Data Protection and Privacy Officer Priorities 2019

Annual survey highlights strategies that matter for governance and compliance

CPO MAGAZINE

Survey Highlights

28% say their primary challenge is working with other business units to integrate data protection and privacy measures

52% named building a privacy-aware culture or enhancing governance of data processing as a top priority

17% of organizations with early stage data protection and privacy programs are prioritizing new technology deployments

45% spend less than $250,000 annually on data protection and privacy

23% have only one employee working in the data protection and privacy function

Preparing for the post-GDPR privacy world

Organizations across the world are taking steps to build data protection and privacy into every business function

If there was one defining event of 2018, it was the much-anticipated enactment of the European General Data Protection Regulation (GDPR) in May. While this new data privacy regulation formally covered European Union data subjects, it was clear from the outset that this regulation would have sweeping, worldwide implications. Any corporation doing business in Europe or with EU citizens would need to play by the new rules of the post-GDPR privacy world.

With that in mind, our survey of 252 data protection and privacy officers from around the world sought to find out how they responded in the immediate aftermath of GDPR, as well as what their new priorities are for 2019. Not all organizations are the same, so this survey also sought to find out how priorities can shift depending on the size or industry of an organization.

Certainly, the role of the Data Protection and Privacy Officer in 2019 is no easier than it has been in past years. Mega breaches tend to be the norm, and not the exception. Every week seems to bring the story of a major new company or government entity that has just reported a new data breach. Moreover, cyber hackers and cyber criminals are becoming increasingly sophisticated in whom they target and how they breach an organization, raising the stakes even higher.

At the same time, consumers are becoming much more aware of privacy. With every new data privacy scandal, they are seeing how their data is openly being bought and sold in the gray corners of the Internet. And, often, it is the companies they trust the most with their data – the big tech companies of the world – that have betrayed them the most.

Not surprisingly, then, this rise of privacy consciousness has led to an increase in regulatory activity on a global basis. Within the United States, for example,

California's new Consumer Privacy Act is set to go into action on January 1, 2020 and several more states are readying privacy legislation of their own. That has raised the very real prospect that the United States could be on the verge of enacting sweeping, federal-level privacy legislation in 2020 that would emulate many of the protections provided to EU citizens under the GDPR.

Against this backdrop, enterprises and businesses of all sizes must be prepared. Data protection and privacy is no longer a "nice-to-have" – it is now a "must-have." Failure to protect consumer data appropriately carries with it the risk of financial penalties and punitive litigation. Clearly, data protection and privacy officers have a much tougher job to do in 2019. So what are their challenges and how can they prioritize their business goals?

The purpose and objective of this report is to provide an important overview of how top data protection and privacy officers are responding to the post-GDPR world. As they go about establishing data protection and privacy policies and procedures, what are they prioritizing? What challenges are they facing? And how successful have they been in making data protection and privacy a fundamental concept that is embedded into every single business function, rather than something that is simply grafted on at the last moment in order to check an item off a checklist?

By reaching out to 252 top professionals in the industry, many of them at some of the top companies in the world, we are closer to answering those questions and determining what steps need to be taken next in 2019 and beyond.

Key Finding 1

Primary challenge faced by organizations is simply getting all business units to embrace the need for a comprehensive data privacy and protection policy

Specific challenges faced by data protection and privacy officers depend on relative maturity of the organization's data protection and privacy program

Data protection and privacy officers continue to face many challenges, including the challenge of building out a comprehensive data protection and privacy strategy that can be embraced by the entire organization. In the post-GDPR world, data privacy and protection needs to be understood, embraced and implemented by all business units – and not just by the legal or compliance functions.

Thus, it is perhaps no surprise that more than one-quarter (28%) of respondents say that "working with various business functions" was the top challenge they faced. Implementing an organization-wide data protection and privacy program is actually harder than it sounds, due in large part to the prevailing consensus that new privacy measures can act within an organization as a brake on overall business activity. The job of the data protection and privacy officer is clear: Make the business case for privacy as a strategic imperative that can help an organization grow.

Surprisingly, only 13% of enterprises said that hiring and retaining qualified personnel was the

New Year Resolution

To embed data protection and privacy operations within the company's business operations.

