, a requirement that would unnecessarily clutter webpages if every jurisdiction were to require such special mentioning in the title of a text link.

3. Law Applicable

California has enacted hundreds of sector-, activity- and data type-specific privacy laws, including some laws that have since been regulated on a federal US level and potentially been pre-empted (such as California’s anti-spam laws and laws on health and financial privacy laws). Particularly relevant, in practice, remain the following California laws:

• Under the California Online Privacy Protection Act, operators of websites and online services within and outside the United States have to post privacy policies with certain prescribed disclosures if they collect personally identifiable information from consumers in California.
• Under the California Shine the Light Law, companies have to disclose certain details of their data sharing practices if they make personal information on California consumers available for direct marketing purposes of unaffiliated companies or affiliates operating under a different brand; companies can satisfy some requirements by posting a notice under a link entitled “Your California privacy rights” on their homepage.

• Under the Song-Beverly Credit Card Act, retailers are prohibited from collecting personal information from credit card holders, even with consent, except as necessary to process credit card transactions or deliver goods or perform services.

• Under the California Penal Code, companies are prohibited from recording or monitoring calls or other communications involving persons in California, unless all persons consent.

• Under the California Civil Code, companies have to apply various data security measures and notify data security breaches, as discussed in more detail in our separate chapters on “United States – State Data Security Laws” and “United States – State Data Security Breach Notification Laws”.

4. Key Privacy Concepts

a. Personal Data
California privacy laws do not use the term “Personal Data” but refer to various other terms, including “personally identifiable information”, “personal identification information”, and “personal information”. Each statute – and often each section in a statute – tends to define the relevant term differently and often with enumerated categories of Personal Data listed.

b. Data Processing
Unlike European data protection laws, California privacy laws do not use the term “data processing” or any other similarly broad definition of “data processing”. California defines in each statute – and often each section of a statute – differently which data processing activities are covered by the particular law.

c. Processing by Data Controllers
Some California laws differentiate between Data Controllers and Processors in the same manner as European data protection laws, e.g., regarding data security breach notification laws (processors must notify controllers and controllers must notify Data Subjects and the California State Attorney General), however, many laws do not differentiate or draw different lines.
d. Jurisdiction/Territoriality
California privacy laws apply to companies in other US states and other countries in situations with a nexus to California (e.g., collection of Personal Data of consumers in California), unless a particular statute expressly states that its applicability is limited to companies in California (e.g., Section 637.7 of the California Penal Code prohibits “entities in this state” from attaching RFID tracking devices) or the applicability of the law is limited by federal US law (e.g., the “Dormant Commerce Clause” of the United States Constitution).

e. Sensitive Personal Data
California privacy laws afford special protection to US social security numbers (because of identity theft risks), credit card and banking information, health information and certain other statutorily defined data categories.

f. Employee Personal Data
Under the California Labor Code, employers are prohibited from recording video or audio of employees in restrooms or changing rooms, regardless of employee consent. Otherwise, employee privacy is only protected where employees have reasonable privacy expectations, which employers can – and usually do – negate with detailed privacy notices.

5. Consent
a. General
Companies are generally permitted to collect and process Personal Data without consent. Many California privacy laws require conspicuous notice and courts tend to assume implied consent if Data Subjects continue showing up for work, using a service or continuing other conduct after they receive notice.

b. Sensitive Data
California privacy laws afford special protections to US social security numbers (because of identity theft risks), credit card and banking information, health information and certain other statutorily defined data categories, but do not typically require consent. Notices tend to suffice.

c. Minors
California law requires operators of websites and other online services to enable minors to remove social media posts. Certain types of advertisements may not be targeted at minors.

d. Employee Consent
Employee privacy is only protected where employees have reasonable privacy expectations, which employers can – and usually do – negate with detailed privacy notices. Affirmative or express consent is not generally
required, except in certain limited scenarios, e.g., tracking of employee location with RFID technology.

e. Online/Electronic Consent
If and to the extent notice or consent is required, it can generally be provided electronically.

6. Information/Notice Requirements
In general, companies should provide detailed, accurate and conspicuous privacy notices under California law to protect and defend against charges of unfair or misleading business practices. Under most of the numerous California privacy laws, companies can defend themselves if they can prove that Data Subjects did not have a reasonable expectation of privacy. Privacy expectations can be defined, qualified or negated in notices. Therefore, privacy notices are the single most crucial measure under California privacy laws.

The risk of lawsuits arising from outdated, inaccurate or incomplete privacy notices under California law is much higher than in other jurisdictions, notably Europe.

A number of California privacy laws prescribe notice content and placement in a lot of detail. For example, under the California Online Privacy Protection Act, operators of websites and online services within and outside the United States have to post privacy policies with certain prescribed disclosures if they collect certain types of personally identifiable information from consumers in California (including, potentially, location information of Data Subjects collected on a no-name basis). In the privacy policies, companies must notify consumers about (i) data categories collected, (ii) processes to review and request changes, (iii) change notification, (iv) the policy’s effective date, (v) responses to “Do Not Track” signals or similar mechanisms, and (vi) third parties’ data collection about consumer online activities over time and across different websites.

7. Processing Rules
In addition to various sector- and data type-specific rules on data processing, California privacy laws impose numerous data security requirements that we discuss in more detail in our separate chapters on “United States – State Data Security Laws” and “United States – State Data Security Breach Notification Laws”.

8. Rights of Individuals
Most California privacy laws provide for a right of private action that can be enforced by way of class action lawsuits. The California Song-Beverly Credit
Card Act and a few other laws provide for statutory penalties, so plaintiffs’ attorneys do not have to substantiate individual damages.

9. Registration/Notification Requirements
None.

10. Data Protection Officers
Not generally required, but many California companies appoint privacy officers for practical reasons.

11. International Data Transfers
Not restricted.

12. Security Requirements
Discussed in more detail in our separate chapters on “United States – State Data Security Laws” and “United States – State Data Security Breach Notification Laws”.

13. Special Rules for the Outsourcing of Data Processing to Third Parties
None.

14. Enforcement and Sanctions
Companies are particularly sensitive to exposure to private lawsuits, including class action lawsuits that are very common and tend to result in judgments, settlements and legal fees in the millions of US dollars. The California State Attorney General has created a “Privacy Task Force”, which has launched criminal and civil actions against companies and individuals relating to a number of violations, including failure to post privacy policies and issue timely data security breach notifications.

15. Data Security Breach
Discussed in more detail in our separate chapter on “United States – State Data Security Breach Notification Laws”.

16. Accountability
Not specifically legislated or regulated. But, under a number of California privacy laws, companies are required or encouraged to implement protocols for employees who handle Personal Data. For example, under the California Medical Information Act, employers “shall establish appropriate procedures” which “may include, but are not limited to, instruction regarding confidentiality of employees and agents handling files containing medical information”. Companies that can prove they have appropriate procedures in place can rely
on a liability safe harbor under the California Song-Beverly Credit Card Act and California law restricting data collection in the context of processing personal checks if an individual employee makes an unintentional, bona fide mistake. Similarly, under California fair debt collections practices laws, companies can benefit from a liability safe harbor if they can prove that they maintained appropriate procedures.

17. Whistle-Blower Hotline

All public companies and more and more private companies in California operate whistle-blower hotlines. Companies that operate whistle-blower hotlines are not required to obtain any government approvals or submit government filings and are less exposed to privacy-related concerns as, for example, in Europe.

18. E-Discovery

Defendants can be compelled to produce documents and information relatively easily under California rules of civil procedure, compared to other jurisdictions. Defendants can try to protect data privacy via protective orders in this context, but rarely oppose information production obligations based on privacy theories.

19. Anti-Spam Filtering

Monitoring and filtering of electronic communication requires all party consent. Plaintiffs have challenged email filtering for marketing purposes under California and US federal privacy laws with some success, but not with respect to anti-spam or anti-virus filtering, which is generally believed not to interfere with reasonable privacy expectations and is therefore generally permitted.

20. Cookies

Cookies are not specifically regulated under California privacy laws, but a number of companies have been sued based on unfair competition and misrepresentation theories for failure to provide adequate disclosures regarding cookies in privacy policies, attempts to disable consumer attempts to block or delete certain types of cookies and placement of certain particularly intrusive tracking technologies without consent. Based on recent updates to the California Online Privacy Protection Act, operators of websites and online services must disclose in privacy policies how they respond to “Do Not Track” signals and similar privacy protection measures selected by consumers and if and to what extent third parties collect personal information regarding consumers on websites or via online services.
21. Direct Marketing

The California “Shine the Light Law” requires companies to provide certain disclosures if they share personal information with other companies for their direct marketing purposes, even to affiliated companies operating under a different brand.

California’s opt-in consent requirements have been largely pre-empted by the federal CAN-SPAM Act, which requires that companies provide certain disclosures, allow and honor opt-out requests and refrain from certain forms of email address harvesting, which does not require opt-in consent.
United States
Children’s Online Privacy Protection Act (“COPPA”)

1. Recent Privacy Developments
The Federal Trade Commission (“FTC”) continued to actively enforce COPPA in 2016. For example, in June 2016, a mobile advertising network settled FTC charges that it tracked hundreds of millions of children’s and consumers’ locations without permission.

In the last few years, areas of particular attention included:

- general audience sites (i.e., sites not explicitly directed at children) that triggered COPPA’s parental notice and consent requirements by collecting date of birth from users without blocking users from their sites who entered dates of birth that would make them under the age of 13; and
- child-directed apps offering games that also collected personal information such as geo-location and email address without obtaining parental consent.

2. Law Applicable
The Children’s Online Privacy Protection Rule (16 C.F.R. § 312.1 et. seq.) (the “Rule”), effective 1 July 2013, implementing the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et. seq.) (the “Act”), along with the FTC’s Frequently Asked Questions, providing guidance on how the FTC applies the Rule.

3. Scope of the Law
a. Personal Data
The Rule applies to the online collection of Personal Information from a child under the age of 13 (“Child” or “Children”). “Personal Information” is defined expansively and includes:

- first and last name;
- a home or other physical address, including a street name and name of a city or town;
• an email address or other online contact information, including an instant messaging user identifier or a screen name that reveals an individual’s email address;

• a telephone number;

• a social security number;

• a persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;

• a photograph, video, or audio file where such file contains a Child’s image or voice;

• geolocation information sufficient to identify street names and names of cities or towns; or

• information concerning the Child, or the parent or legal guardian of that Child (“Parent”), that the Operator (see definition below) collects online from the Child and combines with an identifier described above.

b. Personal Information Collection

The Rule applies to the “collection” of Personal Information from a Child. “Collection” is broadly defined and applies to the online gathering of any Personal Information from a Child, including:

• requesting, prompting or encouraging a Child to submit Personal Information online;

• enabling a Child to make Personal Information publicly available through a chat room, message board, or other means (e.g., social networking/blogging), except where the Operator deletes all individually identifiable information from postings by a Child before they are made public, and also deletes such information from the Operator’s records; or

• the passive tracking or use of any identifying code linked to an individual such as a cookie.

c. Collection by Operator

The Rule applies to any operator of a website or online service that is directed to Children or to any other Operator with actual knowledge that it is collecting or maintaining Personal Information relating to a Child. An “Operator” is any person (or entity) who operates a website or an online service and who collects or maintains Personal Information from or about the users of or visitors to such website or online service, or on whose behalf such information
is collected or maintained, where the website or online service is operated for commercial purposes. Personal Information is collected on behalf of an Operator when either (i) it is collected or maintained by an agent or service provider of the Operator or (ii) the Operator benefits by allowing another person to collect Personal Information directly from users of such website or online service. A website “directed to children” means a commercial website, or portion thereof, that is targeted to Children. A website which refers or links to a commercial website or online service directed to Children by using information location tools, however, does not necessarily meet this definition.

d. Jurisdiction/Territoriality
The Rule applies to the collection of Personal Information about a Child by an Operator who engages in commerce: (i) across more than one state in the US; (ii) in any state in the US and in one or more foreign nations; (iii) in any territory of the US or in the District of Columbia; (iv) in any such territory and another such territory, state or foreign nation; or (v) in the District of Columbia and any state, territory, or foreign nation.

4. Consent Requirements
a. Parental Consent
Prior to the collection, use, and/or disclosure of Personal Information about a Child, an Operator must obtain Verifiable Parental Consent from a Parent of the Child. The Rule explains that obtaining “Verifiable Parental Consent” means that the Operator must make any reasonable effort (taking into consideration the available technology) to ensure that before Personal Information is collected from a Child, a Parent: (i) receives notice of the Operator’s Personal Information collection, use, and disclosure practices; and (ii) authorizes any collection, use, and/or disclosure of the Personal Information. In addition, the Operator must provide a Parent with the option of consenting to the collection and use of the Child’s Personal Information to the Operator without having to consent to its disclosure to a third party.

The Operator also must take steps to ensure that the person providing consent is actually the Child’s Parent. Acceptable forms of consent include: (a) a consent form signed and returned by the Parent by mail or facsimile; (b) the Parent’s use, in conjunction with the transaction, of a credit card, debit card or other online payment system that provides notification of each discrete transaction to the primary account holder; (c) a call to a toll-free number provided by the Operator and staffed by trained personnel; (d) having a Parent connect to trained personnel via video-conference; (e) verifying a Parent’s identity by checking a form of government-issued identification against databases of such information, where the Parent’s identification is deleted by the operator from its records promptly after such verification is complete; or (f) the electronic forms of consent discussed below.
b. **Minor Consent**

A Child cannot consent to the collection of his or her Personal Information. This consent must instead be obtained from a Parent of the Child. The Rule does not address consent requirements for minors who are 13 or over.

c. **Online/Electronic Consent**

If the Operator does not release the Personal Information to a third party, consent may be obtained by using email coupled with additional steps to provide assurances that the person providing the consent is the Parent. Acceptable additional steps to obtain these assurances include sending a delayed confirmatory email to the Parent following receipt of consent, or obtaining a postal address or telephone number from the Parent and confirming the Parent’s consent by letter or telephone call. An Operator that uses this method must provide notice that the Parent can revoke any consent given in response to the earlier email.

d. **Exceptions to Prior Consent/Requirements**

In certain situations, the Operator is not required to obtain Parental consent before collecting and/or disclosing Personal Information about a Child. These situations include:

- where the Operator collects the name or online contact information of a Parent or Child to be used exclusively for obtaining Parental consent or providing Parental notice (the Operator must delete this information after a reasonable time if there is no response);

- where the Operator collects online contact information from a Child for the sole purpose of responding directly to a specific request from the Child on a one-time basis, and the Operator immediately deletes that online contact information immediately after responding to the Child;

- where the Operator collects online contact information from a Child to be used to respond directly more than once to a specific request from the Child; and

- where the Operator collects a Child’s name and online contact information to the extent reasonably necessary to protect the safety of a Child participating on the website.

In all of the situations described above, except for where the Operator deletes the information after responding on a one-time basis to the Child, the Operator must provide notice and seek Parental consent after the Personal Information has been collected. Moreover, the Rule generally requires that the Operator delete all contact information after the relevant transaction has been concluded. An Operator can also provide notice and seek consent after the fact to the extent reasonably necessary to protect the security or integrity of its website, to take precautions against liability, to respond to a judicial process,
to provide information to law enforcement agencies, or for an investigation on a matter related to public safety.

5. Information/Notice Requirements

The Operator must provide two types of notice. The Operator must post a prominent link to a notice of its information practices on its website’s homepage as well as any area where Personal Information is collected from Children. The notice must provide the following information:

- the contact information (name, address, telephone number, and email address) for all Operators collecting information about Children on the website;
- the types of Personal Information collected from Children and the manner of collection (passive versus active);
- how such Personal Information is or may be used by the Operator;
- whether the Personal Information is disclosed to third parties (and the types of businesses engaged in by such third parties, the purposes for which the Personal Information is used, and whether such parties are subject to agreements to protect the information);
- that the Parent has the option to consent to the collection and use of Personal Information without consenting to its disclosure to third parties;
- that the Operator is prohibited from conditioning a Child’s participation in an activity on the Child’s disclosing more Personal Information than is reasonably necessary to participate in the relevant activity; and
- that the Parent can review and have deleted his/her Child’s Personal Information and also refuse to permit collection or use of the Child’s Personal Information (the notice must also specify the corresponding procedures for doing so).

In most instances, the Operator also must provide notice directly to a Parent of the Child from whom it seeks to collect Personal Information before it collects such information. This notice must contain the information listed above. In certain limited situations, the notice may be provided after the information is collected.

6. Processing Rules

In general, the Rule prohibits unfair or deceptive acts or practices in connection with the online collection, use, and/or disclosure of the Personal Information of a Child.
7. Safe Harbor

An Operator will be deemed to comply with the Rule if it complies with self-regulatory guidelines that are issued by representatives of the marketing or online industries, or by other persons, which have been approved by the FTC. Industry groups must file a request with the FTC for approval of self-regulatory guidelines that meet the standards set out in the Rule – such requests are subject to notice and comment requirements prior to approval. Once approved, the self-regulatory program must submit annual reports regarding the efficacy of the program and any disciplinary action taken against any subject Operator. Any subsequent changes to the program also require prior FTC approval. In 2014, the FTC approved the iKeepSafe and kidSAFE Safe Harbor Program.

8. Rights of Individuals

a. Parent Access Rights

The Parent of any Child who has provided Personal Information to an Operator has the right to request access to such information. Upon receiving such a request, the Operator is required to provide the Parent with the following information:

- a description of the specific types or categories of Personal Information collected from the Child by the Operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities;
- the opportunity at any time to refuse to permit the Operator’s further use or future online collection of Personal Information from that Child, and to direct the Operator to delete the Personal Information collected from the Child; and
- a means of reviewing any Personal Information collected from the Child.

b. Child’s Rights

An Operator is prohibited from conditioning a Child’s participation in a game, the offering of a prize, or another activity on the Child’s disclosing more Personal Information than is reasonably necessary to participate in such activity.

9. Registration/Notification Requirements

No specific requirements apply.

10. Data Protection Officers

Not applicable.
11. International Data Transfers
Not restricted.

12. Security Requirements
An Operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from Children. The operator must also take reasonable steps to release Children’s personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

13. Special Rules for the Outsourcing of Data Processing to Third Parties
Persons or entities that delegate or outsource the responsibility for collecting and maintaining Personal Information from a Child are still subject to the Rule.

14. Enforcement and Sanctions
Violations of the Rule are considered to be unfair or deceptive acts prohibited by the Federal Trade Commission Act and, consequently, are subject to FTC enforcement actions and/or financial penalties (USD 11,000 per violation). COPPA also gives states and certain other federal agencies authority to enforce compliance.