Team Lead
Technology & Software Company

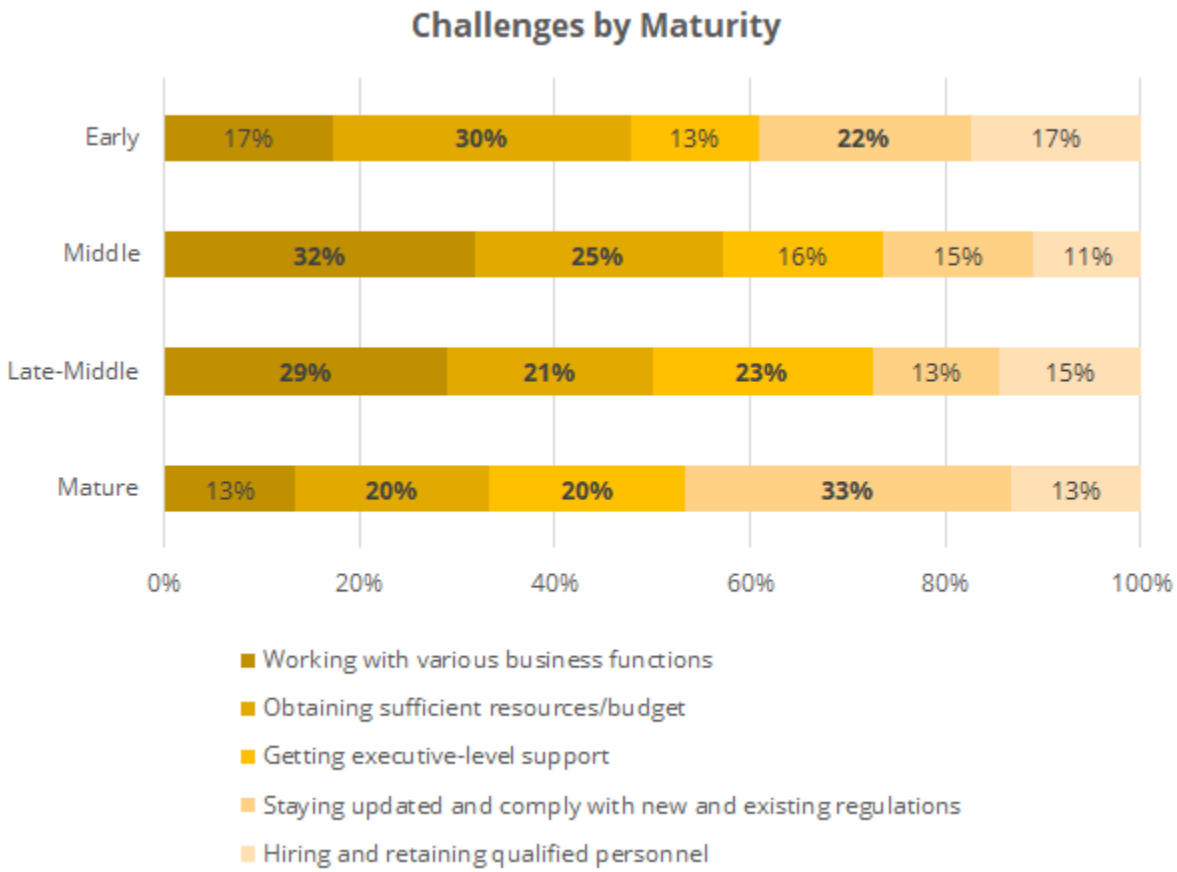
primary challenge they faced. This would seem to contravene the various reports of a "talent gap" in the industry, and the current perception that is difficult to find the right professionals to take on data protection and privacy roles. There are several possible explanations for this. One is that organizations simply have not started to "staff up" yet, and thus, have not started to encounter any competitive pressures in the hiring market. Another explanation is that organizations are simply making internal hires from elsewhere in the organization as they roll out their data protection and privacy programs. Keep in mind, too, that 45% (almost 1 in 2) respondents spend less than $250,000 on data protection and privacy activities across the enterprise. (see Key Finding 4)

From a big picture perspective, then, the cost of hiring additional personnel may not be viewed as a primary challenge when viewed against other organizational costs.

In this study, respondents were asked to rate their organization in terms of maturity of their data protection and privacy programs as follows:

- **Early stage** – Many program activities have not as yet been planned or implemented
- **Middle stage** – Program activities are planned and defined but only partially implemented
- **Late-Middle stage** – Most program activities are implemented across the enterprise
- **Mature stage** – Program has successfully been implemented across the enterprise

A closer look at the challenges based on program maturity shows that early stage and middle stage companies face very different challenges than those faced by late-middle and mature stage companies.



For example, the top challenge of organizations with Early stage data protection and privacy programs is simply obtaining sufficient resources/budget. Interestingly,

the problem of not getting executive-level support ranked 4th overall. This is somewhat surprising, given how often the need for executive-level commitment is often cited as an issue. One possible explanation is that privacy has finally entered the public consciousness to a degree that it is no longer required to "make the case" for privacy – what's needed now is simply putting the plan into action.

Working with various business functions is the top challenge for enterprises in the Middle (32%) and Late-Middle (29%) stage. This is likely due to implementing and cascading the privacy program across the enterprise, and facing pushbacks and roadblocks along the way.

For mature organizations, the top challenge is staying updated and complying with new and existing regulations. This may be due to deeper understanding of nuances and greater awareness of the global nature of business and the myriad of regulations and legislations. With increasing regulatory pressure on organizations, there is a growing realization that a failure to create an ironclad data protection and privacy program can lead to financial, legal and regulatory problems down the road.

New Year Resolution

To create a legally defensible data privacy & security program.

Senior Executive/VP
Technology & Software Company

Key Finding 2

Building a privacy-aware culture and enhancing the governance of data processing activities are the two top priorities of organizations

52% rank one of two options – building a privacy-aware culture or enhancing governance of data processing – as a top priority

According to the data protection and privacy professionals surveyed, there is currently higher priority on the organization and processes of a data program, and lower priority on technological solutions and training. Given the fact that the GDPR is still less than a year old, this is understandable. Building a privacy-aware culture is a necessary cornerstone for any robust data protection and privacy program. Moreover, a key building block in creating this more robust program naturally starts with enhanced governance over data processing activities.

In order to conform to privacy principles and meet all compliance requirements, an organization first must wrap its arms around what data it is collecting from consumers, how it is using this data, with whom it is sharing this data, and what safeguards currently exist so that the organization does not collect data improperly from consumers. Once this has been achieved, an organization can move from the strategic phase to a more tactical phase.

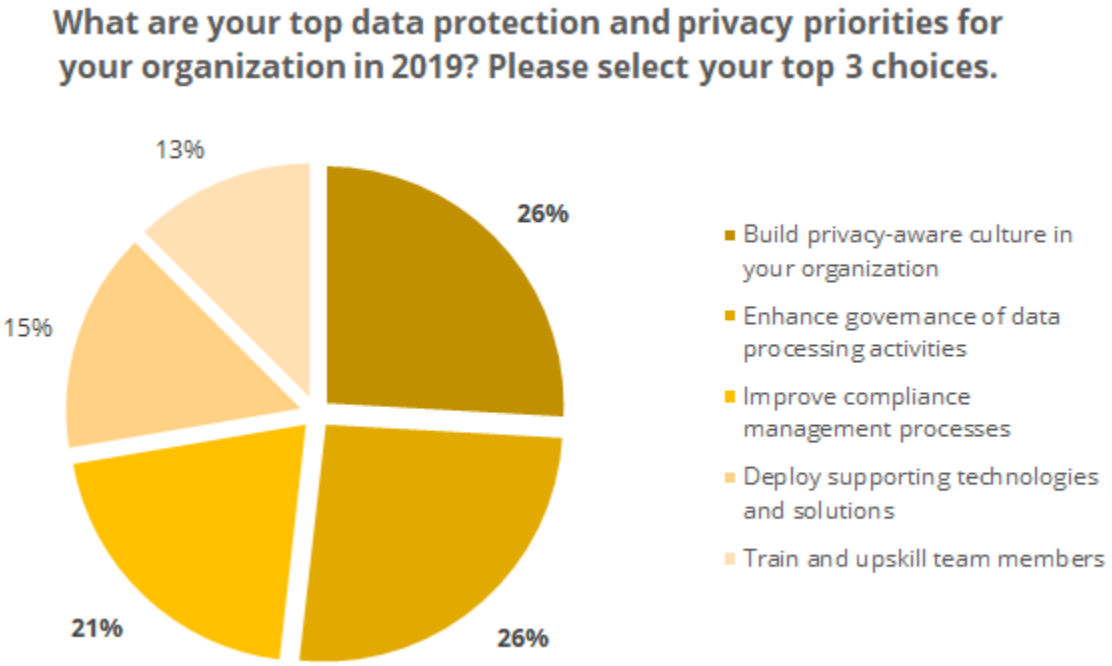
New Year Resolution

Embed more privacy unto organizational culture

Manager
Technology & Software Company

Heading into 2019, it would be expected that greater emphasis would be placed on training and

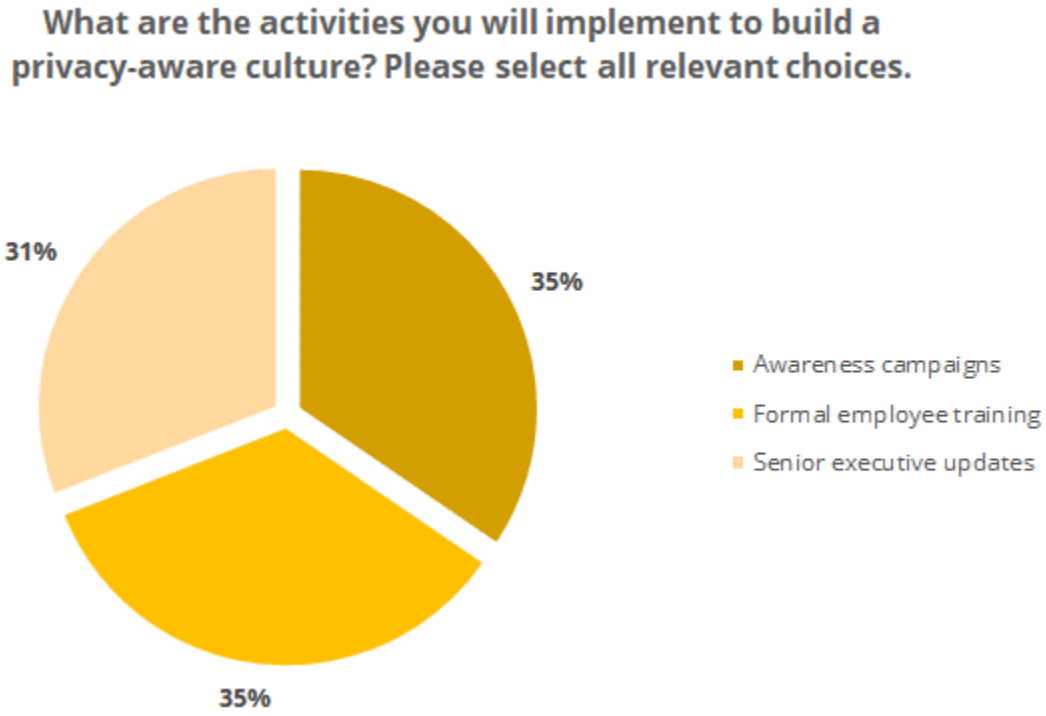
up-skilling of employees. The good news is that, based on other key findings showing that only 13% of organizations view hiring and retaining of employees as a primary challenge, it might not be as difficult as originally assumed to build a highly-trained data privacy team within a relatively short period of time.