15. Data Security Breach
a. Are there any legal requirements, including notification obligations, in the event of a data security breach?
The Rule does not expressly identify such an obligation.

b. Risk of non-compliance
The Act gives states and certain federal agencies, including the FTC, authority to enforce compliance with the Act. A court can impose civil penalties of up to USD 11,000 per violation on website operators who violate the Rule.
United States
Gramm-Leach-Bliley Act and Fair Credit Reporting Act

1. Recent Privacy Developments
The Consumer Financial Protection Bureau (“CFPB”) is the primary federal regulatory authority that administers the GLBA and FCRA (each as defined below), alongside other federal regulators within the scope of their authority, including but not limited to, the Federal Trade Commission (“FTC”), the Securities and Exchange Commission, and the Commodity Futures Trading Commission.

2. Law Applicable


3. Scope of the Law
a. Personal Data
GLBA requires that “financial institutions” must protect certain non-public personal information collected from or about individual consumers in connection with the provision of financial products and services – it does not apply to information collected in other contexts. Non-public personal information includes personally identifiable financial information that:

- is provided by a consumer to a financial institution;
- results from any transaction with the consumer or any service preformed for the consumer; and/or
- is otherwise obtained by the financial institution.

A company’s obligations under GLBA depend on whether the company has consumers or customers who obtain its products or services. A consumer is an individual who obtains or has obtained a financial product or service from a
A customer is a consumer with a continuing relationship with a financial institution. Generally, if the relationship between the financial institution and the individual is significant and/or long term, the individual is a customer of the institution. For example, a person who gets a mortgage from a lender or hires a broker to get a personal loan is considered a customer of the lender or the broker, while a person who uses a check-cashing service is a consumer of that service.

FCRA primarily governs the uses and disclosure of information in “consumer reports”. The definition of a “consumer report” under FCRA is broad, and it incorporates by reference the definition of a “consumer reporting agency”. Analyzing both of these terms together, a consumer reporting agency generally is any person that: (i) for fees or other compensation; (ii) regularly engages in the practice of assembling or evaluating “non-experience” information about consumers; (iii) for the purpose of disseminating such information to third parties for use in connection with the evaluation of the consumer for credit, debt collection, or other “permissible purposes;” and (iv) performs such activities in the context of interstate commerce. See Porter v Talbot Perkins Children’s Services, 355 F. Supp. 174 (SD NY 1973).

b. Data Processing
If a financial institution is within the scope of GLBA, the law will apply to the collection, use, storage, and any other activity that the institution undertakes with respect to non-public personal information.

FCRA applies to any collection, use, disclosure, or other processing of consumer reports by consumer reporting agencies. In addition, FCRA imposes certain obligations on entities that are “users” of consumer reports (e.g., use and disclosure limitations), as well as entities that furnish information to consumer reporting agencies (e.g., related to data integrity and correction of incorrect information), and various other requirements.

c. Processing by Data Controllers
GLBA does not contain a term “Data Controller” and instead coverage is defined by the term “financial institution”, as described above.

FCRA does not contain a term “Data Controller” and instead coverage is defined by the term “consumer reporting agency”, “user”, and “furnisher” as described above, as well as by other definitions.

d. Jurisdiction/Territoriality
GLBA does not contain a specific geographic limitation, but the jurisdictional reach is defined at least in part in the relevant regulations, and also by the jurisdictional reach of the relevant regulatory authority.
FCRA does not contain a specific geographic limitation, but the jurisdictional reach is defined at least in part by the jurisdictional reach of the relevant regulatory authority.

e. Sensitive Personal Data

GLBA does not include a classification of “sensitive” information, although collection of health or medical information may be subject to greater protection under state law implementation of GLBA in the insurance sector, and also may be subject to federal regulation in certain circumstances under other laws, such as the Health Insurance Portability and Accountability Act.

FCRA contains restrictions on the collection, use, and disclosure of medical information and also contains special restrictions related to identity theft, consumer reports furnished for employment purposes, and a special category of consumer reports involving personal interviews with third parties termed “investigative consumer reports”.

f. Employee Personal Data

Employee Personal Data is generally not within the scope of GLBA, except in certain instances where the employee is a consumer of financial products or services provided by the employer or its affiliate, such as in the context of a company credit union. Under FCRA, a consumer reporting agency may generally not provide a consumer report to an employer, or a prospective employer, without that employee’s or prospective employee’s written consent. Additionally, employers performing background checks on prospective or existing employees must use specific, required forms provided under the applicable regulations.

4. Consent Requirements

a. General

GLBA generally requires a financial institution to provide customers and/or consumers in certain circumstances with a privacy notice with specified content. In situations where the financial institution intends to share non-public personal information with a non-affiliated third party, GLBA generally requires that the institution must provide the consumer with notice of the opportunity to opt out of such disclosures, and must respect the expressed wishes of the consumer in this regard. There are important exceptions to these opt-out requirements, such as where the disclosure is necessary to effect, administer, or enforce the transaction, or where the disclosure is required or permitted by law. Providing some added clarity, the CFPB has issued guidance stating that disclosure in the case of suspected financial abuse of older adults would fall under one of the specified exceptions. Under FCRA, a consumer reporting agency may generally not provide a consumer report to an employer, or prospective employer, without the consumer’s written consent. A consumer reporting agency may not report medical information to creditors, insurers, or
employers without the consumer’s permission. In addition, other consent requirements may apply under FCRA in various contexts.

b. Sensitive Data
GLBA does not include a classification of “sensitive” information, although collection of health or medical information may be subject to greater protection under state law implementation of GLBA in the insurance sector, and also may be subject to federal regulation in certain circumstances under other laws, such as the Health Insurance Portability and Accountability Act.

FCRA contains restrictions on collection, use, and disclosure of medical information and also contains special restrictions related to identity theft, consumer reports furnished for employment purposes, and a special category of consumer reports involving personal interviews with third parties termed “investigative consumer reports”.

c. Minors
GLBA does not specifically establish rules related to minors, although under general principles of contract law and regulatory requirements, minors might not be able to provide valid consent because of a lack of capacity to enter into an enforceable contract.

FCRA does not specifically establish rules related to minors, although under general principles of contract law and regulatory requirements, minors might not be able to provide valid consent because of a lack of capacity to enter into an enforceable contract.

d. Employee Consent
Under GLBA, where employees also qualify as consumers or customers, the same requirements regarding notice and opt-out consent apply equally to such individuals.

For FCRA, see Section 5(a) above.

e. Online/Electronic Consent
Under GLBA, the extent to which electronic notice and opt-out consent are sufficient depends upon applicable regulations and various factors, including whether the financial institution regularly conducts transactions with the consumer electronically.

For FCRA, the extent to which electronic notice and opt-out consent are sufficient depends upon applicable regulations and various factors, including whether the consumer agrees to engage in such transaction electronically.

5. Information/Notice Requirements
Generally, under GLBA, consumers are entitled to receive a privacy notice from a financial institution only if the company shares the consumers’
information with companies not affiliated with it, with some exceptions. Customers must receive a notice at the time the customer relationship is established and annually for every year during the continuation of the customer relationship. In 2014, however, the CFPB announced a finalized rule that enables certain financial institutions to comply with GLBA by publishing their privacy notices online instead of mailing them to their customers. This new rule only applies to financial institutions regulated by the CFPB, and does not impact those entities regulated by the Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Trade Commission, or a state insurance regulator. The final rule requires the financial institution that wishes to rely on this alternative method of delivery to continuously post the annual privacy notice in a clear and conspicuous manner on a page of its website, without requiring a log-in or similar steps to access the notice. It allows financial institutions to use the alternative delivery method for annual privacy notices if:

- no opt-out rights are triggered by the financial institution's information sharing practices under GLBA or the Fair Credit Reporting Act ("FCRA") Section 603, and opt-out notices required by FCRA Section 624 have previously been provided, if applicable, or the annual privacy notice is not the only notice provided to satisfy those requirements;
- the information included in the privacy notice has not changed since the customer received the previous notice; and
- the financial institution uses the model form provided in Regulation P as its annual privacy notice.

Under FCRA, any user of a consumer report from a consumer reporting agency that takes an adverse action against a consumer based on the report – such as denying an application for credit, insurance, or employment – must notify the consumer of that fact, and give the consumer the name, address, and phone number of the consumer reporting agency that provided the consumer report. In addition, see Section 4(a) above for further requirements related to providing notice of opt-out rights in connection with sharing non-experience information among affiliates.

6. Processing Rules

In addition to the rules described above, other important provisions of GLBA also affect how a company conducts business. For example, financial institutions are prohibited from disclosing their customers’ account numbers to non-affiliated companies when it comes to telemarketing, direct mail marketing, or other marketing through email, even if the individuals have not opted out of sharing the information for marketing purposes. Another provision

---

prohibits “pretexting” – the practice of obtaining customer information from financial institutions under false pretenses.

Under FCRA, consumer reporting agencies, users of consumer reports, and furnishers of information to consumer reporting agencies are subject to a wide range of requirements with respect to the collection, use, and disclosure of this relevant information.

7. Rights of Individuals

a. Access Right

GLBA generally does not contain a right for the consumer to access and correct his or her non-public personal information.

Under FCRA, at the request of the consumer, a consumer reporting agency must provide the consumer with the information in his or her consumer report as well as a list of everyone who has requested it recently. There is generally no charge for the report if a user has taken an adverse action against the consumer because of information supplied by the consumer reporting agency. The consumer also is entitled to one free report every 12 months upon request in some instances, and has various rights to challenge the accuracy of information in his or her consumer report (as described below under “Additional Rights”).

b. Additional Rights

Consumers and customers have a wide range of other rights under applicable federal and state financial privacy regulations. For example, a significant additional right under FCRA and The Fair and Accurate Credit Transactions Act of 2003 relates to direct marketing. Specifically, when an organization markets to consumers based on information received from an affiliate, there may be a separate, additional notice and opportunity to opt-out of receiving such marketing.

With respect to consumer reporting agencies under FCRA, if a consumer tells a consumer reporting agency that his or her file contains inaccurate information, the consumer reporting agency must investigate the identified items (usually within 30 days) by providing the agency’s information source with all relevant evidence submitted by the consumer, unless the dispute is frivolous.

The information source must review the submitted evidence and report its findings to the consumer reporting agency. (The information source also must advise national consumer reporting agencies to which it has provided the data of any error.) The consumer reporting agency must give the consumer a written report of the investigation, and also a copy of the consumer’s report if the investigation results in any change. If the consumer reporting agency’s investigation does not resolve the dispute, the consumer may add a brief
statement to his or her file. The consumer reporting agency must normally include a summary of the statement in future reports. If an item is deleted or a dispute statement is filed, the consumer may ask that anyone who has recently received the report be notified of the change.

A consumer reporting agency must remove or correct inaccurate or unverified information from its files, usually within 30 days after the consumer disputes it. However, the consumer reporting agency is not required to remove accurate data from the consumer’s file unless it is outdated (as described below) or cannot be verified. If the consumer’s dispute results in any change to the consumer’s report, the consumer reporting agency cannot reinsert the disputed item into the consumer’s file unless the information source verifies its accuracy and completeness.

In addition, the consumer reporting agency must give the consumer a written notice telling the consumer that it has reinserted the item. The notice must include the name, address, and phone number of the information source. If the consumer tells anyone – such as a creditor who reports to a consumer reporting agency – that the consumer disputes an item, they may not then report the information to a consumer reporting agency without including a notice of the consumer’s dispute. Furthermore, once the consumer has notified the information source of the error in writing, it may not continue to report the information if it is, in fact, an error.

In most cases, a consumer reporting agency may not report negative information that is more than seven years old; the term is 10 years for bankruptcies. Creditors and insurers may use file information as the basis for sending a consumer unsolicited offers of credit or insurance. Such offers must include a toll-free phone number for the consumer to call to remove the consumer’s name and address from future lists. If the consumer calls, the consumer must be kept off the lists for two years. If the consumer requests, completes, and returns the consumer reporting agency form provided for this purpose, the consumer must be taken off the lists indefinitely.

8. Registration/Notification Requirements

GLBA contains no requirements to register with or notify regulatory authorities about data handling practices, although privacy and data security are often important components of regulatory oversight and audits.

FCRA does not generally establish registration requirements for a consumer reporting agency.

9. Data Protection Officers

For GLBA, see Section 12 below regarding security requirements.

FCRA does not generally establish requirements for a consumer reporting agency to appoint a chief privacy officer.
10. International Data Transfers

Like other US privacy laws, neither GLBA nor FCRA contains any express geographic restrictions on international data transfers.

11. Security Requirements

GLBA Interagency Guidelines establish requirements for financial institutions to protect the security of non-public personal information, including taking steps to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must:

- designate one or more employees to coordinate the safeguards;
- identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select appropriate service providers and contract with them to implement safeguards; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business arrangements or operations, or the results of testing and monitoring of safeguards. Additional rules apply in the area of security breach notification and safe disposal of consumer information.

FCRA contains a wide range of data integrity and accuracy requirements, including those described above. Additional rules also apply to the safe disposal of information in or derived from consumer reports. In addition, pursuant to an amendment of the FCRA, the Federal Trade Commission’s Red Flag Rules (16 CFR Part 681) became effective. The rules require creditors that use consumer reports, furnish information to consumer credit reporting agencies, or advance funds to or on behalf of a person with certain covered accounts to develop and implement written identity theft prevention programs. The programs must provide for the identification, detection, and response to red flags that could indicate identity theft.
12. Special Rules for the Outsourcing of Data Processing to Third Parties

GLBA establishes special rules for the protection, security and confidentiality of non-public personal information when disclosed to third-party service providers.

FCRA generally does not specifically establish restrictions on the use of outsourcing providers, although case law contains some relevant requirements on the use of “agents”, and any organization should be aware of other applicable regulatory requirements as well as other general fiduciary obligations to maintain the integrity and security of information.

13. Enforcement and Sanctions

The CFPB, the federal banking agencies, other federal regulatory authorities, and state insurance authorities enforce GLBA with regard to entities within their authority. Each federal agency has issued substantially similar rules implementing GLBA’s privacy provisions. The states are responsible for issuing regulations and enforcing the law with respect to insurance providers.

In relation to FCRA, the CFPB generally has regulatory authority over consumer reporting agencies, and federal functional regulators generally have certain authority over financial institutions that are users of consumer reports or furnishers of information to consumer reporting agencies or that otherwise are regulated under FCRA. State attorneys general have certain authority to pursue organizations for violations of FCRA, and aggrieved individuals can also pursue organizations in certain circumstances for violations of FCRA requirements.

14. Data Security Breach

a. Are there any legal requirements, including notification obligations, in the event of a data security breach?

While GLBA does not specifically impose notification obligations, federal regulators have issued guidance on notification obligations to financial institutions when a data security breach occurs. Among other elements, this Guidance calls for financial institutions to notify their affected customers and primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. In addition, GLBA requires financial institutions to ensure the security and confidentiality of customer information and to protect against the unauthorized access or use of customer data that may result in harm to the customer. Under GLBA, financial institutions are required to establish a comprehensive information security program that includes appropriate incident response procedures. GLBA security guidelines generally provide that financial institutions must implement a program to address
unauthorized access of customer data, including customer and authority notification, and mandate disclosure of a security breach if the financial institution determines that “misuse of its information about a customer has occurred or is reasonably possible”.

b. Risk of non-compliance
Violations of GLBA can result in various civil penalties and sanctions, including fines and other consequences that vary depending on the responsible regulatory authority.

Violations of FCRA can result in criminal and civil penalties. Civil penalties in the case of willful non-compliance can include up to USD 1,000 in statutory damages if no actual damages exist, actual damages, punitive damages, plus attorneys’ fees and costs.
United States
Health Insurance Portability and Accountability Act

1. Recent Privacy Developments
The most recent significant developments to HIPAA/HITECH (both defined below) occurred in 2013. The Health Information Technology for Economic and Clinical Health Act, Sec. 13001 of the American Recovery and Reinvestment Act, Public Law 111-005 (“HITECH”), established important amendments to HIPAA, including: (i) mandatory notification in the event of a security breach; and (ii) direct application of certain information security and other HIPAA provisions, including the heightened penalty provisions, to an expanded range of organizations, such as: (a) Business Associates of Covered Entities (which previously only needed to adhere to agreements with such Covered Entities); and (b) application of breach notification obligations to vendors of personal health records (previously not covered by HIPAA).

Since the enactment of HITECH, the Department of Health and Human Services (“HHS”), through the HHS Office for Civil Rights, had engaged in considerable rulemaking activity and increased its enforcement of HIPAA’s Privacy and Security Rules (discussed further below in Section 14). Then, after a number of delays, HHS released on 25 January 2013 the final omnibus rules codifying and modifying many of these interim rules, including those regarding heightened penalties, breach notification, and direct applicability to Business Associates (the “Final Rules”). The effective date of the Final Rules was 26 March 2013, and Covered Entities and Business Associates were required to be in compliance with the new requirements by 23 September 2013.

In part, the Final Rules:

- confirm that Business Associates (as well as their subcontractors that access or receive Protected Health Information) are directly liable for compliance with certain of the requirements of the HIPAA Privacy and Security Rules and are subject to related penalties for violation of such requirements;

- impose more stringent limitations on the use and disclosure of Protected Health Information for marketing and fundraising purposes, as well as prohibitions on the sale of Protected Health Information without individual authorization;
require modifications to and redistribution of a Covered Entity's Notice of Privacy Practices;

• modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools and to enable access to decedent information by family members or others;

• increase individual rights of access to Protected Health Information by allowing patients to request a copy of their electronic medical record in electronic form and allowing individuals to instruct their providers not to share information about their treatment with their health plan if they pay in full for the relevant product or service;

• adopt the increased and tiered civil money penalty structure provided by HITECH (which was originally published as an interim final rule on 30 October 2009); and

• adopt the breach notification rule for Covered Entities and Business Associates and replace the “harm” threshold for notification with an evaluation regarding whether the breached data was “compromised”.

The Final Rules also include additional modifications related to the use and disclosure of genetic information.

Prior to the issuance of the Final Rules, HHS released on 31 May 2011, a notice of proposed rulemaking on the HIPAA accounting of disclosures requirement. The purpose was, in part, to implement the statutory mandate under HITECH to require Covered Entities and Business Associates to account for disclosures of Protected Health Information to carry out treatment, payment, and health care operations. Under the pre-HITECH rule, covered entities were not required to provide an accounting of disclosures for these types of uses and disclosures.