Based on their initial response to the priority question, respondents were further asked to identify the activities that will be important to them to meet their business goals.

Building privacy-awareness culture as a priority

Respondents who ranked building culture as a top priority would like to focus on conducting awareness campaigns and implementing formal employee training. The focus is on the individuals in the organization. Any successful data protection and privacy program requires highly-trained individuals who are up-to-date on the latest privacy rulings and regulations and can make informed decisions.

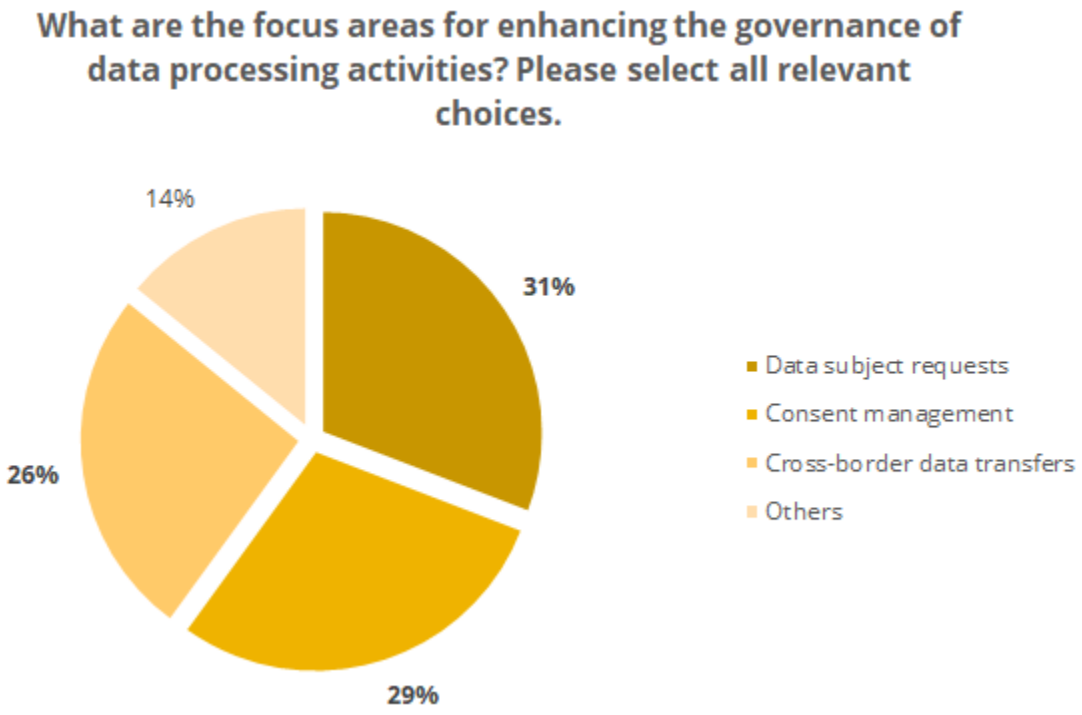


Governing data processing activities as a priority

Nearly one-third (31%) of respondents who ranked governance of data processing activities as a top priority stated a preference to focus on enhancing the process for data subject requests. Another 29% are looking to focus on consent management. Both of these are extremely important as part of the European GDPR and other data protection and privacy regulations. Companies must now obtain formal consent from data subjects, rather than simply relying on implied consent, and they must also make all data subjects aware of how their personal information will be used, how long it will be stored, and with whom the data will be shared.

In terms of focus areas for improving governance of data processing activities, 14% of respondents answered "Others." This broad classification of activities includes those not covered by data subject requests, consent management, and cross-border data transfers. The two most widely cited activities in “Others” included managing and tracking the use of personal data, and the retention and destruction of personal data. Other focus areas include implementing Privacy by Design to integrate privacy into the software, product and program development lifecycle;

and updating and aligning privacy notices. Privacy by Design is a new area of focus that stems directly from the GDPR: it is meant to ensure that all products are built in accordance with privacy principles from the very outset.



Enhancing compliance management as a priority

Respondents who ranked improving compliance management process as a top priority were evenly divided on which activity should be given the highest priority. For example, 20% of respondents are looking to focus on data protection and privacy impact assessment; 18% are looking to focus on data inventory and mapping; 17% are looking to focus on third-party assessment; and another 17% are looking to focus on data breach readiness.

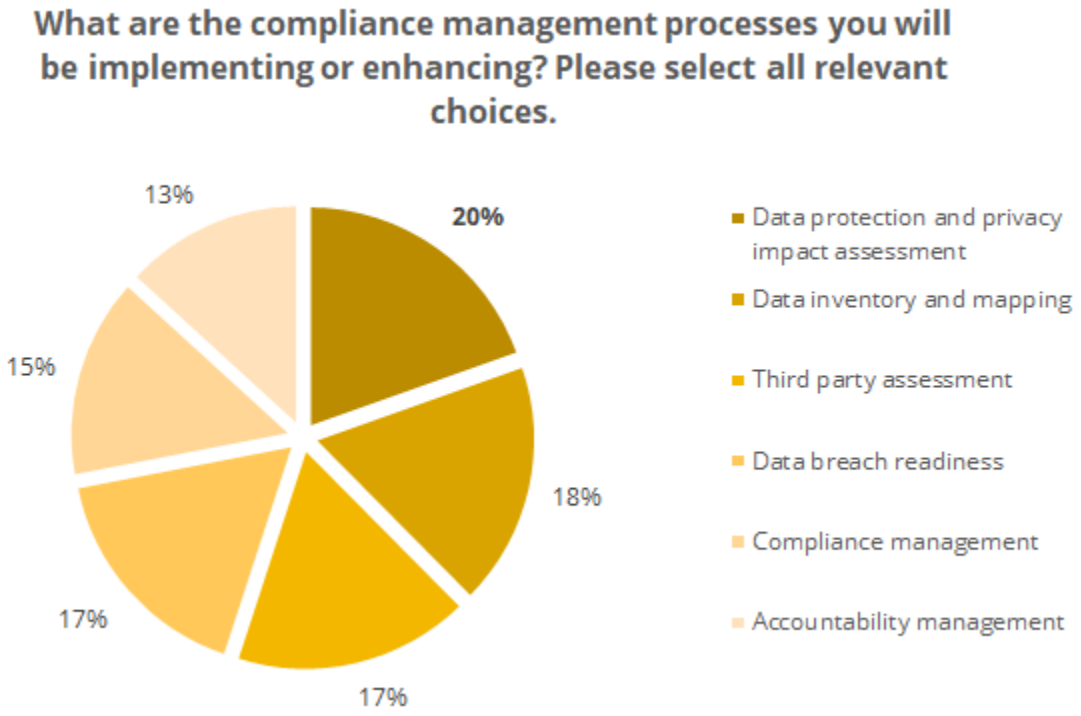
The top priority – data protection and privacy impact assessment – is particularly important in the framework of GDPR because it is one of the

New Year Resolution

To complete PIA and implement PbD into the company ecosystem.

Director
Technology & Software Company

first steps for ensuring that any new products are fully GDPR-compliant. Thus, the fact that companies are choosing to focus on these privacy impact assessments should be seen as a positive sign – it means that they are already starting to take a more proactive approach to making sure that data privacy is built into every product from the very outset.