In addition, the proposed 2011 rules, apparently based on HHS’s general authority under HIPAA, expanded the current accounting provision to provide individuals with the right to receive an access report detailing the internal access to Protected Health Information in a designated record set. If adopted in this form, these rules may pose challenges for Covered Entities that otherwise may be in the process of adopting electronic health records, as the detailed provisions regarding access tracking may not be contemplated by their current implementations. Comments for this proposed rule were accepted until 1 August 2011. The proposed May 2011 rules were not addressed in the Final Rules. HHS noted in the Final Rules, however, that these rules remain in effect and will be subject to additional rulemaking.
2. Emerging Privacy Issues and Trends

HITECH represents a significant expansion of federal law to protect health and medical privacy, and to protect individuals from medical identity theft. The adoption of the Final Rules, which contain more stringent penalties, obligations on Business Associates, and breach requirements, as well as the related enforcement activity by HHS, signals the on-going focus on this issue. In addition, with the increase in the number of high-profile security breaches, special focus on the breach notification requirements seems likely. There will likely be attention paid to how and if cloud providers are subject to HIPAA (for example, as Business Associates).

3. Law Applicable


4. Scope of the Law

The regulations are applicable to the following entities, defined as “Covered Entities”:

- a health plan;
- a health care clearing house; and
- a health care provider that transmits any health information in electronic form in connection with a transaction covered by a HIPAA standard.

Certain portions of the regulations related to information security, breach notification, and other provisions are directly applicable to service providers of Covered Entities, defined as “Business Associates”; in addition, breach notification requirements apply to third-party vendors of personal health records and certain other non-HIPAA covered entities.

a. Personal Data

The regulations govern the use and disclosure of “Protected Health Information”, which is individually identifiable health information, maintained in any format, that has been transmitted in an electronic format. Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- is created or received by a health care provider, health plan, employer, or health care clearing house; and
• relates to: (i) the past, present, or future physical or mental health or condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present, or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

5. Consent Requirements

A Covered Entity may obtain consent of the individual to use or disclose Protected Health Information to carry out treatment, payment, or health care operations. A Covered Entity must obtain an individual’s authorization to use and disclose Protected Health Information for any purpose other than those permitted by the HIPAA Privacy Standards. The requirement to seek authorization for the use and disclosure of Protected Health Information for research may be waived with the approval of an Institutional Review Board or a privacy board appointed by the Covered Entity.

a. Authorization Content

A valid authorization must include the following elements:

• a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
• if the information will be used for marketing purposes in exchange for financial remuneration from a third party, a statement to that effect;
• if information is to be sold, a statement that disclosure will result in remuneration to the Covered Entity;
• the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
• the name or other specific identification of the person(s), or class of persons, to whom the Covered Entity may make the requested use or disclosure;
• a description of each purpose of the requested use or disclosure;
• an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure; and
• signature of the individual and date.

In addition, the authorization must contain statements adequate to place the individual on notice of all of the following:

• the individual’s right to revoke the authorization in writing, and either: (i) the exceptions to the right to revoke and a description of how the
individual may revoke the authorization; or (ii) a reference to the Covered Entity’s privacy notice;

• the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either: (i) the Covered Entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization; or (ii) the consequences to the individual of a refusal to sign the authorization when the Covered Entity may, in compliance with HIPAA, condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization; and

• the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by HIPAA.

The authorization must be written in plain language, and certain restrictions apply with regard to compound authorizations. If a Covered Entity seeks an authorization from an individual for a use or disclosure of Protected Health Information, the Covered Entity must provide the individual with a copy of the signed authorization.

6. Information/Notice Requirements

A Covered Entity must provide a notice that is written in plain language and that contains the following elements:

• a header;

• a description, including at least one example, of the types of uses and disclosures that the Covered Entity is permitted to make for each of the following purposes: treatment, payment, and health care operations;

• a description of each of the other purposes for which the Covered Entity is permitted or required to use or disclose Protected Health Information without the individual’s written authorization;

• a description of any applicable legal limitation more stringent than the HIPAA Privacy Standards on the uses or disclosure of Protected Health Information;

• if applicable, a statement that the Covered Entity may contact the individual to raise funds for the Covered Entity and that the individual has the right to opt out of receiving such communications;

• if applicable, that a group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan;
• notice of the right to request restrictions on certain uses and disclosures of Protected Health Information, including a statement that the Covered Entity is not required to agree to a requested restriction (except where an individual requests a restriction on disclosure to a health plan for a product or service for which payment has been made in full);

• notice of the right to receive confidential communications of Protected Health Information;

• notice of the right to inspect and copy Protected Health Information;

• notice of the right to amend Protected Health Information;

• notice of the right to receive an accounting of disclosures of Protected Health Information;

• notice of the right to obtain a paper copy of the notice from the Covered Entity upon request;

• a statement that the Covered Entity is required by law to maintain the privacy of Protected Health Information and to provide individuals with notice of its legal duties and privacy practices with respect to Protected Health Information and to notify individuals following a breach of unsecured Protected Health Information;

• a statement that the Covered Entity is required to abide by the terms of the notice currently in effect;

• a statement that the Covered Entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all Protected Health Information that it maintains (the statement must also describe how the Covered Entity will provide individuals with a revised notice);

• a statement that individuals may complain to the Covered Entity and to HHS if they believe their privacy rights have been violated;

• the name, or title, and telephone number of a person or office to contact for further information; and

• the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

The Covered Entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual’s rights, the Covered Entity’s legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected. A covered health plan must distribute
its privacy notice at least once every three years to all then-current participants.

7. Rights of Individuals

a. Access Right
An individual has a general right of access to inspect and obtain a copy of Protected Health Information about the individual in a designated record set, for as long as the Protected Health Information is maintained in the designated record set. A designated record set is broadly defined as a set of records on which a Covered Entity may make decisions about an individual.

As noted above, the 11 May 2011 proposed rules in their current form expand such access rights. Moreover, the Final Rules provide specific additional rights to request information in a particular form.

b. Accounting of Disclosure Rights
An individual has a right to receive an accounting of disclosures of Protected Health Information made by a Covered Entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- to carry out treatment, payment and health care operations;
- to individuals of Protected Health Information about them;
- incident to a use or disclosure otherwise permitted or required;
- pursuant to an authorization;
- for the facility’s directory or to persons involved in the individual’s care or other notification purposes;
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials;
- as part of a limited data set; or
- that occurred prior to the compliance date.

As noted above, the 11 May 2011 rules in their current form expand the situations for which Covered Entities must provide an accounting of disclosures of Protected Health Information.

c. Amendment Rights
A Covered Entity must permit an individual to request that the Covered Entity amend the Protected Health Information maintained in the designated record set. The Covered Entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested
amendment, provided that it informs individuals in advance of such requirements.

d. Right to Restrict Uses and Disclosures
A Covered Entity must allow an individual to request restrictions on the uses and disclosures of Protected Health Information about the individual. A Covered Entity is not obliged to agree to a requested restriction, but must abide by any agreed upon restriction except in the event that the information is required to provide emergency treatment to the individual. Under the Final Rules, individuals have the right to instruct their provider not to share information about their treatment with their health plan if they pay in full for the relevant product or service.

e. Right to Request Confidential Communications
A health care provider must accommodate reasonable requests from individuals to receive communications by alternate means or locations. A health plan must accommodate reasonable requests for such confidential communications when the individual states that the basis for the request is that the disclosure of Protected Health Information could endanger the individual.

8. Privacy Officer
A Covered Entity must appoint a privacy officer who is generally responsible for the implementation and enforcement of policies and practices of the Covered Entity required by the HIPAA Privacy Standards.

9. International Data Transfers
There are no specific requirements within the regulations applicable to international transfers of data. A Covered Entity is required to comply with the requirements of HIPAA with respect to data that has been transferred outside of the US.

10. Data Retention Obligations
Covered Entities are required to maintain all documents required under these regulations for six years.

11. Security Requirements
Covered Entities and Business Associates must comply with the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164. The application of many of the Security Standards to Business Associates was re-confirmed in the Final Rules.
12. Requirements Applicable to Employer-Sponsored Health Plans

An employer plan sponsor who requires access to Protected Health Information other than summary health information or enrollment/disenrollment information must certify to the plan that the plan documents have been amended to incorporate provisions required by the HIPAA Privacy Standards before the plan may disclose Protected Health Information to the employer plan sponsor. The plan amendment must provide that the employer plan sponsor will:

- not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
- ensure that any agents, including a subcontractor, to whom it provides Protected Health Information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
- not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
- report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
- make available Protected Health Information, as required by the HIPAA Privacy Standards;
- make available Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with the HIPAA Privacy Standards;
- make available the information required to provide an accounting of disclosures in accordance with the HIPAA Privacy Standards;
- make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from the group health plan available to HHS for purposes of determining compliance by the group health plan with the HIPAA Privacy Standards;
- if feasible, return or destroy all Protected Health Information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;
• describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the Protected Health Information to be disclosed, provided that any employee or person who receives Protected Health Information relating to payment under, health care operations of, or other matters pertaining to, the group health plan in the ordinary course of business must be included in such description;

• restrict the access to and use by such employees to plan administration functions that the plan sponsor performs for the group health plan; and

• provide an effective mechanism for resolving any issues of non-compliance with plan document provisions.

13. Requirements Applicable to Outsourcing or Transfer to Third Parties

Generally, disclosures of Protected Health Information to third parties can only be made pursuant to a valid authorization from each individual whose Protected Health Information is being disclosed. Subject to the conditions described below, a Covered Entity may disclose Protected Health Information without prior authorization to Business Associates, which are third parties that:

• on behalf of the Covered Entity, assist in the performance of: (i) a function or activity involving the use or disclosure of individually identifiable health information; or (ii) any other function or activity regulated by standards promulgated pursuant to the HIPAA statute; or

• provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity, where the provision of the service involves the disclosure of Protected Health Information from the Covered Entity, or from another Business Associate of such Covered Entity, to the Business Associate. A Covered Entity may disclose Protected Health Information to a Business Associate and may allow a Business Associate to create or receive Protected Health Information on its behalf, if the Covered Entity obtains satisfactory assurance that the Business Associate will appropriately safeguard the information.

“Business Associate” also includes: (i) a Health Information Organization, E-Prescribing Gateway, or other person that provides data transmission services with respect to Protected Health Information to a Covered Entity and that requires access on a routine basis to such Protected Health Information; (ii) a person that offers a personal health record to one or more individuals on behalf of a Covered Entity; and (iii) a subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of a Business Associate.
In particular, the Covered Entity must enter into a contract with the Business Associate that:

- establishes the permitted and required uses and disclosures of Protected Health Information by the Business Associate;

- prohibits the Business Associate to use or further disclose the information in a manner that would violate the requirements of HIPAA, if done by the Covered Entity, except that: (i) the contract may permit the Business Associate to use and disclose Protected Health Information for the proper management and administration of the Business Associate; and (ii) the contract may permit the Business Associate to provide data aggregation services relating to the health care operations of the Covered Entity;

- provides that the Business Associate will: (i) not use or further disclose the information other than as permitted or required by the contract or as required by law; (ii) use appropriate safeguards to prevent the use or disclosure of the information other than as provided for by its contract; (iii) report to the Covered Entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including any breaches of unsecured Protected Health Information; (iv) ensure that any agents, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information; (v) make available Protected Health Information in accordance with the HIPAA Privacy Standards; (vi) make available Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with the HIPAA Privacy Standards; (vii) make available the information required to provide an accounting of disclosures in accordance with the HIPAA Privacy Standards; (viii) to the extent the Business Associate is to carry out a Covered Entity’s obligation under the HIPAA Privacy Standards, comply with the requirements of the Privacy Standards that apply to the Covered Entity in the performance of such obligation; (ix) make its internal practices, books, and records relating to the use and disclosure of Protected Health information received from, or created or received by the Business Associate on behalf of, the Covered Entity available to the US government (Secretary of HHS) for purposes of determining the Covered Entity’s compliance with HIPAA; and (x) at termination of the contract, if feasible, return or destroy all Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity that the Business Associate maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the
information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

- authorizes termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the contract.

In addition, the contract may permit the Business Associate to use the information received by the Business Associate in its capacity as a Business Associate to the Covered Entity, if necessary: (i) for the proper management and administration of the Business Associate; or (ii) to carry out the legal responsibilities of the Business Associate; and the Business Associate may be permitted to disclose the information received by the Business Associate in its capacity as a Business Associate, if: (a) the disclosure is required by law; or (b) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

A Covered Entity is not in compliance with the HIPAA Privacy Standards if the Covered Entity knows of a pattern of activity or practice of the Business Associate that constituted a material breach or violation of the Business Associate’s obligation under the contract or other arrangement, unless the Covered Entity takes reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminate the contract or arrangement, if feasible. The same obligation applies to Business Associates with regard to downstream subcontractors.

Additionally, pursuant to the HIPAA Security Standards, a Business Associate must agree to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, availability and integrity of electronic Protected Health Information that is created, received, maintained or stored on behalf of a Covered Entity. The Business Associate must report any security incident to the Covered Entity of which it becomes aware. In addition, as noted above, the Business Associate must ensure that its agreement with any subcontractor includes a requirement that these safeguards be implemented as well.

Under the Final Rules, Covered Entities have until September 2014 to make sure that existing Business Associate Agreements conform to the new requirements for Business Associate Agreements.

14. Enforcement and Sanctions

HHS may impose a civil money penalty on any person who violates the HIPAA Privacy Standards in the range from USD 100 to USD 50,000 per
violation, with a total of USD 25,000 to USD 1.5 million for all violations of a single requirement in a calendar year. Violations of the HIPAA Privacy Standards can also carry criminal penalties, including up to 10 years’ imprisonment in certain cases. Under HITECH, such penalties may now be imposed on Business Associates as well as Covered Entities.

Over the course of the year, HHS continued to demonstrate a heightened interest in enforcing HIPAA and imposed additional civil money penalties on entities for violations of the HIPAA Privacy and Security Rules.

15. Data Security Breach

a. Are there any legal requirements, including notification obligations, in the event of a data security breach?

The HITECH Act amended HIPAA to include a security breach notification requirement. These notification requirements apply in the event of a breach of unsecured Protected Health Information, which generally means Protected Health Information that is not secured by technology (e.g., encryption) that makes it unreadable, unusable or indecipherable to unauthorized individuals. A “breach” is presumed to have occurred if there is an acquisition, access, use or disclosure of Protected Health Information in a manner not permitted by the Privacy Rule unless a risk assessment determines a “low probability” that the breached data was compromised. The four factors that risk assessments must consider are:

- the nature and extent of the Protected Health Information involved, including the likelihood data could be re-identified;
- the unauthorized person who used Protected Health Information or to whom an improper disclosure was made;
- whether the Protected Health Information was actually acquired or viewed; and
- the extent to which the risk to the Protected Health Information was mitigated.

Several features of the notification requirement include:

- obligations for the Covered Entity to notify affected individuals upon discovery of a breach (and in no case later than 60 days after such discovery or after such breach should have reasonably been discovered);
- obligations for Business Associates to notify the relevant Covered Entity upon discovery of a breach;
• definitions for key terms, such as: “discovery” of breach; “unsecured protected health information” (i.e., the type of Data Subject to the notification requirement); and “timeliness” of transmitting the notification;

• obligations to transmit the notice to affected individuals in writing or other specified means;

• if more than 500 individuals are affected, mandatory obligations to notify media;

• obligations to notify the HHS of all breaches (if 500 or more individuals are affected, such notification must be made at the time of the notification to the affected individuals; if fewer than 500 individuals are affected, such notification must be made at the end of the calendar year);

• content requirements for notices (e.g., date of breach, date of discovery, data compromised, and the like); and

• other specific obligations.

Additional breach notification duties apply to vendors of personal health records, as per the Health Breach Notification Rule adopted by the Federal Trade Commission (16 CFR Part 318).

b. **Risk of non-compliance**

Failure to comply with the breach notification requirements constitutes a violation of HIPAA that can be subject to the penalties described in Section 14 above.
United States State Data Security Laws

1. Recent Developments and Trends

A growing number of US states have enacted laws requiring entities that possess certain categories of personal information to implement reasonable security requirements. Such laws generally apply to any entity that owns or licenses certain categories of personal information about a resident of the state that has promulgated such laws. Certain US states, such as Massachusetts and Oregon, have promulgated fairly specific requirements for the protection of personal information. For example, the Massachusetts Office of Consumer Affairs and Business Regulation has promulgated data security regulations pursuant to Chapter 93H of the General Laws of Massachusetts. The Massachusetts regulations differ from other US state data security laws in that they require covered entities to implement a number of specific administrative, physical, and technical safeguards on a comprehensive level, rather than articulating a reasonableness standard or establishing certain data security measures for particular data fields (e.g., social security number). Other states may find the regulations influential in interpreting or making law, as shown by a large volume of pending state bills on data security. The broad scope of the Massachusetts regulations and similar state data security laws in the future, will likely cover many entities that participate in interstate commerce but are outside of a state that has enacted such laws, since such entities typically process personal information of individuals from many states.

In addition, certain states are taking action to promulgate more expansive regulation in key sectors. Most notably, New York has recently adopted the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500 (the “New York Financial Regulations”). The New York Financial Regulations apply broadly to personally identifiable information as well as business information held by covered entities, and establish a broad range of information security, record retention, governance, breach notification, and annual reporting requirements on such covered entities.

2. Laws Applicable

Massachusetts Gen. Laws (“MGL”) 93H, §§ 1-6 and Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR § 17.00 et seq., as amended on 12 February 2009 (hereinafter, the “Massachusetts Regulations”). See also California Civil Code § 1798.81.5 and
Oregon Rev. Stat. § 646A.622 as other examples of US state laws with specific data security requirements.

3. Key Privacy Concepts

a. Personal Data
“Personal information” is defined as “a Massachusetts resident’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (i) social security number; (ii) driver’s license number or state-issued identification card number; or (iii) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public”.

b. Data Processing
The Massachusetts Regulations apply to persons that “own, license, store or maintain” personal information about a resident of the Commonwealth of Massachusetts, regardless of the medium in which such information is recorded or preserved (e.g., paper or electronic records).

c. Processing by Data Controllers
A covered entity may include “a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof”.

d. Jurisdiction/Territoriality
The Massachusetts Regulations apply on their face to persons that “own, license, store or maintain” personal information about a resident of the Commonwealth of Massachusetts. Accordingly, the Massachusetts Regulations may have extra-jurisdictional effect on entities located outside of Massachusetts if they process personal information on Massachusetts residents.

e. Sensitive Personal Data
The Massachusetts Regulations do not distinguish between sensitive personal information and non-sensitive personal information.

f. Employee Personal Data
While the Massachusetts Regulations were primarily promulgated to protect consumers from identity theft, on their face, they can potentially apply to personal information of covered entities’ employees as well.
4. Processing Rules

“Every person that owns, licenses, stores or maintains personal information about a resident of the [Commonwealth of Massachusetts] shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records”. The following safeguards, among others, must be included:

- identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks;

- developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises;

- imposing disciplinary measures for violations of the comprehensive information security program rules;

- preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records;

- limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected;

- limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements;

- identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information;

- reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers;
• regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrading information safeguards as necessary to limit risks;

• reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

• documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

5. Data Protection Officers

Every comprehensive information security program must include the designation of at least one employee to maintain it.