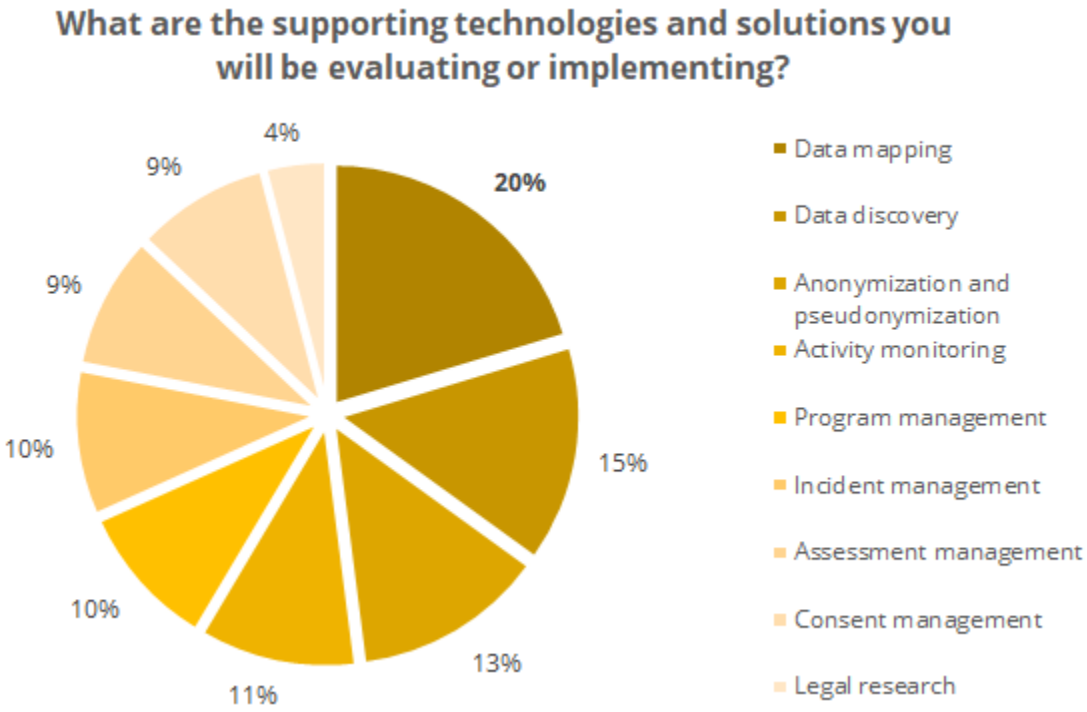


Supporting technologies and solutions as a priority

Respondents who ranked implementing technology as a top priority had the most interest in data mapping (20%) and data discovery (15%) solutions. This is very much in line with the top priority to "Enhance governance of data processing activities" (and within that category - "Data protection and privacy impact assessment" and "Data inventory and mapping").

Data mapping and data discovery solutions are more important than ever, now that organizations are expected to know exactly where data is being collected within an organization, how it is being used, and with whom it is being shared. Thus, these technologies and solutions support the priority of enhancing data governance by making it easier to manage and track data use. This is also seen in the interest in

activity monitoring solutions (cited by 12% of respondents). There is also interest in anonymization and pseudonymization solutions, which were mentioned by 13% of respondents. In the GDPR era, organizations must be more careful than ever that they do not include personally identifiable information in their data sets unless they have received the expressed written consent of their data subjects.



Training as a priority

More than one-third (39%) of respondents who ranked training and upskilling team members as a top priority mentioned understanding specific regulations and legislations as the most important, closely following by general privacy principles and frameworks (37%). New regulations are constantly appearing on the landscape, and while most are built on the same principles, each has its nuances and focus.

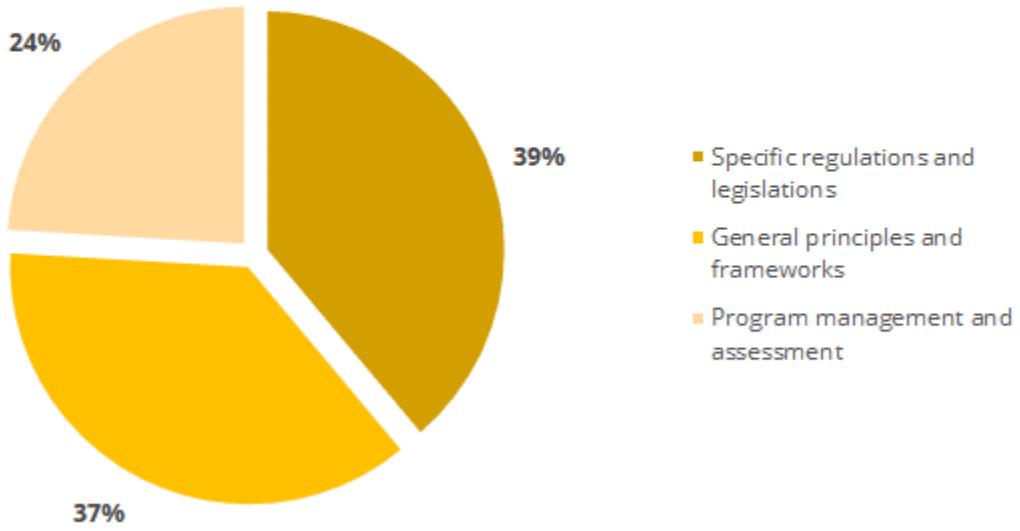
For example, within the United States, each of the 50 states has the ability to delineate what is meant by terms such as “personal data” or “personal information,” and they also have the ability to set their own penalties for failure to comply with their regulations. Since there is as yet no federal privacy legislation in the U.S., this can lead to a lot of uncertainty and confusion. For organizations doing business within any state, one key consideration is whether or not an individual has the right to private action, or the right to bring a civil lawsuit against a company, for a breach of data privacy regulations. Obviously, those geographies where individuals have the right to bring private action are the highest risk for organizations, and it would be expected that training budgets in those geographies would be the highest.

New Year Resolution

Being able to cope with the new forthcoming laws and regulations on data privacy.