6. International Data Transfers

A covered entity is required to comply with the regulations' requirements with respect to personal information that has been transferred outside of the United States. There are, however, no specific requirements in the Massachusetts Regulations that are relevant to international transfers of data.

7. Security Requirements

Every covered entity that electronically stores or transmits personal information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, has the following elements:

• secure user authentication protocols;

• secure access control measures;

• encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly;

• reasonable monitoring of systems, for unauthorized use of or access to personal information;

• encryption of all personal information stored on laptops or other portable devices;
• reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of personal information in files on a system that is connected to the internet;

• reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions; and

• education and training of employees on the proper use of the computer security system and the importance of personal information security.

8. Special Rules for the Outsourcing of Data Processing to Third Parties

Every comprehensive information security program must include taking all reasonable steps to: (i) verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in the Massachusetts Regulations; and (ii) ensure that such third-party service provider is applying security measures to personal information that are at least as stringent as those required under the Massachusetts Regulations.

9. Enforcement and Sanctions

Since 2011, the Massachusetts Attorney General has brought enforcement actions against companies that have violated the Massachusetts Regulations by failing to protect personal information in connection with data security breaches. For example, in 2012, the Massachusetts Attorney General announced that a Massachusetts hospital agreed to pay USD 750,000 to resolve allegations that the hospital failed to protect the personal and confidential health information of more than 800,000 consumers when hundreds of computer back-up tapes were lost in transit to an off-site location to be erased. In 2013, the Massachusetts Attorney General announced that former owners of a medical billing practice agreed to collectively pay USD 140,000, settling allegations that sensitive medical records and confidential billing information for tens of thousands of Massachusetts patients were improperly disposed of at a public dump. In 2014, the Massachusetts Attorney General announced that a nationally chartered bank agreed to pay USD 825,000 to resolve allegations that it lost unencrypted personal information of more than 90,000 consumers when two back-up tapes were lost in transit by a third-party courier and that the bank delayed notifying the Massachusetts Attorney General and impacted consumers. As part of the settlement, the bank was also required to take steps to strengthen its security practices.
10. Data Security Breach

a. Are there any legal requirements, including notification obligations, in the event of a data security breach?
Data breach notification obligations are set forth in MGL 93H §3.

b. Risk of non-compliance
The Massachusetts Attorney General may bring an action pursuant to its statutory authority to remedy violations of the law. A Massachusetts court may issue injunctions and make such other orders or judgments as may be necessary to compensate injured parties. In addition, Massachusetts law provides for a civil penalty of USD 5,000 for each violation and may require the violator to pay the reasonable costs of investigation and litigation of such violation, including reasonable attorneys’ fees. Other states with data security laws provide for civil penalties of up to USD 1,000 per violation and up to USD 750,000 in the aggregate for continuing violations.
United States
State Security Breach Notification Laws

1. Recent Developments and Trends

As of February 2018, 48 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted notification laws involving security breaches of personal information. New Mexico enacted a law becoming the 48th state in 2017. Only two states – Alabama and South Dakota – have no law requiring consumer notification of security breaches involving personal information. Generally, US state data breach notification laws apply to any entity that owns or licenses certain categories of personal information about a resident of the state that has promulgated such a law. In 2013, the state of North Dakota expanded the scope of Personal Data subject to data breach notification to include medical and health insurance information. California expanded the scope of Personal Data subject to breach notification to include a user name or email address, in combination with a password or security question and answer that would permit access to an online account in 2014, and several other states, including Florida, Illinois and Wyoming, have followed suit. On 1 January 2016, three new California data security laws have come into effect, including Senate Bill 570 (adding requirements to form and content of breach notifications), Assembly Bill 964 (containing a definition of “encrypted”) and Senate Bill 34 (prescribing requirements for automated license plate recognition systems).

2. Law Applicable

This summary will focus on California’s security breach notification law, Cal. Civ. Code § 1798.82, the first such law both in the United States and worldwide (enacted in 2002, it became effective 2003). Accordingly, although the requirements and scope of other state laws differ from those of California, most state laws follow the basic principles of Cal. Civ. Code § 1798.82.

No generally applicable federal law on security breach notification has been enacted to date, but the federal Health Insurance Portability and Accountability Act also contains certain security breach notification requirements, which were introduced by the Health Information Technology for Economic and Clinical Health Act (see summary on HIPAA). The Gramm-Leach-Bliley Act also establishes breach notification requirements that apply to financial institutions (see summary on GLBA/FCRA).
3. Key Privacy Concepts

a. Personal Data

“Personal information” means: (i) an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (a) social security number, (b) driver’s license number or California identification card number, (c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account, (d) medical information, (e) health insurance information, (f) information collected through an automated license plate recognition system; or (ii) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

“Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

“Medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. “Health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

Note that state breach notification requirements outside of California can often have a broader scope and apply to a name in combination with additional data fields, such as: (i) date of birth; (ii) mother’s maiden name; (iii) digitized or electronic signature; (iv) unique electronic identifier or routing code, in combination with any access code or password that would permit access to a financial account; (v) passwords; and (vi) identification number assigned to an individual by the individual’s employer.

b. Employee Personal Data

Notice obligations under Cal. Civ. Code § 1798.82 do not distinguish between types of Data Subjects, e.g., customers or employees. However, only customers of a covered business are eligible to recover damages for violations of Cal. Civ. Code § 1798.82.

4. Information/Notice Requirements

Cal. Civ. Code § 1798.82 requires that a data breach notice must meet certain content requirements, as follows:

- The security breach notification shall be written in plain language.
The security breach notification shall include, at a minimum, the following information: (A) the name and contact information of the reporting person or business subject to this section; (B) a list of the types of personal information that were or are reasonably believed to have been the subject of a breach; (C) if the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred; (D) the date of the notice; (E) whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; (F) a general description of the breach incident, if that information is possible to determine at the time the notice is provided; and (G) the toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver’s license or California identification card number.

At the discretion of the person or business, the security breach notification may also include any of the following: (A) information about what the person or business has done to protect individuals whose information has been breached; and (B) advice on steps that the person whose information has been breached may take to protect himself or herself.

In the case of a breach of the security of the system involving a “user name or email address, in combination with a password or security question and answer that would permit access to an online account” (and no other categories of personal information described by the statute), the person or business may (except in certain circumstances described by the statute) comply with the notification requirements by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

Since 1 January 2016, the California Civil Code now offers a “model security breach notification form”. Companies and state agencies do not have to use this form. But, if they choose to use the form for written notices, provide all required information and comply with the “plain language” requirement, they are deemed to comply with the applicable form requirements.
California’s new form requirements and existing minimum content requirements are at odds with some other states’ laws, which limit the details companies shall disclose about a breach, in the interest of further investigations. But, for the most part, companies should continue to be able to issue relatively uniform, global breach notices to address requirements in different states and countries pertaining to breaches affecting individuals in multiple jurisdictions.

5. Rights of Individuals

California residents are entitled to damages and injunctions if companies violate data security breach notification requirements, but California breach notification laws do not generally provide for sanctions or remedies for the breach itself. As an exception to this rule, effective 1 January 2016, Senate Bill 34 added a new right to private action and claims for liquidated damages in the amount of USD 2,500 to any other sanctions, penalties and remedies for Data Subjects who are harmed by a knowingly committed violation of California laws regarding automated license plate recognition systems, including data security breaches affecting such data.

6. Registration/Notification Requirements

Like many other US State laws, Cal. Civ. Code § 1798.82 now requires notification to the State’s Attorney General in certain circumstances. Specifically, Cal. Civ. Code § 1798.82 requires notification to the State’s Attorney General if a person or business subject to the law is required to notify more than 500 California residents.
7. **Data Protection Officers**

California law does not require the appointment of a data protection officer.

8. **Security Requirements**

A separate California Civil Code provision (Cal. Civ. Code § 1798.81.5) requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.

9. **Special Rules for the Outsourcing of Data Processing to Third Parties**

A separate California Civil Code provision (Cal. Civ. Code § 1798.81.5) requires a business that discloses personal information about a California resident to a non-affiliated third party to require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

10. **Enforcement and Sanctions**

The California Attorney General created a Privacy Enforcement and Protection Unit in the California Department of Justice, which has enforced California’s breach notification requirements against companies that delayed to notify. Also, data breaches are usually followed by private litigation in the form of class action lawsuits or individual complaints.

11. **Data Security Breach**

“Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

Any person or business that maintains computerized data that includes personal information that the person or business does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notice may be provided by one of several methods, including written notice, electronic notice, substitute notice, email notice, a website posting, and notification to major state-wide media.
EU-US Privacy Shield

Since 1 August 2016, companies in the United States can join the EU-US Privacy Shield Program operated by the US Department of Commerce. More than 2700 companies joined the program by February 2018.

Participation is voluntary and not required or beneficial from a US law perspective. US companies consider joining Privacy Shield for ease of doing business with European companies and customers.

Companies established or using equipment in the European Economic Area ("EEA") are prohibited from sharing Personal Data with affiliates, vendors, customers and anyone else outside the EEA, unless an adequate level of data protection in the recipient jurisdiction is assured or an exception or derogation applies. This prohibition stems from the EU Data Protection Directive of 1995 ("EU Data Protection Directive") and a comparable requirement will continue to apply when the new General Data Protection Regulation ("GDPR") becomes effective on 25 May 2018 (see Art. 25 of the EU Data Protection Directive and Art. 44 of the GDPR). In the Directive and in Art. 4 No. 1 GDPR, the term “Personal Data” is broadly defined to include any information relating to an identifiable individual. Practically, companies cannot conduct any business without sharing at least some contact information and many transactions require more intensive information sharing. Therefore, companies in the EEA need to ensure adequate data protection safeguards to do business or otherwise transmit data outside the EEA.

The EU Commission has approved a few countries as generally assuring adequate data protection levels, including Argentina, Israel, Canada, New Zealand, Switzerland, and Uruguay but has not issued a blanket adequacy finding for all of the USA, even though US data privacy laws are in many respects more specific, effective and up to date than data protection laws in Europe and other countries.

In the year 2000, the EU Commission issued a uniquely limited adequacy finding for the USA whereby US companies would be deemed to assure adequate data protection if they joined a “Safe Harbor” program that the US Commerce Department had agreed with the EU Commission to enable US companies to satisfy EU adequacy requirements. 15 years and approximately 4500 company registrations later, the Court of Justice of the European Union ("CJEU") invalidated the Commission’s adequacy decision from the year 2000 on 6 October 2015 due primarily to concerns that the Safe Harbor itself did not embed protections against US law and policy on government surveillance (Case C-362/14). As of 31 October 2016, the US Commerce Department will no longer maintain the Safe Harbor program.
After the CJEU challenge to the Safe Harbor program, the EU Commission and US Commerce Department intensified their work on a successor program, which they had been working on for a couple of years already. They created the EU-US Privacy Shield program to address all concerns that the CJEU had raised. On 12 July 2016, after obtaining all requisite approvals and engaging in appropriate consultations, the EU Commission issued its decision finding that “the United States ensures an adequate level of protection for personal data transferred from the Union to organizations in the United States under the EU-US Privacy Shield”. As expected, certain politicians, activists and data protection authorities in the EU immediately criticized the program and announced plans to challenge it. However, speaking collectively, the Article 29 Working Party of EU Data Protection Authorities affirmed that Privacy Shield offers “major improvements” as compared to Safe Harbor, and has issued statements indicating that it will raise any ongoing concerns about Privacy Shield in the context of the annual review of the program, and that the EU data protection authorities will not plan to challenge the program collectively for at least a year. US companies can certify online to the US Commerce Department that they comply with the Privacy Shield Principles after they conduct and document a self-assessment. The Commerce Department reviews the applicants’ submission information and privacy policy and can also request information regarding onward transfer agreements.
Uruguay

Martin Pesce
Montevideo
Tel: +598 2900 1000 ext. 1431
mpesce@ferrere.com

Stephania Bresque
Montevideo
Tel: +598 2900 1000 ext. 1450
sbresque@ferrere.com
1. Recent Privacy Developments

In Uruguay, Personal Data protection is regulated under Law No. 18,331 and its Regulatory Decree No. 414/009. In August 2012, Uruguay was granted the adequacy note for international transfer purposes by the European Commission as the aforementioned regulation has been deemed aligned with European regulatory standards.

Furthermore, on 12 April 2013, the Council of Europe announced that Uruguay had become the first non-European country to accede to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol 3.3. The approval makes Uruguay the 45th country to be party to the Convention, which was included within the internal Uruguayan legal framework through Law No. 19,030 in November 2011.

2. Emerging Privacy Issues and Trends

- **Cloud computing**: This emerging technology is gaining popularity among multinational companies, especially as it is seen to improve productivity and lower costs. The local data protection authority has participated and hosted several events aimed at analyzing the risks involved in the implementation of cloud computing. The main issue of concern has been the fact that most cloud computing providers do not disclose the specific place where customer data will be held. This scenario implies a certain degree of risk for companies and becomes an issue in terms of ensuring compliance with local data protection regulation, which prohibits Personal Data transfers to certain countries.

- **Bring Your Own Device (“BYOD”)**: Many companies have started to shift to a BYOD system. One of the issues to consider when implementing a BYOD system is whether and to what extent the employer is entitled to monitor and control the use of such devices by their employees during work hours and personal time as an exercise of the employer’s right of control. The local data protection authority has yet to issue an opinion on the subject, and has yet to define the parameters within which said monitoring may be put in place when employees are using their own devices. It is therefore highly recommended to have a policy in place.

- **Remote Working**: An increasing number of companies, mostly those that are multinationals, have introduced this mode of work, which implies that employees are entitled to perform their work-related tasks from their homes. In this case, the comments are similar to those of the BYOD system, regarding the lack of regulation or an opinion of the local data protection authority, and the right of employers to conduct monitoring activities. It is therefore highly recommended to have a policy in place.
• **Whistle-blowing hotlines:** Mostly as a response to regulatory requirements from affiliate companies located abroad, several companies have implemented whistle-blowing hotlines. These hotlines are aimed at granting employees a manner to report misconduct, misbehavior and other immoral activities from coworkers and even their bosses. To date, the local data protection authority has not issued an opinion on the same. Nevertheless, given the fact that the law expressly prohibits the collection of personal information related to the commission of criminal, civil and/or administrative penalties, except by authorized public agencies pursuant to a legal obligation, such information shall not be collected in the event that is revealed over the hotline. It is highly recommended to have a policy in place.

• **Cybercrime/cybersecurity:** In 2014, the Executive Branch filed a bill before the Legislative Branch in order to regulate and sanction cybercrimes. The bill is currently under analysis in the Parliament, and it classifies the following as felonies: unauthorized access to a computer system; computer damage; computer fraud; phishing; and Personal Data treatment through deceitful, abusive or extortive means.

3. **Law Applicable**

In Uruguay, the legal framework concerning Personal Data protection is rather new, and consists of two main regulations (the “Law”):

• **Law No. 18,331 on Personal Data Protection and Habeas Data Action**¹ (as amended by Law Nos. 18,719 and 18,996), which was adopted on 6 August 2008; and

• **Decree No. 414/009,**² which regulates the aforementioned law (as amended by Decree No. 308/014) enacted on 31 August 2009.

The aforementioned regulations broadly follow the European Directive 95/46 EC. Accordingly, they follow the European protective parameters. Both the Law and the Decree seek to protect the privacy of individuals and legal entities whose records are kept in databases.

---

¹ [http://datospersonales.gub.uy/wps/wcm/connect/829161004d0a999d861fcedfd6066fd91/Descargar+Ley+N%C2%B0+18.331.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=829161004d0a999d861fcedfd6066fd91](http://datospersonales.gub.uy/wps/wcm/connect/829161004d0a999d861fcedfd6066fd91/Descargar+Ley+N%C2%B0+18.331.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=829161004d0a999d861fcedfd6066fd91)

The Law introduces several principles that ought to be complied with when collecting and processing Personal Data:

**Principle of legality:** The formation of a database will be lawful when the database is properly registered. Moreover, a database cannot have purposes that infringe human rights or are contrary to law or public morals.

i. **Principle of truthfulness/veracity:** Personal Data collected for processing shall be truthful, adequate, impartial and not excessive regarding the purpose for which it was obtained. Data collection shall not be carried out through unfair, fraudulent, abusive or extortive means, or in any way contrary to the provisions of the Law. Data shall be accurate and updated, if necessary. Whenever the inaccuracy or falseness of data is verified, the controller, as soon as it becomes aware of said circumstance, shall delete, complete or replace the data with the accurate, truthful and updated version. Furthermore, out of date data shall be deleted.

ii. **Purpose limitation principle:** Data that is subject to processing shall not be used for purposes other than or incompatible with those motivating their collection. Data shall be deleted whenever they cease to be necessary or relevant for the purposes for which they were collected. The regulations shall determine cases and procedures in which, exceptionally, and considering historical, statistical or scientific values, and according to specific legislation, Personal Data shall be kept even when said need or appropriateness has expired. Data shall not be communicated between databases, without it being stated by law or without the prior informed consent of the Data Subject.

iii. **Principle of prior consent:** Personal Data processing shall be legal whenever the Data Subject has given his/her prior free, express and informed consent, which has to be documented, save for the exceptions detailed below.

iv. **Principle of data security:** The Data Controller or user of the database must take the necessary steps to ensure the security and confidentiality of Personal Data. Such measures must prevent the alteration, loss, consultation or unauthorized data treatment, as well as detect any re-direction of information, intentional or not, whether the risks come from human action or from the technical means used.

v. **Principle of confidentiality:** Natural or legal persons that lawfully obtain information from a database providing processing are obliged to use it by keeping it confidential and exclusively for the usual operations of their business or activity; any disclosure of said information to third parties is prohibited. People who, due to their labor situation or other type of relationship with the Data Controller, have access or take part in any
stage of Personal Data processing are bound to protect the secrecy of data (article 302 of the Criminal Code), whenever the data is collected from non-publicly-accessible sources. The above shall not apply in cases where there is an order by a competent justice, according to regulations in force on this subject or upon the Data Subject’s consent. This obligation shall prevail even after the relationship with the Data Controller has ended.

vi. Principle of liability: The Data Controller shall be liable for non-compliance of the provisions stated in the Law.

4. Key Privacy Concepts

a. **Personal Data**
   Personal Data: Any kind of information regarding identified or identifiable natural or legal persons.

b. **Data Processing**
   Data Processing: Systematic procedures and operations, whether or not by automated means, allowing the processing of Personal Data, as well as their assignment to third parties through communications, queries, interconnections or transfers.

c. **Processing by Data Controllers**
   Processing by Data Controllers: The Privacy Act applies to entities that undertake any of the acts or practices covered by the Law. No distinction is made between entities that are Data Controllers and those that are mere Data Processors treating the data on behalf of other entities. The only difference is on the degree of liability of the processing party, depending on whether the entity is a Data Controller or a Data Processor.

d. **Jurisdiction/Territoriality**
   Jurisdiction/Territoriality: Personal Data treatment/processing is subject to the Law in the following cases:
   - the processing is being carried out by a Data Controller established within Uruguayan territory, the latter being the place where processing takes place; and
   - when the Data Controller is not established within Uruguayan territory but uses means located in the country for the processing of the data. An exception to this rule is that the aforementioned means are used exclusively for transit purposes, as long as the Data Controller designates a representative before the local data protection authority, with an address and permanent residency in Uruguay, in order to comply with its legal obligations. Such designation will not impede the initiation of legal
actions against the Data Controller, nor will it diminish its liability as to the compliance of its obligations under the Law and the Decree.

Although the local data protection authority has not yet clearly defined what “means” would include, it is likely to follow the Spanish Regulator’s criteria, which is broad and includes any type of device or tool (e.g., PCs, cookies, etc.).

e. Sensitive Personal Data

**Sensitive Personal Data:** Personal Data revealing racial or ethnic origin, political preferences, religious and moral beliefs, trade union membership and information regarding health or sex life.

f. Employee Personal Data

**Employee Personal Data:** local regulation does not provide a definition of “Employee Personal Data”. Notwithstanding the foregoing, please note that, under the Law, Personal Data that is derived from a contractual, scientific, or professional relationship with the Data Subject, and is necessary for the development or fulfilment of such relationship (such as Employee Personal Data) is exempted from the prior consent requirement for its collection and treatment.

5. Consent

a. General

As a general rule, the Data Subjects’ free, prior, explicit and informed consent has to be obtained and documented prior to the collection and processing of Personal Data.

There are exceptions to the aforementioned principle. As such, prior consent shall not be necessary when:

- the data comes from public sources of information, such as registries or publications in mass media;
- the data is collected for the implementation of typical functions of the State powers or on account of a legal obligation;
- it involves lists whose data regarding natural persons are only limited to: names and surnames, identity card numbers, nationalities, addresses and dates of birth; in the case of legal entities, corporate names, fancy names, tax payer numbers, addresses, phone numbers and identities of the people in charge;
- the data derives from a contractual, scientific or professional relationship with the Data Subject, and is necessary for its development or execution; or
• the processing is carried out by a natural person for his/her exclusive personal or household use.

A recent modification to the wording of the Law included a specific detail of sources that will be deemed public sources of information and/or public information, as follows:

• the Official Gazette and official publications, whatever their record carrier or communication channel may be;

• publications in mass media, such as those from the press, regardless of the medium in which they are contained or the channel through which the communication is practiced;

• guides, yearbooks, directories and similar lists where names and addresses are shown, or other personal details that were included with the Data Subject’s consent; and

• any other record or publication in which general interest prevails, which Personal Data contained therein can be accessed, disseminated or used by third parties.

For the consent to be considered informed, the law mandates the following information to be provided to the Data Subject:

• the purpose for which data shall be processed and who the recipients or categories of recipients of the data may be;

• the existence of the corresponding database, whether electronic or any other type, and the identity and address of the Data Controller;

• whether replies to the proposed questionnaire are mandatory or voluntary, particularly regarding sensitive data;

• consequences of the provision of data and of the refusal to do so, or their inaccuracy; and

• the Data Subject’s possibility of exercising his/her rights of access rectification and deletion of his/her data.

b. Sensitive Data

The Law requires that sensitive data may only be processed with the express written consent of the Data Subject. Furthermore, sensitive data may only be collected and processed for reasons of public interest specifically provided in the Law.

Sensitive data can only be collected and subject to processing for reasons of general interest authorized by law, or when the requesting body has a legal
order to do so. Moreover, these data can also be processed for statistical or scientific purposes when dissociated from the holders.

The formation of databases which store information that directly or indirectly discloses sensitive data is prohibited, except for those belonging to political parties, trade unions, churches, religious beliefs, associations, foundations and other non-profit entities with political, religious, philosophical or trade union links, making reference to racial or ethnic origin, health and sex life regarding the data of their members or partners. In any case, the communication of said data shall always require the Data Subject’s previous consent.

c. Minors
Minors need their parents or tutors’ consent since the law indicates that they cannot express valid consent. In Uruguay, the age of majority is 18.

d. Employee Consent
The local data protection authority has issued several resolutions admitting employees’ consent for certain data treatment.

e. Online/Electronic Consent
Electronic records are acceptable under Uruguayan law. Notwithstanding, validity of the Data Subject’s consent will depend on compliance with the abovementioned requirements established by the law. It should be underlined that electronic consent would not be sufficient in case of treatment of sensitive data, unless the consent is granted through a certified electronic signature, since written consent is required.

6. Information/Notice Requirements
Under the Uruguayan Data Protection Law, whenever Personal Data is collected and processed, regardless of the need to obtain prior consent, Data Subjects should be informed of the following:

- the purpose for which data shall be processed and who the recipients or categories of recipients of the data may be;
- the existence of the corresponding database, whether electronic or any other type, and the identity and address of the Data Controller;
- whether replies to the proposed questionnaire are mandatory or voluntary, particularly regarding sensitive data;
- consequences of the provision of data and of the refusal to do so, or their inaccuracy; and
- the Data Subject’s possibility of exercising his/her rights of access rectification and deletion his/her data.
7. Processing Rules

When processing Personal Data, both Data Controllers and Data Processors ought to comply with the principles of the law detailed in the previous sections.

Furthermore, the Law establishes that when third parties provide Personal Data processing services, said Personal Data may not be used for a purpose not specified in the service agreement. Additionally, the data may not be given to third parties, not even for storage thereof. Once the contractual service has been provided, the processed Personal Data should be destroyed, except upon express authorization of the service provider in those situations in which there is a reasonable presumption that there may be further orders. If this is the case, the Personal Data may be stored with the appropriate security conditions for a period of up to two years.

8. Rights of Individuals

The Law grants Data Subjects certain rights regarding their Personal Data. These are the rights of access, rectification, inclusion and suppression (deletion) of their data, as well as the right to update their data.

The right of access implies that Data Subjects, whether natural persons or legal entities, having proved their identity with the corresponding identity card or respective proxy, shall have the right to obtain any information on themselves registered in any database. Said right shall only be exercised free of charge within six-month intervals, unless a legitimate interest arises prior to the lapse of the six-month period according to the local legal framework. The exercise of the right of a deceased person concerning his/her Personal Data shall belong to any of his/her duly proven universal successors.

The information requested must be provided to the Data Subject in a clear way, which should not be encoded, in which case it shall be accompanied by an explanation of the terms used in a language accessible to the average knowledge of the population. Moreover, the information shall be comprehensive and associated to the entire record belonging to the Data Subject, even when the request only includes one aspect of his/her Personal Data. In no case shall the report disclose data belonging to third parties, even when related to the interested person. The Data Subject may choose whether the information should be provided in writing or through electronic, telephone, imaging or similar appropriate means for such purpose.

In relation to the remaining rights, persons or legal entities shall have the right to request the rectification, updating, inclusion or deletion of their Personal Data included in a database, when verifying an error, falseness or exclusion in the information of which the person/entity is the Data Subject.
The deletion or suppression of Personal Data shall only proceed in the following cases:

- damage to the rights and legitimate interests of third parties;
- obvious error; and
- contravention of a legal obligation.

During the process of verification, rectification or inclusion of Personal Data, the Data Controller, upon third parties’ request to access reports on such data, shall record the fact that said information is subject to review. In the case of data transfer or communication, the Data Controller must notify the rectification, inclusion or deletion to the recipient within five working days after the data processing is carried out.

The rectification, updating, inclusion, erasure or deletion of Personal Data, when appropriate, shall be carried out free of charge for the Data Subject.

Whenever Data Subjects exercise any of the rights detailed in this section, the Data Controller shall have five business days to either comply with the request to access, update, delete, rectify or include the data, or to state the reasons why it considers it not appropriate to do so. Once the aforementioned period has expired without any of the foregoing situations having taken place, the Data Subject shall have the right to initiate a “habeas data” action before the courts.

9. Registration/Notification Requirements

The principle of legality provides that the formation of a database will be lawful when the database is properly registered. The Law establishes the obligation for Data Controllers to duly register all their existing databases before the local data protection authority.

The Decree establishes the steps to be taken in order to file for the registration of databases, as well as the information required to be disclosed to the data protection authority in connection with said filing. Notwithstanding the foregoing, lately, registrations are carried out directly and solely through the local data protection authority’s website, it not being necessary to file the hard copy of the documentation as part of the registration process.

10. Data Protection Officers

In Uruguay there is currently no requirement to appoint or designate a data privacy officer or other individual accountable for the privacy practices of the organization.
11. International Data Transfers

There is a prohibition against transferring any Personal Data to countries or international organizations that do not offer proper protection in accordance with the standards of international or regional law on this matter.

This prohibition does not apply in the cases of:

- international judicial cooperation, in accordance with the corresponding international instrument, being either a treaty or a convention, with the particular circumstances under consideration;
- exchange of medical information, whenever required for the treatment of patients either for health or public hygiene reasons;
- bank or stock exchange transactions, pertaining to the respective transactions and in accordance with the applicable legislation;
- agreements within the framework of international treaties agreed upon by the Oriental Republic of Uruguay; and
- international cooperation among intelligence organizations to fight against organized crime, terrorism and drugs trade.

International transfer of data may also be possible in the scenarios mentioned below:

- the interested party has given his/her unmistakable consent to the intended transfer;
- the transfer is required to execute a contract between the interested party and the Data Processor or to execute pre-contractual measures taken at the interested party’s request;
- the transfer is required to enter into or execute a contract entered into, or to be entered into on behalf of the interested party, between the Data Processor and a third party;
- the transfer is required or demanded by law to protect a major public interest, or to acknowledge, exercise or defend a right in a judicial procedure;
- the transfer is required to protect the vital interest of the interested party; and
- the transfer takes place from a registry, which is created, by virtue of legal or regulatory provisions, to release information to the public and receive queries from the general public or from any person who may prove that he/she has a legitimate interest, as long as the conditions established by law for the query are met for each particular case.
Without prejudice to the above, the local data protection authority may authorize international transfers of Personal Data to a third country which does not guarantee the proper protection if the Data Controller offers the necessary guarantees for the protection of private life, of essential rights and freedoms of people, as well as guarantees for the exercise of their respective rights. Said guarantees may stem from the corresponding contractual clauses.

As a final note, international transfers of data within multinational companies (i.e., affiliates, subsidiaries, branches or a parent company) would be permitted if the local entity (Data Controller) files for the registration of a Code of Conduct (type of Corporate Binding Rules) before the local data protection authority, which would govern such transfers.

The local data protection authority has issued a resolution stating that countries deemed as providing the required levels of Personal Data protection include the European Union, as well as those to which the European Commission has granted an adequacy note. In practice, companies located in the US which have adhered to the Privacy Shield Framework are also deemed adequate under the local data protection authority's criterion.

12. Security Requirements

In order to comply with the principle of data security, the Data Controller or user of the database must take the necessary steps to ensure the security and confidentiality of Personal Data. Such measures must include the prevention of the alteration, loss or unauthorized data treatment, as well as detection of any re-direction of information, intentional or not, whether the risks come from human action or from the technical means used.

The Law expressly prohibits the inclusion of Personal Data within databases that do not comply with the technical conditions of integrity and security.

The local data protection authority has suggested that Data Controllers adopt the parameters established by ISO 27001 in order to comply with the obligations of the Law.

13. Special Rules for Outsourcing of Data Processing to Third Parties

The Law establishes that when third parties provide Personal Data processing services, said Personal Data may not be used for a purpose not specified in the service agreement. Additionally, the data may not be given to other persons, not even for storage thereof. Once the contractual service has been provided, the processed Personal Data should be destroyed, except upon express authorization of the service provider in those situations in which there is a reasonable presumption that there may be further orders. If this is the case, the Personal Data may be stored with the appropriate security conditions for a period of up to two years.
14. Enforcement and Sanctions

The local data protection authority is empowered to apply sanctions to Data Controllers or Data Processors whenever the provisions of the Law are infringed.

The sanctions are graduated according to the level of severity of non-compliance, the relapse of the non-compliant entity, and the damage, as follows:

- observation, when the infringement is very mild;
- warning, when the infringement is mild and the controller has no previous record of any other infringement;
- fine, when the infringement is mild and there is previous record of other infringements, or whenever the infringement is severe or very severe;
- suspension of the corresponding database, when the infringement is very severe; and
- closing of the corresponding database, when the infringement is very severe.

The suspension and closing of databases are to be applied when the infringement is very severe and the fine is not adequate to address the violations of the Privacy Act.

In practice, the local data protection authority does not have a policy of active control, but it acts upon claims of Data Subjects.

15. Data Security Breach

The Decree establishes that whenever an occurrence of a data security breach likely to affect the interests of Data Subjects in a significant manner comes to the knowledge of the Data Controller or Data Processor, regardless of the phase of processing, the Data Subjects shall be informed of such situation.

16. Accountability

According to local regulation, the Data Controller is accountable before the Data Subjects and the local data protection authority for non-compliance with the Law. Accordingly, the local data protection authority may impose sanctions for violations of the Law. In addition, the Data Subjects may resort to habeas data actions when rights related to their Personal Data are compromised. Data Subjects could further claim damages via a judicial procedure if a breach of the law concerning the treatment of their Personal Data results in damage to them.
17. Whistle-Blower Hotline

In Uruguay, while there is no specific law or regulation on whistle-blowing, a document referred to by the Spanish Regulator, issued by the WP117 concerning whistle-blowing in the field of accounting and internal auditing, which has been previously applied to other cases of whistle-blowing within the labor relationship context, may be used for reference. This document establishes certain requirements to be fulfilled when a company installs a whistle-blowing program.

18. E-Discovery

There is no specific law or regulation in Uruguay on e-discovery. Notwithstanding this, following the parameters of the Law, when implementing an e-discovery system, an organization may be required to: obtain the consent of employees if the collection of Personal Data is involved; and advise employees of the implementation of an e-discovery system, the monitoring of work tools and the storage of information.

19. Anti-Spam Filtering

There is no specific law or regulation in Uruguay on anti-spam filtering solutions. Notwithstanding this, following the parameters of the Law, when implementing an anti-spam filter solution into its operations, an organization is required to inform employees of the monitoring policies being implemented in the workplace.

20. Cookies

There is no specific regulation requiring the collection of Data Subjects’ consent before putting cookies or other tracking technologies on their devices. Nevertheless, and according to the criterion of the local data protection authority, consumers ought to be duly informed of the fact that said technologies will be activated, the manner to disable them, and the consequences for deactivating them. In practice, the most common manner to comply with the latter is through a clause within the site’s Privacy Policy.

21. Direct Marketing

The Law establishes that in the collection of addresses, the distribution of documents, advertising, commercial prospecting, sale or other similar activities, appropriate data may be processed to establish specific profiles with promotional, business or advertising purposes; or that help determine consumer habits, whenever they appear on publicly accessible documents or are provided by the Data Subjects themselves or obtained with their consent.
In the scenarios envisaged above, the Data Subject may exercise the right of access free of charge. Moreover, at any time, the Data Subject may request the removal or blocking of his/her data from the databases.

Accordingly, local regulation provides for:

- an opt-in option, except in those cases where the data is collected from public sources of information; and

- an opt-out possibility, which implies that the Data Subjects can request his/her removal from the database created for marketing/promotional purposes at any time, and that in every communication to the Data Subject, the option to be removed from the database shall be provided.
Venezuela

**Maria Eugenia Salazar**  
Caracas  
Tel: +58 212 276 5161  
mariaeugenia.salazar@bakermckenzie.com

**Hector Martinez**  
Caracas  
Tel: +58 212 276 5056  
hector.martinez@bakermckenzie.com
1. Recent Privacy Developments

Supreme Court of Venezuela establishes the main principles that regulate data privacy in Venezuela.

On 4 August 2011, the Constitutional Chamber of the Supreme Court issued Decision N° 1318 ("Decision 1318"), which is the first court decision that discusses the principles contained in Article 28 of the Venezuelan Constitution. Pursuant to Decision 1318, the main principles that regulate data privacy in Venezuela are the following:

- **The Autonomy of the Will Principle** – Any person whose data is included in a database is entitled to be informed about: (i) the collection of his or her data; (ii) the entity responsible for his or her data; (iii) the purposes for which the data is gathered; and (iv) the manner by which he or she may exercise the right of self-determination. These are subject to the existence of a "prior, free, informed, unequivocal and revocable consent" by the party affected, in the event the organization that is responsible for the data needs to disclose them.

- **Legality Principle** – The right to “information self-determination” can only be limited by means of rules having the rank of law, provided this is justified by the public interest, and such rules must be interpreted restrictively. In this regard, the Chamber makes it clear that the information gathered cannot be: (i) used for purposes that are contrary to the principles set forth in the decision under analysis or to constitutional guarantees; or (ii) processed by illegal or unfair methods.

- **Purpose and Quality Principle** – Organizations that wish to compile Personal Data of individuals must do so in strict compliance with the constitutional and sectorial laws and regulations, and this must be done with a clear purpose, reason or cause. This principle is deemed to be essential in order for the individual’s consent to be valid. According to this principle, the gathering and use of Personal Data of individuals must follow the principle of good faith and proportionality, and only data that is adequate, pertinent and not excessive for the purpose sought can be gathered.

- **Temporality and Preservation Principle** – Based on the right to protection of data, to intimacy, and to update the information contained in databases and in files of public and private persons, the Chamber held that the information contained in such systems must be updated regularly in order to avoid damage to the individuals as a result of obsolete data. In addition, the Chamber adopted the decisions of Colombian case law regarding the “right to oblivion” which is the right of all individuals to have their Personal Data updated once a default or delay has been remedied, and to forget the prior condition.
• **Accuracy and Self-Determination Principle** – The Personal Data must reflect the true condition of the individual. In this regard, the data must not only be up to date, but accurate and complete as well. In order to achieve the efficacy of this principle, clear and expeditious procedures must be set in order to ensure that the individuals have access to and knowledge about the Personal Data kept by public and private institutions about them. This also implies the right of individuals to demand the correction or deletion of incomplete, inaccurate, inadequate and excessive data, and to be advised of their correction.

• **Foresight and Integrality Principle** – Technological advances call for an analysis of the storage, compilation and use of personalized data jointly with other databases or records in which the individual’s Personal Data is stored, since if shown as a whole, they may be prejudicial to the individual or his or her interests or rights.