Senior Executive/VP
Technology & Software Company

What are the training areas most relevant for your team members? Please select all relevant choices.

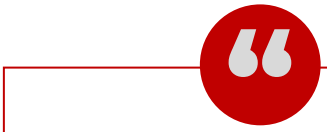


Key Finding 3

Priorities shift with the maturity of data protection and privacy programs

Organizations start with building a privacy aware culture and enhancing their governance of data processing before moving on to advanced technological or training solutions

Just as we have seen that challenges faced by organizations can differ significantly, depending on where their privacy program is on the maturity scale (i.e. Early stage, Middle, Late-Middle and Mature), the same is true for the data protection and privacy priorities of these organizations. It would be natural to assume that most organizations start with building an overall privacy culture, and then begin to implement specific steps needed to make that happen. Once the right policies and procedures have been put into place, organizations can begin to focus on training, technological adoption and implementation of advanced compliance processes.



New Year Resolution

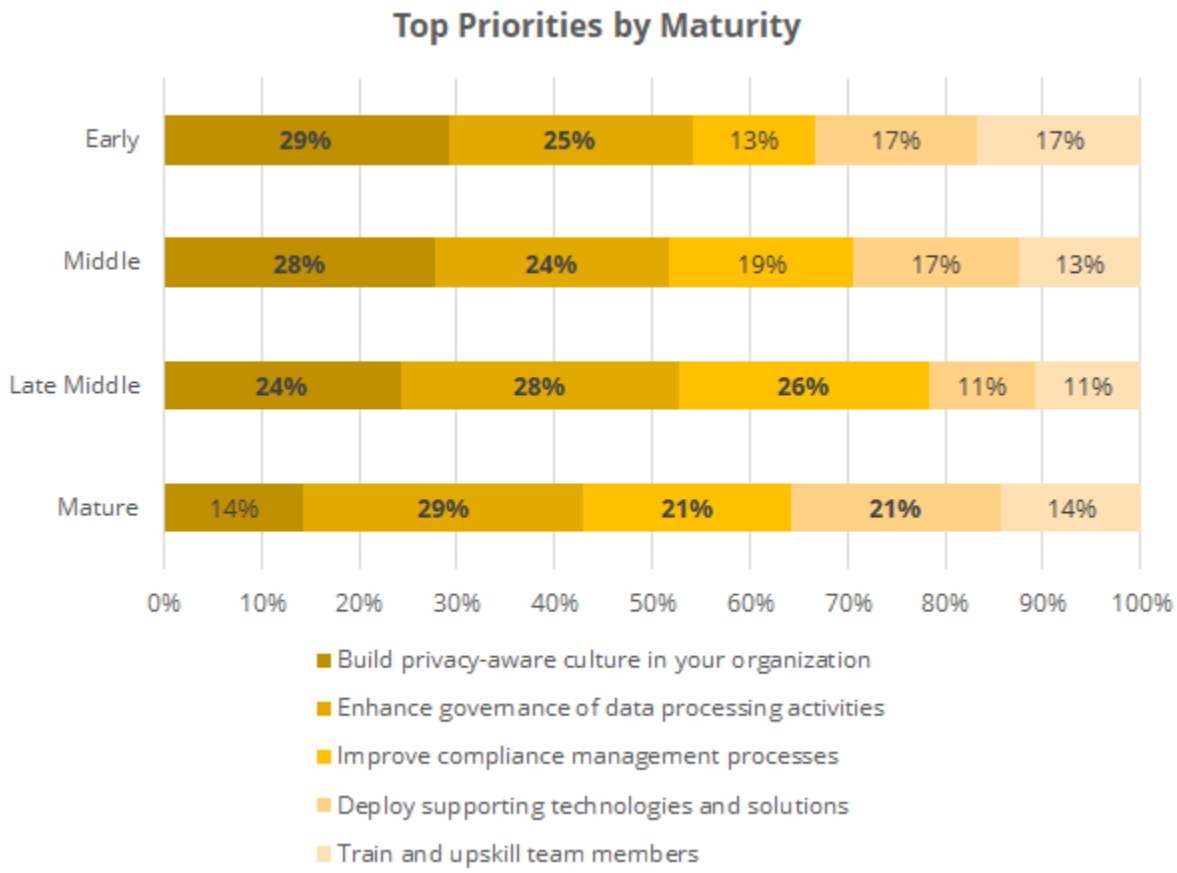
Strengthening the maturity level of data privacy implementation within the organization and build awareness culture.

Manager
Financial Services Company

And, indeed, that is exactly what this survey found. Building a privacy-aware culture is the highest priority for enterprises with Early stage data privacy programs, and steadily becomes less important as an organization's program matures. For example, 29% of organizations with Early stage data privacy programs cited the need for building a privacy-aware culture as their top priority. Contrast that to just 14% of organizations with Mature data privacy programs. This points to the

importance of starting with the right privacy culture in order to build a foundation for effective data privacy policies and procedures.