• **Safety and Confidentiality Principle** – All entities that handle the compilation, storage and use of databases are required to ensure the security of such data, and to prevent the modification thereof by unrelated third parties. This obligation remains even after the termination of the relationship between the entity and the relevant person. Additionally, the Chamber stated that this principle includes a prohibition on the transfer of the contents of databases to other states that do not ensure the adequate protection of Personal Data.

• **Protection Principle** – Judicial protection is not sufficient and it is necessary to have public entities with jurisdiction to prepare and implement models based on technical standards whereby the information in these databases is protected.

• **Responsibility Principle** – Any infringement of the right to protection of data will give rise to civil, administrative and criminal penalties. The liability for breach of this right will fall not only on officers in the banking sector, but also extends to any other sector responsible for information systems.

*Supreme Court of Venezuela holds that the address, local telephone number, mobile phone number and name of the relations of an individual constitute Sensitive Data*

On 8 May 2012, the Constitutional Chamber of the Supreme Court issued Decision N° 568 (“Decision 568”), in which the Chamber held that information regarding the address, local telephone number, mobile phone number, and name of the relations of an individual constitutes “Sensitive Data”.

In the decision under analysis, the Chamber decided to delete the above-mentioned data from the electronic version of a judicial decision published on
the website of the Supreme Court and stated that the disclosure of such data in the abovementioned website: (i) was considered to be excessive for the purposes of identifying the affected party; and (ii) constituted an unnecessary “privacy inherency” in the private life of the affected party.

Furthermore, Decision 568 ratified the Constitutional Chamber of the Supreme Court’s criteria provided for under Decision N° 344 dated 24 February 2006 pursuant to which the Constitutional Chamber held that in case of publication of electronic versions of judicial decisions on the website of the Supreme Court, which may (i) include “sensitive information”, or (ii) cause infringements to constitutional rights as a consequence of their publication, any judge or individual is entitled to request that the information identifying any affected party in such electronic versions is replaced with suspension points in square brackets (i.e., [...]).

Supreme Court of Venezuela decides that the “habeas data” action is not an ideal means of establishing the liability of individuals who obtain and use Personal Data to the detriment of individuals’ rights

On 5 June 2012, the Constitutional Chamber of the Supreme Court issued Decision N° 779 (“Decision 779”), pursuant to which the Constitutional Chamber held that the “habeas data” action is not an ideal means of establishing the liability of individuals who, despite not being responsible for the collection of certain data, obtain such data and use the same to the detriment of individuals’ rights to honor, reputation and “public image”. Furthermore, Decision 779 expressly provides that affected parties may submit their claims in connection with this issue before the competent criminal and/or civil courts in order to demand the liabilities, sanctions and indemnifications which may be applicable.

The Infogovernment Law

On 17 October 2013, the Infogovernment Law (“InfoLaw”) was published in the Official Gazette N° 40,274. The purpose of the InfoLaw is to establish the principles, basis and guidelines regarding the use of information technologies by Venezuelan governmental entities and organizations. Among the specific data privacy regulations included in the InfoLaw are the following:

- The use of information technologies by governmental entities and organizations comprises the protection of the honor, private life, intimacy, self-image, confidentiality and reputation of individuals, and therefore is subject to the limitations provided for under applicable laws.
- The information contained in public files and registries of governmental entities and agencies is public, save for cases where such information is related to the honor, private life, intimacy, self-image, confidentiality and reputation of individuals, and the security and defense of the Nation. Likewise, governmental agencies and entities must protect the
information that they: (a) obtain by means of information technologies; or (b) store in files and electronic registries.

- Governmental agencies and entities must notify individuals through information technologies with respect to: (a) the automatic collection of their data; (b) the purpose and use of their data and the individuals with whom such data will be shared; (c) the options available for accessing, ratifying, deleting and opposing the use of their data; (d) the safety measures applied to protect their data; and (e) the registration and storage of their data in the databases of governmental organizations and entities.

- Governmental agencies and entities may, upon the request of an authorized individual, collect data of children and adolescents in connection with their constitutional rights and guarantees through information technologies. Such data shall not be disclosed, assigned, transferred or shared without the prior consent of the legal representative of the child, save for the following cases: (a) when the child is emancipated; (b) within the course of criminal investigations; (c) when so ordered by a judicial decision; or (d) when so determined by applicable law. It is expressly established that the consent to collect children’s data may be revoked.

2. Emerging Privacy Issues and Trends

**Autonomy of the Will Principle** – The InfoLaw constitutes the first law that includes a specific provision reflecting the Autonomy of the Will Principle provided for under Decision 1318. Said law expressly indicates that any person whose data is included in a governmental agency or entity’s database is entitled to be informed about: (a) the automatic collection of their data; (b) the purpose and use of their data and the individuals with whom such data will be shared; (c) the options available for accessing, ratifying, deleting and opposing the use of their data; (d) the safety measures applied to protect their data; and, (e) the registration and storage of their data in the databases of governmental agencies and entities. Until the publication of the InfoLaw in the Official Gazette, the Autonomy of the Will Principle had only been developed in the jurisprudence of the Constitutional Chamber of the Supreme Court.

3. Law Applicable

There are no specific regulations on data privacy in Venezuela. Regulations contained in Venezuelan law in connection with data privacy and the transfer of Personal Data are limited to: (i) a few provisions set forth in the Constitution of the Bolivarian Republic of Venezuela; (ii) the principles regulated in Decision 1318; and (iii) certain references contained in special laws, some of which provide for sanctions in case of violation of the right to data privacy. The main laws that regulate data privacy issues in Venezuela are the following:
• Law of Informatic Crimes published in the Official Gazette N° 37.313 dated 30 October 2001;
• Law Protecting the Privacy of Communications published in Official Gazette N° 34.863 dated 16 December 1991;
• Law on Data Messages and Electronic Signatures published in the Official Gazette N° 37.148 dated 28 February 2001;
• Law of Credit, Debit, Prepaid and any other Financial Card or Electronic Payment published in the Official Gazette N° 39.021 dated 22 September 2008;
• Law for the Protection of Children and Adolescents, published in the Official Gazette N° 6.185 dated 8 June 2015;
• Law on Banking Sector Institutions published in the Official Gazette N° 40.557 dated 8 December 2014;
• The InfoLaw, published in the Official Gazette N° 40.274 dated 17 October 2013; and

4. Key Privacy Concepts

a. Personal Data

There is no specific definition for Personal Data under Venezuelan Law. However, on 14 March 2001, the Constitutional Chamber of the Venezuelan Supreme Court issued Decision N° 332, in which the Chamber ruled that privileged information subject to constitutional protection is such information contained in one or more registries that, when combined, could create a complete or partial profile of the individual whose data is included in such registry.

b. Data Processing

There is no specific definition for Data Processing under Venezuelan law. However, under the Law of Informatic Crimes, it is unlawful to access, capture, interfere with, reproduce, modify, deviate or eliminate, by means of any information technology, any data message, transmission signal or any other communication of a third party. It is also illegal to publish any information obtained by unlawful means.
c. **Processing by Data Controllers**  
There is no definition of a Data Controller under Venezuelan Law.

d. **Jurisdiction/Territoriality**  
General rules apply.

e. **Sensitive Personal Data**  
There is no specific definition of Sensitive Personal Data under Venezuelan Law. However, Decision 568 provides that information regarding the address, local telephone number, mobile phone number, and name of the relations of an individual constitutes “Sensitive Data”.

f. **Employee Personal Data**  
There is no specific definition for Employee Personal Data under Venezuelan Law. However, the principles contained in Decision 1318 should be taken into consideration when analyzing any Employee Personal Data issue.

5. **Consent**

a. **General**  
Consent of the Data Subject is required prior to the collection, processing and disclosure of Personal Data. Consent by the Data Subject must always be voluntary, informed, explicit and unambiguous. Under Venezuelan law, consent of the Data Subject can be obtained not only in writing, but also in different forms or formats that signify that consent has been provided.

When a Data Subject gives consent, it is understood to cover only the identified purpose(s). Fresh consent is required for purposes that have not been previously identified and consented to. The Data Subject has the right to withdraw consent at any time.

To be valid, consent of the Data Subject must be in the local language.

b. **Sensitive Data**  
There are no specific rules in Venezuela defining or regulating Sensitive Personal Data. It is generally subject to the same consent requirements as other Personal Data.

c. **Minors**  
The general principle is that consent from minors must be given by a legal guardian or parent. In certain cases, consent may be obtained directly from minors.

d. **Employee Consent**  
Employee consent is required to collect and process an employee’s Personal Data at all times.
e. **Online/Electronic Consent**

There are no specific rules in Venezuela defining or regulating online/electronic consent. However, electronic consent is permissible and can be effective in Venezuela if it (i) is properly structured and evidenced; and (ii) complies with the principles contained in Decision 1318.

6. **Information/Notice Requirements**

An organization that collects Personal Data is not obliged to provide Data Subjects with information or notice, before or after collection of Personal Data, absent a request for information from a Data Subject. The Data Subject may request and the organization must then provide the following information: (i) the organization’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) the organization’s privacy practices (which must be given in a clear and transparent manner); (v) third parties to which the organization discloses Personal Data; (vi) the consequences of not providing consent; (vii) the rights of the Data Subject; (viii) how Personal Data is retained; (ix) where Personal Data is transferred; (x) where Personal Data is stored; (xi) how to access and/or correct the Data Subject’s Personal Data; and (xii) the duration of the proposed processing.

7. **Processing Rules**

An organization that processes Personal Data must limit the use of the Personal Data to those activities that are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

8. **Rights of Individuals**

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data that the organization holds about the Data Subject and how the Personal Data is being processed; (ii) access the Data Subject’s Personal Data subject to some restrictions and/or qualifications; (iii) request the correction of the Data Subject’s Personal Data; (iv) request the deletion and/or destruction of the Data Subject’s Personal Data; and (v) exercise the writ of habeas data.

9. **Registration/Notification Requirements**

There are no requirements for organizations that collect and process Personal Data to register, file or notify before Venezuelan authorities. Data processing authorities are not provided for under Venezuelan Law.

10. **Data Protection Officers**

There is no requirement for organizations to designate a privacy officer or other individual who will be accountable for the privacy practices of the organization.
11. International Data Transfers

Organizations may transfer Personal Data outside of Venezuela provided that the receiving jurisdiction provides a similar level of protection, affected Data Subjects have been informed or have provided consent, and reasonable steps have been taken to safeguard the Personal Data to be transferred.

In addition, the Safety and Confidentiality Principle prohibits the transfer of the contents of databases to other states that do not have rules that guarantee the protection of the individuals’ Personal Data.

12. Security Requirements

Organizations are required to take steps to ensure that Personal Data in their possession and control are protected from unauthorized access and use; implement appropriate physical, technical and organization security safeguards to protect Personal Data; and ensure that the level of security is in line with the amount, nature, and sensitivity of the Personal Data involved.

13. Special Rules for Outsourcing of Data Processing to Third Parties

Organizations that disclose Personal Data to third parties are required to use contractual or other means to protect Personal Data, and may be required to comply with sector-specific requirements. Organizations may be liable, together with third-party providers, in case of breach by the latter.

Any disclosure of Personal Data to third parties is subject to the prior, express and revocable consent of the Data Subject.

14. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, administrative fines, penalties or sanctions, seizure of equipment, civil actions, class actions, criminal proceedings and/or private rights of action.

15. Data Security Breach

While there may be no specific rules addressing data security breaches, organizations that are involved in a data breach situation may, depending on the nature and scope of the breach, be required to notify authorities, notify the affected Data Subjects, gather information about the breach, assess the potential risk of harm to the Data Subjects, take steps to mitigate the harm to affected Data Subjects, take steps to contain the breach and to prevent future similar breaches, and assist authorities with any investigation relating to the breach.

Organizations involved in a data breach situation must comply with court orders.
An organization that is involved in a data breach situation may be subject to civil actions, class actions, and criminal prosecutions, depending on the circumstances.

16. Accountability
Organizations are not required to conduct privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of Personal Data.

17. Whistle-Blower Hotline
Whistle-blower hotlines may be established in Venezuela as long as they are in compliance with local laws.

18. E-Discovery
When implementing an e-discovery system, an organization is required to obtain the consent of employees if the collection of Personal Data is involved, and advise employees of the implementation of the system, the monitoring of work tools, and the storage of information.

19. Anti-Spam Filtering
There are no laws/rules on the implementation of an anti-spam filtering solution in Venezuela.

20. Cookies
There are no specific laws/rules in Venezuela that regulate the use and deployment of cookies. In general, the use of cookies must comply with data privacy laws to be valid. The consent of Data Subjects may be required before cookies can be used.

21. Direct Marketing
An organization that plans to engage in direct marketing activities with a Data Subject is required to obtain the Data Subject’s prior express (opt-in) consent.
Vietnam

Manh Hung Tran  
Hanoi  
Tel: +84439369398  
tmh@bmvn.com.vn

Thanh Son Dang  
Hanoi  
Tel: +84439369607  
thanhson.dang@bakermckenzie.com

Yee Chung Seck  
Ho Chi Minh City  
Tel: +84835202633  
yeechung.seck@bakermckenzie.com

Mai Phuong Nguyen  
Ho Chi Minh City  
Tel: +84835202630  
maiphuong.nguyen@bakermckenzie.com
1. Applicable Law

- Law No. 91/2015/QH13, adopted by the National Assembly on 24 November 2015 ("Civil Code").

- Law No. 92/2015/QH13, adopted by the National Assembly on 24 November 2015 ("Civil Procedure Code").

- Law No. 67/2006/QH11, adopted by the National Assembly on 29 June 2006 ("IT Law").

- Law No. 51/2005/QH11, adopted by the National Assembly on 29 November 2005 ("E-Transactions Law").

- Law No. 59/2010/QH12, adopted by the National Assembly on 17 November 2010 ("Consumer Protection Law").


- Law No. 86/2015/QH13 adopted by the National Assembly on 19 November 2015, on Cyber Information Security ("LOCIS").

- Law No. 10/2016/QH13 dated 5 April 2016, effective from 1 June 2017 ("Law on Children").

- Law No. 64/2006/QH11, dated 1 January 2007 ("Law on HIV/AIDS Prevention and Control").

- Law No. 40/2009/QH12, dated 23 November 2009 ("Law on Medical Examination and Treatment").

- Decree No. 99/2011/ND-CP guiding the implementation of the Consumer Protection Law, issued by the government on 27 October 2011 ("Decree No. 99").

- Decree No. 85/2016/ND-CP, issued 1 July 2016, detailing information security level classification ("Decree No. 85").

- Decree No. 58/2016/ND-CP, dated 1 July 2016, detailing the business of civil encryption products and services, and the exportation and importation of civil encryption products ("Decree No. 58").

- Decree No. 108/2016/ND-CP, dated 1 July 2016, detailing regulations on the provision of cyber information security services and products ("Decree No. 108").

- Decree No. 72/2013/ND-CP, dated 15 July 2013, on the management, provision, and use of internet services and online information ("Decree No. 72").
• Decree No. 64/2007/ND-CP, dated 10 April 2007, of the government on the application of information technology in state agency activities ("Decree No. 64").

• Decree No. 90/2008/ND-CP on Anti-Spam, dated 13 August 2008, as amended by Decree No. 77/2012/ND-CP dated 13 August 2012 ("Decree No. 90").

• Decree No. 52/2013/ND-CP, dated 16 May 2013, on e-commerce ("Decree No. 52").

• Decree No. 158/2013/ND-CP, dated 12 November 2013, on penalties for administrative violations pertaining to culture, sports, tourism and advertising ("Decree No. 158").

• Decree No. 174/2013/ND-CP, dated 13 November 2013, providing penalties for administrative violations pertaining to postal, telecommunication, information technology and radio frequency areas ("Decree No. 174").

• Decree No. 185/2013/ND-CP, dated 15 November 2013, providing penalties for administrative violations pertaining to trading activities, production, trade of counterfeiting or prohibited goods, and protection of consumers’ rights ("Decree No. 185").

• Decree No. 56/2017/ND-CP, dated 9 May 2017, guiding several articles of the Law on Children ("Decree No. 56").

• Decree No. 124/2015/ND-CP, dated 19 November 2015, amending and supplementing a number of provisions of Decree No. 185/2013/ND-CP, dated 15 November 2013, providing penalties for administrative violations pertaining to trading activities, production, trade of counterfeiting or prohibited goods, and protection of consumers’ rights ("Decree No. 124").

• Decision No. 05/2017/QD-TTg on providing emergency response plans to ensure national cyber information security ("Decision No. 05").

• Joint Circular No. 07/2012/TTLT-BTTTT-BVHTTDL, dated 19 June 2012, stipulating the Duties of Enterprises Providing Intermediary Service in Protection of Copyright and Related Rights in the Internet and Telecommunications Networks Environment ("Joint Circular No. 07").

• Circular No. 87/2013/TT-BTC, dated 28 June 2013, guiding e-transactions on the securities market ("Circular No. 87").

• Circular No. 20/2017/TT-BTTTT, dated 1 November 2017, provides regulations on coordinating and responding to information security incidents nationwide ("Circular No. 20").
2. Recent Privacy Developments

Vietnam has yet to pass a codified law or framework concerning data protection and privacy. References to data privacy and required levels of protection thereof are scattered throughout the Civil Code, Penal Code and sector-specific laws (including in banking, consumer protection, information technology, and telecommunications legislation) and implementing regulations. However, the first comprehensive law regulating cybersecurity in Vietnam, LOCIS, effective from 1 July 2016, enhanced the principles and requirements on the collection and use of data and its protection in “cyberspace”.

LOCIS applies to entities and individuals directly involved in or related to “cyber information security activities in Vietnam”, meaning the “protection of information and information systems in cyberspace from being illegally accessed, utilized, disclosed, interrupted, altered or sabotaged in order to ensure the integrity, confidentiality and usability of information”. Due to the broad definition of cyberspace (“an environment where information is provided, transmitted, collected, processed, stored and exchanged over telecommunications networks and computer networks”), it appears that LOCIS applies to entities and individuals engaged in cyber security activities on both public and private information networks. LOCIS regulates the collection, use, revision and removal of “personal information”\(^1\) (“Personal Data”) and requires Data Processors/Controllers\(^2\) to delete Personal Data once the purpose for which the information was collected no longer exists, or after the announced storage period has expired. Under LOCIS, state agencies are also legislatively empowered to investigate “information processing individuals and organizations”, both at their own initiative or upon complaint from a Data Subject, presumably to ensure legal compliance.

In 2017, two instruments were released to give greater direction on LOCIS and its implementing decrees, particularly around issues of security breaches.

3. Emerging Privacy Issues and Trends

The Vietnamese government is continuing its efforts to regulate online activities in order to exert greater control over content published on the internet and maintain national security.

---

\(^1\) For ease of reference, we use the generally accepted term “Personal Data”, noting that the direct translation from Vietnamese is actually “personal information.”

\(^2\) Vietnam does not delineate between a Data Processor and Data Controller, and thus responsibility in regard to protection of Personal Data does not vary depending on whether an entity would be considered a “processor” or “controller.”
Cybercrime and cybersecurity

As in other nations, cybersecurity continues to be of critical importance to the Vietnamese government, especially in light of recent cyberattacks on Vietnam’s aviation infrastructure and national airline’s network.

On 1 January 2018, the Penal Code 2015 came into effect. New sections on cybercrime can be found from Articles 285 to Article 291. For most offenses, the primary change from the previous Penal Code is the placement of these offenses under different articles, which often also come with increased penalties.

Relevant provisions include the following offenses:

- using computers, telecommunications network and electronic means to appropriate assets;
- illegally collecting, storing, transferring and disclosing information regarding bank accounts; and
- deliberately interfering with radio frequency systems in a harmful manner.

On 8 June 2017, the Ministry of Public Security (“MPS”) published a draft Cybersecurity Law for comment (“Draft Law”). This recently published Draft Law is the 14th version and was issued in October 2017. The Draft Law applies to organizations and individuals, regardless of geographical location, that are directly involved in the management, supply, and use of the cyberspace or cybersecurity of Vietnam.

The MPS has the broad authority to protect national sovereignty, security, social order, and safety. The Draft Law contains provisions granting the MPS the authority to temporarily suspend the operation license of service providers for posting illegal information, and requires that any products or services to be used in “critical systems” be appraised and approved by the MPS. The Draft Law also imposes a cooperation requirement and requires information system administrators/owners, telecoms and internet service providers to closely coordinate with the competent authorities to handle illegal cyber information, such as information prejudicial to the state or government. This imposes an obligation to put in place technical measures to prevent the displaying of and to delete any “illegal information”.

The 14th version of the Draft Law also includes a data localization requirement, which requires telecommunication and internet service providers to maintain all personal information of Vietnamese citizens on servers located in Vietnam. The 14th version of the Draft Law also imposes commercial presence and storage requirements for telecommunication and internet service providers.
On 10 January 2018, mainstream media outlets in Vietnam reported that the Standing Committee of the National Assembly (“Standing Committee”) discussed various issues regarding the Draft Law. According to local news reports, the server localization provision, which requires that offshore telecommunications and Internet service providers put servers in which Vietnamese users’ data is administered within the territory of Vietnam, is absent in the version of the Draft Law that was submitted to the Standing Committee. This version is an update of the 14th version but has not been officially published.

Nonetheless, Article 27 of this recently updated draft requires offshore entities, when providing telecommunications and Internet services in Vietnam, among other conditions, to store within the territory of Vietnam (i) data of Vietnamese users, and (ii) other important data collected and/or generated from the use of Vietnam’s national cyber-infrastructure.

Additionally, any cross-border transfer of Personal Data in a critical system must be approved by the MPS or a competent agency as designated by the MPS following a security assessment.

Data Localization Requirements

Vietnamese law requires IT service providers to maintain, within Vietnam, a copy of any information they hold in order to facilitate inspection by authorities. Currently, Decree No. 72 also requires online social networks, aggregated information websites, mobile telecom network-based services and online games services to have a local server in Vietnam (i.e., at least one server must be located in Vietnam).3

The local server must meet the following requirements:

- store all user registration information that allows users to connect and authenticate user information with a personal identification number system at the request of the competent state agencies;
- store the entire history of the information posting activities on the general information websites and user information provision and sharing on social networks;
- allow the conduct and storage of all activities relating to censoring information posted on general information websites and social networks; and
- permit the competent authority’s full inspection and examination activities at any given time as well as settling users’ complaints in accordance with

---

3 Articles 24, 25, 28, and 34 of Decree No. 72.
user agreements on general information websites, social networks, and relevant regulations.

Non-compliance will result in an administrative fine of up to VND 40 million.4 In practice, it remains unclear to what extent these requirements apply to cross-border service providers, as implementing provisions mainly contemplate onshore entities.

In the banking sector there are residency-esque regulations when it comes to the matter of backing up data. In particular, any entity with its primary IT system and backup IT system both outside of Vietnam must conduct daily backups of electronic data on trading operations and store them within Vietnam. The entity must ensure the ability to convert original raw data from the backup. Backed up data must be checked and converted at least once every six months.

As mentioned, if the draft Cybersecurity Law is passed as currently worded in the 14th draft, administrators of information systems critical to national security (“Critical Systems”) will be required to store Personal Data and critical data within the national territory of Vietnam. For movement of such data outside of Vietnam, an assessment on the level of security will need to be carried out according to regulations by the MPS or other existing laws (if any). The Draft Law, which outlines the criteria to classify Critical Systems and the list of Critical Systems, is very broad. It remains unclear when an information system develops to a point that it is critical to national security and social order. If the information system is considered critical to national security and maintaining social order, the obligations under the law could greatly hinder the sharing of information with servers outside of Vietnam. In addition, as mentioned above, the Vietnamese media has recently reported that the most recent updates of the draft Cybersecurity Law requires offshore entities, when providing telecommunications and Internet services in Vietnam, among other conditions, to store within the territory of Vietnam (i) data of Vietnamese users, and (ii) other important data collected and/or generated from the use of Vietnam’s national cyber infrastructure. Again, we note that the updated version of the draft Cybersecurity Law has not yet been officially published.

4. Key Privacy Concepts

a. Personal Data

Vietnam does not have a single comprehensive law that addresses individual and organizational privacy rights. Instead, relevant provisions are contained in the Civil Code, the IT Law, the Consumer Protection Law, the Penal Code, the Telecommunications Law, the Law on Children, and LOCIS. Although these

---

4 Articles 64, 65 and 68, Decree No. 174.
matters are addressed in fairly general terms, implementing regulations contain more specific provisions.

As a general principle, these laws protect information pertaining or belonging to individuals or (to a lesser degree, organizations) that can serve to personally identify individuals (i.e., Personal Data). The above laws and regulations do not employ consistent definitions of what information constitutes Personal Data. The definition and specificity thereof vary depending on the sector to which the regulation/law applies.

The Civil Code grants individuals privacy rights to their mail, telephone, electronic mail and other types of electronic information, providing that the “collection and publication of information and materials on the private life of an individual must be consented to by that person...”5. These provisions grant individuals the right to the privacy of their Personal Data which, when violated, may provide grounds for a civil suit under Article 38 of the Civil Code.

The IT Law provides that entities and individuals are not permitted to supply the personal information of another person to any third party unless otherwise provided by law or agreed to by such person.6 The Telecommunications Law defines “personal information” in the context of call log data that telecommunication providers must protect and keep secure.7

LOCIS broadly defines Personal Data as “information associated with the identification of a specific person”, and the owner of such information is “a person identified based on such information”.8

Decree No. 72, which concerns online content, defines Personal Data as “information associated with the identifications of individuals, including names, ages, addresses, ID numbers, phone numbers, email addresses, and other information defined by law”. Decree No. 72 also introduces the concept of “private information”, which is defined as “the online information of an organization or individual not publicized by that organization or individual, or only provided for a group of receivers that are identified”. Article 3.14 of Decree No. 72 also defines “public information” as “online information of an organization or individual publically provided without identifications or addresses of receivers”. In the context of e-transactions, Decree No. 52 defines Personal Data as “information contributing to identifying a specific individual, including his/her name, age, home address, phone number, medical information, bank account number, information on personal payment

---

5 Article 38.2, Civil Code. Please note that although Vietnamese law does not define “publication” in this context, a reasonable interpretation would conform to the common law definition of transmission to third parties.
6 Article 22.2, IT Law.
7 Article 6.3, Telecommunications Law.
8 Article 3.15, LOCIS.
transactions and other information that the individual would like to keep confidential”.

In the context of implementing the Law on Children, Decree No. 56 defines “private [and/or] personal data of children” as information regarding: names, ages, personal identification features, health status and private information included in health records; personal images; family members’ information [and/or] caretakers’ information; personal property; phone numbers; personal mailing addresses; addresses [and/or] information regarding residence [and/or] origin; addresses [and/or] information on school, class, academic results, and friendship; [and] information on services provided to an individual child.

b. Data Processing
LOCIS defines the processing of Personal Data as the performance of one or more of the following: collecting, editing, using, storing, providing, sharing or spreading Personal Data in cyberspace for a commercial purpose.

Entities that collect, process and use the personal information of other persons in the network environment must obtain the Data Subject’s consent. They must also notify the Data Subject of the form, scope, place and purpose of the processing of his or her personal information. Entities and individuals are entitled to collect, process, and use the personal information of an individual without his or her consent where the Personal Data is used for the following purposes:

- signing, modifying or performing of contracts for the collection, processing and use of information, products or services in the network environment;
- pricing or calculating charges for the use of information, products or services in the networked environment; and
- performing other obligations in accordance with the law.

Otherwise, Data Processors/Controllers must not transfer Personal Data to any third party without the Data Subject’s consent, unless otherwise provided by law.

c. Jurisdiction/Territory
No provision specifically limits the scope of privacy laws to the jurisdiction/territory of Vietnam.

d. Sensitive Personal Data
Sensitive Personal Data is not a well-developed concept under Vietnamese law.

Decree No. 72 (which broadly governs the management and use of the internet) distinguishes between “private” and “personal” information. “Private information” is defined as “the online information of an organization or
individual that is not publicized by that organization or individual, or has only been provided for a group of receivers that are identified”. On the other hand, “Personal Information” is defined as “information associated with the identifications of individuals, including names, ages, addresses, ID numbers, phone numbers, email addresses, and other information defined by law”. Although somewhat vague in the Decree, it appears a Data Processor’s duty to protect a Data Subjects’ “Private Information” is greater than the duty to protect “Personal Information”. The foregoing suggests that certain Personal Data belonging to individual and organizational Data Subjects may be protected and may represent the first step towards creating a separate category of “Sensitive” Data – as seen in other jurisdictions.

In addition, sector-specific regulations protect certain data, such as medical records, and information provided to insurance providers, against illegal disclosure and use.

e. **Employee Personal Data**
Vietnamese law does not specifically regulate the protection of Personal Data in the employment context.

f. **Access and correction**
To the extent that information is collected, processed, or used in a digital electronic system, the IT Law requires information holders to permit individuals to require the information holder to re-inspect, correct, or cancel information upon request, and refrain from supplying or using relevant personal information until it is corrected.⁹

5. **Consent**
a. **General**
Consent of the Data Subject is generally required prior to the collection, processing and disclosure of Personal Data, subject to certain prescribed exceptions.

Consent is contemplated as a justification or legal grounds for the collection, processing, and/or use of Personal Data.

In general, consent may be express or implied, but the appropriate form of consent will depend upon the circumstances, expectations of the Data Subject, and sensitivity of the Personal Data. When the Data Subject gives consent, it is understood to only cover the identified purpose(s). There is no explicit requirement for consent to be in writing. Broadly interpreted, consent may be provided orally or in different forms and formats. However, it is more prudent to have the Data Subject’s consent in writing. In addition, the Data Subject also has the right to withdraw consent at any time.

⁹ Article 21(2)(d), IT Law.
Consent does not need to be in the local language, provided that the Data Subject understands the language in which consent is given.

b. Sensitive Data
The concept of Sensitive Data is not well developed in Vietnam. Generally, the collection and publication of information and data about the private life of an individual requires that person’s consent.

c. Minors
As a general principle, announcing or disclosing information about the privacy or secret of a child who is under seven years old requires the consent of the child’s parent(s) or guardian. For children from seven years old to under 16 years old, consent of the child is also required.\(^{10}\)

The Law on Children does not specify how consent is obtained from either the child or their parent(s)/guardian for the collection and use of the Personal Data of the child.

It is noticed that under the Civil Code, for a minor under the age of six, a parent or other representative must give consent to any transaction concerning the minor’s private life. Minors from six to under 18 years of age must have the consent of their legal representatives to enter into and perform civil transactions, except for civil transactions which are for the daily needs of such age group.\(^{11}\)

d. Employee Consent
Vietnamese law does not specifically regulate the protection of Personal Data in the employment context.

An employee has the obligation to provide to his/her employer information about full name, age, gender, residence address, education level, occupational skills, health condition and other information directly relating to the execution of their employment agreement.\(^{12}\)

However, while it is not explicitly required under the law that the employer requires consent from the Data Subject to process and/or disclose to third parties, it is still prudent to obtain consent for such purpose.

e. Online/Electronic Consent
Vietnamese law does not specifically address the issue of online/electronic consent. Up to now, the validity of online/electronic consent has not been challenged by the relevant authority.

---

\(^{10}\) Article 36.1, Decree No. 56.
\(^{11}\) Article 21.2, Civil Code.
6. Notice Requirements

An entity that collects Personal Data must provide Data Subjects with information about: (i) the entity’s identity; (ii) the types of Personal Data being collected; (iii) the purposes for collecting Personal Data; (iv) third parties to which the entity will disclose the Personal Data; (v) the rights of the Data Subject; (vi) how the Personal Data is retained; (vii) where the Personal Data is to be transferred; (viii) where the Personal Data is to be stored; and (ix) how to access and/or correct the Data Subject’s Personal Data.

7. Sector-Specific Regulations – Healthcare

Currently, there is no comprehensive provision addressing the collection and use of healthcare information. Accordingly, general data privacy laws should apply.

That said, there are specific provisions that outline information that can be considered sensitive in the context of healthcare. For instance, this includes HIV status13, medical records14, sperm/embryo donation information, organ/tissue donation information, gender reassignment information, etc.

There are also specific data retention obligations that can apply to healthcare information. Medical records of inpatients and outpatients must be retained for at least 10 years. Medical records of victims of labor and daily-life accidents must be retained for at least 15 years. Further, medical records of patients with mental illness and dead patients must be retained for at least 20 years. Healthcare specific privacy breaches can result in sanctions that range from monetary fines to public apologies.

8. Processing Rules

An entity that processes Personal Data must limit the use of Personal Data to only those activities that are necessary to fulfill the identified purpose(s) for which the Personal Data was collected.

9. Rights of Individuals

Data Subjects have the general right to: (i) be informed by an organization of the Personal Data the organization holds about the Data Subject and how the Data Subject’s Personal Data is being processed; (ii) request the correction of the Data Subject’s Personal Data; and (iii) request the deletion and/or destruction of the Data Subject’s Personal Data.

---

13 Article 8.5, Law on HIV/AIDS Prevention and Control.
14 Article 8, Law on Medical Examination and Treatment.
10. Registration/Notification Requirements

No authority is specifically tasked with administering the collection, processing, use and transfer of Personal Data in Vietnam.

11. Data Protection Officers

No requirement for an entity employing an “information system” to appoint or designate a data privacy officer exists in Vietnam. However, government information systems that serve the public or those of state bodies must have a department in charge of the information system’s operation and protection, which would include the protection of Personal Data located therein.

12. International Data Transfers

No provision explicitly addresses international data transfers. Generally, requirements around data transfers to third parties, as described above, apply.

13. Security Requirements

Data Controllers/Processors are required to protect Personal Data in their possession by implementing appropriate physical, technical and organizational security safeguards to prevent unauthorized access and use of Personal Data. Data Controllers/Processors must make publicly available the measures employed to process and protect Personal Data.

14. Special Rules for Outsourcing of Data Processing to Third Parties

Entities must obtain the consent of the Data Subject before outsourcing Personal Data for processing to third parties. If an entity discloses Personal Data to third parties, the disclosing entity may be required to use contractual or other means to protect the Personal Data. In case a data breach occurs, the outsourcing organization may be held liable together with the third-party provider.

15. Enforcement and Sanctions

Failure to comply with data privacy laws can result in complaints, data authority investigations/audits, data authority orders, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions, and/or criminal proceedings.

16. Data Security Breach

A data security breach is broadly defined under LOCIS as a “cyber information security incident”, which is an incident that harms or affects the integrity, confidentiality or usability of data contained in the system, or harms the information system itself.
If a cyber information security incident occurs, the Ministry of Information and Communications and other relevant parties must coordinate an emergency response. Network users must notify service providers or specialized departments if they are aware of a breach. Entities and individuals must report an internet incident or breach that they are unable to handle on their own to one or more of the following members of the Incident Response Network: the network member responsible for incident response for that user (if any); the internet service provider (“ISP”) that directly supplies internet services to the user; and/or the Vietnam Computer Emergency Response Team (“VNCERT”).

On 16 March 2017, the Prime Minister issued Decision No. 05, which lays out the basic framework for reporting and responding to cyber information security incidents. Circular No. 20, further elaborates on the action plans to respond to non-serious cyber information security incidents.

Incidents under the authority of Ministry of Defence and Ministry of Public Security are not covered by Decision No. 05 or Circular No. 20.

Serious incidents under the scope of Decision No. 05 include:

a. Information systems of Level 4 or Level 5, or of the List of Important National Information Systems, of which:
   - the service is interrupted;
   - state confidential/top secret data is likely disclosed;
   - important data cannot be secured as to integrity and recovered;
   - the system administrator has been deprived of the control right; or
   - the incident likely occurs on a wide scale or impacts on and causes damage to the other Level 4/Level 5 systems; AND

b. The operator of the information system is not able to control and remedy the incident.

Responding procedures for serious cyber information incidents will follow the action plans set out in Decision No. 05. Responding procedures for non-serious cyber information incidents are regulated under Circular No. 20.

Decision No. 05 provides that certain entities must become members of the National Cyber Information Security Incident Response Network (“Incident Response Network”). This Incident Response Network includes entities in the state sector, such as:

- units in charge of incident response, information security or information technology of ministries, ministerial-level agencies, the government’s affiliates and central-level agencies; Departments of Information and Communications of provinces or central-affiliated cities;
relevant agencies/units affiliated with the Ministry of Information and communications; the Authority of Information Security, VNCERT, Vietnam Internet Network Information Center and the Authority of Central Posts;

• relevant agencies/units affiliated with the MPS: Authority of Cyber Security; Police Department for High-Tech Crime Prevention; and

• relevant agencies/units affiliated with the Ministry of National Defence: Department of Information Technology; Governmental Cipher Committee.

Decision No. 05 also requires certain entities and units that are possibly in the private sector to join the Incident Response Network. This includes telecommunications companies, ISPs, data centers, data storage leasing companies, IT and cybersecurity departments/units of banking and financial institutions, National Treasury, tax, and customs bodies/authorities.

Members of the Incident Response Network are responsible for complying with the operating regulations of the Network and coordination orders given by the National Coordination Center.

Particularly, telecommunications enterprises and ISPs shall store and provide information concerning the IP address of subscribers, servers, internet of things equipment, log files and logs of domain name systems within the scope of their management; provide space for installing monitoring/sampling equipment and provide data flows on the Internet to serve the supervision and detection of incidents upon request of the National Coordination Center; arrange a 24/7 standing team and personnel and material resources to cooperate and develop solutions for responding to and remedying consequences of incidents in cases where the source of cyberattacks originates from subscriber(s) under the enterprise’s management or at the request of the National Coordination Center.

The following subjects may be directly involved or related to cyber information security activities in Vietnam:

• Administrator of the information system ("Administrator"): as defined under LOCIS, it means an organization or individual who directly administers an information system. More specifically, as defined under Circular No. 03, it means the body (the term used by Circular No. 03) of an organization/entity that has the authority to make decisions on the investment, establishment, upgrade and expansion of the information system.

• Operator of the information system ("Operator"): as defined under Circular No. 03, it means a body designated by the Administrator to operate such information system. If the Administrator outsources information technology services, the Operator shall be the service provider. Circular No. 20 contemplates that any individual/organization
being the Operator must report to the Administrator, VNCERT and other relevant agencies about incidents.

- Other organizations and individuals that do not operate the information ("Other Persons"): not defined by law.

Pursuant to Article 9.1 of Circular No. 20, the Operator shall, within five days after detecting an incident, report information on the incident to the following agencies and units:

- the Administrator;
- the national coordinating agency: VNCERT;
- the specialized accident response unit; and
- the member of the concerned incident rescue network (if any).

At the time of reporting, if the incident has not been completely solved, organizations and individuals operating the system shall have to update its incident report to the agencies and units that received the report before the incident was completely resolved.

The Operator has a duty to notify when a “cyber information security incident” occurs, which is defined in Circular No. 20 as an incident where information or an information system is attacked or harmed, affecting the integrity, confidentiality or usability of the information or information system.

Currently, penalties for not complying with incident reporting obligations are provided under Article 71 of Decree No. 174 (up to VND 70 million, approx. USD 3,180).

17. Accountability

“Information owning” entities must classify the data in their possession based on its level of secrecy and take appropriate security measures to ensure the protection of such data.\(^\text{15}\)

Telecommunication enterprises, enterprises providing telecommunications applications services and enterprises providing information technology services and enabling the sharing of information are required to provide information on their technical and professional security measures upon request by competent state agencies to manage and ensure cyber information security.\(^\text{16}\)

\(^{15}\) Article 9, LOCIS.
\(^{16}\) Article 10, LOCIS.
18. Whistle-Blower Hotline

A whistle-blower hotline has not been established by any of the rules. However, LOCIS requires state agencies to establish an online system to receive petitions and reports from the public concerning information system security systems and protection of Personal Data. State agencies must inspect and examine data processing entities and conduct extraordinary inspection and examination when necessary.

19. E-Discovery

Vietnamese law does not contemplate the concept of e-discovery and no guidelines exist on the use of such a system. Electronic data is recognized as evidence in both civil and criminal litigation.

According to the Civil Procedure Code, the court may not disclose material that contains “business secrets”, “family secrets” or “secrets concerning an individual’s private life” during the course of an investigation, which to that effect could include Personal Data.

In a criminal investigation, the retrieval and seizure of electronic data must follow the principles of due process according to the Criminal Procedure Code.

20. Anti-Spam Filtering

When implementing an anti-spam filter solution into its operations, an entity may be required to inform users of the filtering policies being implemented, particularly if the collection of Personal Data is involved. The entity must afford the user an opportunity to review the isolated emails designated as spam.

Email service providers are required to provide free anti-spam filtering to users.17

21. Cookies

No specific laws/rules regulate the use of cookies. The use of cookies would have to comply with data privacy laws.

22. Direct Marketing

An organization that plans to engage in direct marketing activities with a Data Subject may be required to obtain the Data Subject’s prior consent. The request for prior consent must be clearly expressed.18

---

17 Article 19, Decree No. 90.
18 Article 7, Decree No. 90.
Consent must specify:

- the type of advertised information, products and services;
- the maximum number of advertising emails/text messages sent within a given period of time and the time of sending advertisements.\(^{19}\)

An organization cannot infer consent from a Data Subject's failure to respond.

\(^{19}\) Article 8, Decree No. 90.
Baker McKenzie Offices Worldwide

Office phone numbers and addresses change from time to time. Please refer to www.bakermckenzie.com for current contact information.

**Argentina – Buenos Aires**
Cecilia Grierson 255, 6th Floor
Buenos Aires C1107CPE
Argentina
Tel: +54 11 4310 2200
Fax: +54 11 4310 2299

**Australia – Brisbane**
Level 8
175 Eagle Street
Brisbane QLD 4000
Australia
Tel: +61 7 3069 6200
Fax: +61 7 3069 6201

**Australia – Melbourne**
Level 19
181 William Street
Melbourne VIC 3000
Australia
Tel: +61 3 9617 4200
Fax: +61 3 9614 2103

**Australia – Sydney**
Tower One - International Towers
Sydney, Level 46
100 Barangaroo Avenue
Sydney, Australia
Tel: +61 2 9225 0200
Fax: +61 2 9225 1595
Austria – Vienna
Schottenring 25
1010 Vienna
Austria
Tel: +43 1 24 250
Fax: +43 1 24 250 600

Azerbaijan – Baku
The Landmark Building
90A Nizami Street
Baku AZ1010
Azerbaijan
Tel: +994 12 497 18 01
Fax: +994 12 497 18 05

Bahrain – Manama
18th Floor
West Tower
Bahrain Financial Harbour
P.O. Box 11981
Manama
Kingdom of Bahrain

Belgium – Antwerp
Meir 24
2000 Antwerp, Belgium
VAT BE 0426.100.511 RPR Brussels
Tel: +32 3 213 40 40
Fax: +32 3 213 40 45

Belgium – Brussels
Louizalaan 149 Avenue Louise
Eleventh Floor
1050 Brussels, Belgium
VAT BE 0426.100.511 RPR Brussels
Tel: +32 2 639 36 11
Fax: +32 2 639 36 99

Brazil – Brasilia
SAF/S Quadra 02,
Lote 04, Sala 203
Ed. Comercial Via Esplanada
Brasilia
DF - 70070-600
Tel.: (55-61) 2102-5000
Fax.: (55-61) 3323-3312

Brazil – Porto Alegre
Av. Borges de Medeiros,
2233 - 4º andar - 90110-150
Porto Alegre - RS
Tel.: (55-51) 3220-0900
Fax: (55-51) 3220-0901

Brazil – Rio de Janeiro
Av. Rio Branco,
1 - 19º andar
Ed. RB1
Setor B - 20090-003
Rio de Janeiro - RJ
Tel.: (55-21) 2206-4900
Fax: (55-21) 2206-4949

Brazil – São Paulo
Rua Arq. Olavo Redig de Campos,
105 – 31º andar - Ed. EZ Towers
Torre A
04711-904
São Paulo - SP
Tel.: (55-11) 3048-6800
Fax: (55-11) 5506-3455

Canada – Toronto
181 Bay Street, Suite 2100
Toronto, Ontario M5J 2T3
Canada
Tel: +1 416 863 1221
Fax: +1 416 863 6275
**Chile** – **Santiago**
Avenida Andrés Bello 2457, Piso 19
Providencia, CL 7510689
Santiago
Chile
Tel: +56 2 2367 7000

**China** – **Beijing**
Suite 3401, China World Office 2,
China World Trade Centre,
1 Jianguomenwai Dajie,
Beijing 100004
Tel: +86 10 6535 3800
Fax: +86 10 6505 2309

**China** – **Hong Kong**
14th Floor, Hutchison House,
10 Harcourt Road, Central,
Hong Kong SAR
Tel: +852 2846 1888
Fax: +852 2845 0476

**China** – **Shanghai**
Unit 1601, Jin Mao Tower,
88 Century Avenue, Pudong,
Shanghai 200121
Tel: +86 21 6105 8558
Fax: +86 21 5047 0020

**Colombia** – **Bogota**
Avenue 82 No. 10-62 6th Floor
Bogota
Colombia
Tel: +57 1 634 1500 / 644 9595
Fax: +57 1 376 2211

**Czech Republic** – **Prague**
Praha City Center,
Klimentská 46
Prague 110 02
Czech Republic
Tel: +420 236 045 001
Fax: +420 236 045 055

**Egypt** – **Cairo**
Nile City Building, North Tower
21st Floor 2005C, Cornich El Nil
Ramlet Beaulac
Cairo
Egypt
Tel: +20 2 2461 9301, +20 2 2461 5520
Fax: +20 2 2461 9302

**France** – **Paris**
1 rue Paul Baudry
75008 Paris
France
Tel: +33 1 4417 5300
Fax: +33 1 4417 4575

**Germany** – **Berlin**
Friedrichstraße 88/Unter den Linden
10117 Berlin
Germany
Tel: +49 30 2 20 02 81 0
Fax: +49 30 2 20 02 81 199

**Germany** – **Dusseldorf**
Neuer Zollhof 2
40221 Dusseldorf
Germany
Tel: +49 211 3 11 16 0
Fax: +49 211 3 11 16 199

**Germany** – **Frankfurt**
Bethmannstraße 50-54
60311 Frankfurt/Main
Germany
Tel: +49 69 2 99 08 0
Fax: +49 69 2 99 08 108

**Germany** – **Munich**
Theatinerstrasse 23
80333 Munich
Germany
Tel: +49 89 5 52 38 0
Fax: +49 89 5 52 38 199
Hungary – **Budapest**
Dorotyta utca 6.
1051 Budapest
Hungary
Tel: +36 1 302 3330
Fax: +36 1 302 3331

**Indonesia – Jakarta**
Hadiputra, Hadinoto & Partners,
The Indonesia Stock Exchange
Building
Tower II, 21st Floor
Sudirman Central Business District
Jl. Jendral Sudirman Kav. 52-53
Jakarta 12190
Indonesia
Tel: +62 21 2960 8888
Fax: +62 21 2960 8999

**Italy – Milan**
Piazza Meda, 3
Milan 20121
Tel: +39 02 76231 1
Fax: +39 02 7623 1620

**Italy – Rome**
Viale di Villa Massimo, 57
Rome 00161
Tel: +39 06 44 06 31
Fax: +39 06 4406 3306

**Japan – Tokyo**
Ark Hills Sengokuyama Mori Tower,
28th Floor
1-9-10, Roppongi, Minato-ku
Tokyo 106-0032
Japan
Tel: +81 3 6271 9900
Fax: +81 3 5549 7720

**Kazakhstan – Almaty**
Samal Towers, 8th Floor
97, Zholdasbekov Street
Almaty Samal-2, 050051
Kazakhstan
Tel: +7 727 330 05 00
Fax: +7 727 258 40 00

**Luxembourg**
10 - 12 Boulevard Roosevelt
Luxembourg 2450
Luxembourg
Tel: +352 26 18 44 1
Fax: +352 26 18 44 99

**Malaysia – Kuala Lumpur**
Wong & Partners, Level 21, The Gardens South Tower
Mid Valley City
Lingkaran Syed Putra
Kuala Lumpur 59200
Malaysia
Tel: +603 2298 7888
Fax: +603 2282 2669

**Mexico – Guadalajara**
Av. Paseo Royal Country 4596
Torre Cube 2, 16th Floor
Fracc. Puerta de Hierro
Zapopan, Jalisco 45116
Mexico
Tel: +52 33 3848 5300
Fax: +52 33 3848 5399

**Mexico – Juárez**
P.O. Box 9338 El Paso, TX 79995
P.T. de la República 3304, 1st floor
Juárez, Chihuahua 32330
Mexico
Tel: +52 656 629 1300
Fax: +52 656 629 1399
Mexico – Mexico City
Edificio Virreyes
Pedregal 24, 12th floor
Lomas Virreyes / Col. Molino del Rey
Mexico City, 11040
Mexico
Tel: +52 55 5279 2900
Fax: +52 55 5279 2999

Mexico – Monterrey
Oficinas en el Parque
Torre Baker McKenzie, 10th floor
Blvd. Antonio L. Rodríguez 1884 Pte.
Monterrey, N.L. 64650
Mexico
Tel: +52 81 8399 1300
Fax: +52 81 8399 1399

Mexico – Tijuana
P.O. Box 1205 Chula Vista, CA 91912
Blvd. Agua Caliente 10611, 1st floor
Tijuana, B.C. 22420
Mexico
Tel: +52 664 633 4300
Fax: +52 664 633 4399

Morocco – Casablanca
Ghandi Mall - Immeuble 9 Boulevard Ghandi
20380 Casablanca
Morocco
Tel: +212 522 77 95 95
Fax: +212 522 77 95 96

Myanmar – Yangon
Level 18, Unit 18-03 Sule Square
221 Sule Pagoda Road,
Kyauktada Township
Yangon
Myanmar
Tel: +95 1 925 5095

Netherlands – Amsterdam
Claude Debussylaan 54
1082 MD Amsterdam
P.O. Box 2720
1000 CS
Amsterdam
The Netherlands
Tel: +31 20 551 7555
Fax: +31 20 626 7949

Peru – Lima
Av. De la Floresta 497
Piso 5 San Borja
Lima 41
Peru
Tel: +51 1 618 8500
Fax: +51 1 372 7171/ 372 7374

Philippines – Manila
Quisumbing Torres,
12th Floor, Net One Center
26th Street Corner 3rd Avenue
Crescent Park West
Bonifacio Global City
Taguig City 1634
Philippines
Tel: +63 2 819 4700
Fax: +63 2 816 0080; 728 7777

Poland – Warsaw
Rondo ONZ 1
Warsaw 00-124
Poland
Tel: +48 22 445 3100
Fax: +48 22 445 3200
Qatar – Doha
Al Fardan Office Tower, 8th Floor
Al Funduq Street
West Bay
P.O. Box 31316
Doha, Qatar
Tel: +974 4410 1817
Fax: +974 4410 1500

Russia – Moscow
White Gardens
9 Lesnaya Street
Moscow 125047
Russia
Tel: +7 495 787 2700
Fax: +7 495 787 2701

Russia – St. Petersburg
BolloevCenter, 2nd Floor
4A Grivtsova Lane
St. Petersburg 190000
Russia
Tel: +7 812 303 9000
Fax: +7 812 325 6013

Saudi Arabia – Jeddah
Abdulaziz I. Al-Ajlan & Partners,
Bin Sulaiman Center, 6th Floor, Office No. 606,
Al-Khalidiyah District, P.O. Box 128224
Prince Sultan Street and Rawdah Street Intersection
Jeddah 21362
Saudi Arabia
Tel: +966 12 606 6200
Fax: +966 12 692 8001

Saudi Arabia – Riyadh
Abdulaziz I. Al-Ajlan & Partners,
Olayan Complex
Tower II, 3rd Floor
Al Ahsa Street, Malaz
P.O. Box 69103
Riyadh 11547
Saudi Arabia
Tel: +966 11 265 8900
Fax: +966 11 265 8999

Singapore
8 Marina Boulevard
#05-01 Marina Bay Financial Centre
Tower 1
Singapore 018981
Singapore
Tel: +65 6338 1888
Fax: +65 6337 5100

South Africa – Johannesburg
1 Commerce Square
39 Rivonia Road
Sandhurst
Sandton
Johannesburg
South Africa
Tel: +27 11 911 4300
Fax: +27 11 784 2855

South Korea – Seoul
17/F, Two IFC
10 Gukjegeumyung-ro
Yeongdeungpo-gu
Seoul 150-945
Korea
Tel: +82 2 6137 6800
Fax: +82 2 6137 9433
Spain – Barcelona
Avda. Diagonal, 652
Edif. D, 8th Floor
Barcelona 08034
Spain
Tel: +34 93 206 0820
Fax: +34 93 205 4959

Spain – Madrid
Paseo de la Castellana, 92
Madrid 28046
Spain
Tel: +34 91 230 4500
Fax: +34 91 391 5149

Sweden – Stockholm
Vasagatan 7, Floor 8
P.O. Box 180
Stockholm SE-101 23
Sweden
Tel: +46 8 566 177 00
Fax: +46 8 566 177 99

Switzerland – Geneva
Rue Pedro-Meylan 5
Geneva 1208
Switzerland
Tel: +41 22 707 9800
Fax: +41 22 707 9801

Switzerland – Zurich
Holbeinstrasse 30
Zurich 8034
Switzerland
Tel: +41 44 384 14 14
Fax: +41 44 384 12 84

Taiwan – Taipei
15F, 168 Dunhua North Road
Taipei 10548
Taiwan
Tel: +886 2 2712 6151
Fax: +886 2 2712 8292

Thailand – Bangkok
25th Floor, Abdulrahim Place
990 Rama IV Road
Bangkok 10500
Thailand
Tel: +66 2636 2000
Fax: +66 2636 2111

Turkey – Istanbul
Ebulula Mardin Cad., Gül Sok. No. 2
Maya Park Tower 2, Akatlar-Beşiktaş
Istanbul 34335
Turkey
Tel: +90 212 339 8100
Fax: +90 212 339 8181

Ukraine – Kyiv
Renaissance Business Center
24 Bulvaro-Kudriavska (Vorovskoho)
Street
Kyiv 01601
Ukraine
Tel: +380 44 590 0101
Fax: +380 44 590 0110

United Arab Emirates – Abu Dhabi
Level 8, Al Sila Tower
Abu Dhabi Global Market Square
Al Maryah Island, P.O. Box 44980
Abu Dhabi
United Arab Emirates
Tel: +971 2 696 1200
Fax: +971 2 676 6477

United Arab Emirates – Dubai
Level 14, O14 Tower
Al Abraj Street
Business Bay, P.O. Box 2268
Dubai
United Arab Emirates
Tel: +971 4 423 0000
Fax: +971 4 447 9777
Venezuela – Caracas
Centro Bancaribe, Intersección Avenida Principal de Las Mercedes con inicio de Calle Paris, Urbanización Las Mercedes Caracas 1060 Venezuela
Tel: +58 212 276 5111
Fax: +58 212 993 0818; 993 9049

Venezuela – Valencia
Urbanización La Alegria P.O. Box 1155 Valencia Estado Carabobo Venezuela
Tel: +58 241 824 8711
Fax: +58 241 824 6166

Vietnam – Hanoi
Unit 1001, 10th floor, Indochina Plaza Hanoi 241 Xuan Thuy Street, Cau Giay District Hanoi 10000 Vietnam
Tel: +84 24 3825 1428
Fax: +84 24 3825 1432

Vietnam – Ho Chi Minh City
12th Floor, Saigon Tower 29 Le Duan Blvd District 1 Ho Chi Minh City Vietnam
Tel: +84 28 3829 5585
Fax: +84 28 3829 5618
Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.