Enhancing governance of data processing activities is a priority for organizations across all levels of maturity. And, in fact, the priority becomes slightly more important as an organization's data privacy program matures. This points to a constant issue for privacy teams: as business expands, an organization will also have an expanding set of new privacy issues. This naturally leads to a need to embrace new technologies and business models in order to keep data processing activities at the required level (or higher).



Improving compliance management processes becomes more important as an organization matures. At the outset, when many privacy program activities have not been planned or implemented, compliance management is inevitably viewed as a long-term goal rather than an immediate priority. As new privacy programs start to

be implemented, this naturally leads to a greater understanding of the responsibilities of an organization from a compliance perspective.

Deploying supporting technologies and solutions is a higher priority for organizations with mature data privacy programs. This suggests that organizations view technology as a way to streamline the compliance process. Organizations with Early or Middle stage privacy programs are (rightfully) focusing on the organizational and process aspects of building a privacy culture. Only 17% of organizations with Early stage programs, for example, mentioned technological solutions as a top priority, compared to 21% of organizations with Mature programs. Tech solutions, if implemented from the outset, might help them accelerate their maturity.

New Year Resolution

Mature privacy capability. Begin monitoring of privacy controls.

Senior Executive/VP
Technology & Software Company

Key Finding 4

Almost half of organizations allocate less than 5% of governance, risk and compliance budget for data protection and privacy

Are organizations spending enough?

Given the unprecedented visibility of data protection and privacy as an issue impacting all organizations regardless of size, one expectation was that organizations across the board would be significantly increasing their spending in this area. Theoretically, organizations with early stage data privacy programs would be spending to put into place the right policies and procedures, while organizations with mature programs would be spending to hire more employees.

New Year Resolution

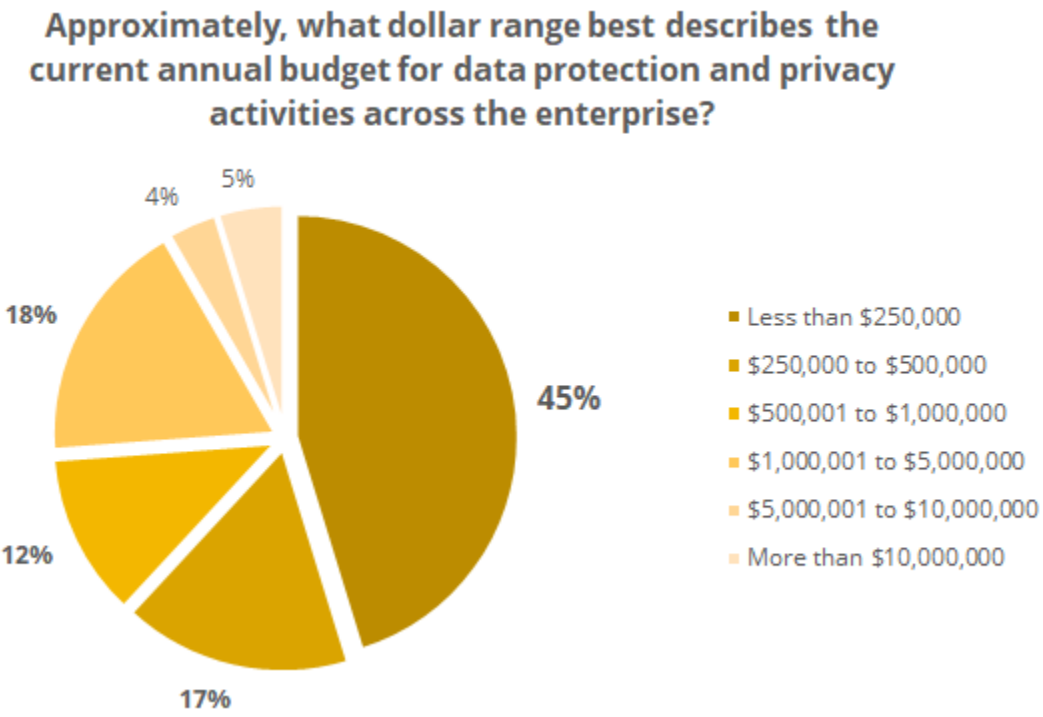
Hold senior executives accountable for data protection and tap their respective budgets for specific breach prevention strategies and/or remediation to include proactive monitoring and reporting.

Director
Agriculture & Food Service Company

Yet, nearly one-half (45%) of respondents spend less than $250,000 on data protection and privacy activities across the enterprise. To put that number into context, according to a recent IAPP survey, the average salary of a privacy professional is $123,000 per year. This means that half of enterprises surveyed hire a maximum of 2 privacy professionals, assuming that all of the annual budget is spent on headcount.

The expectation, however, is that organizations are spending on more than just headcount. They are also deploying technological solutions and spending money on training programs for employees, for example, in addition to investing in other

resources for the data protection and privacy team. This might help to explain the reason why many organizations employ only a single data protection and privacy professional. (see Key Finding 5)

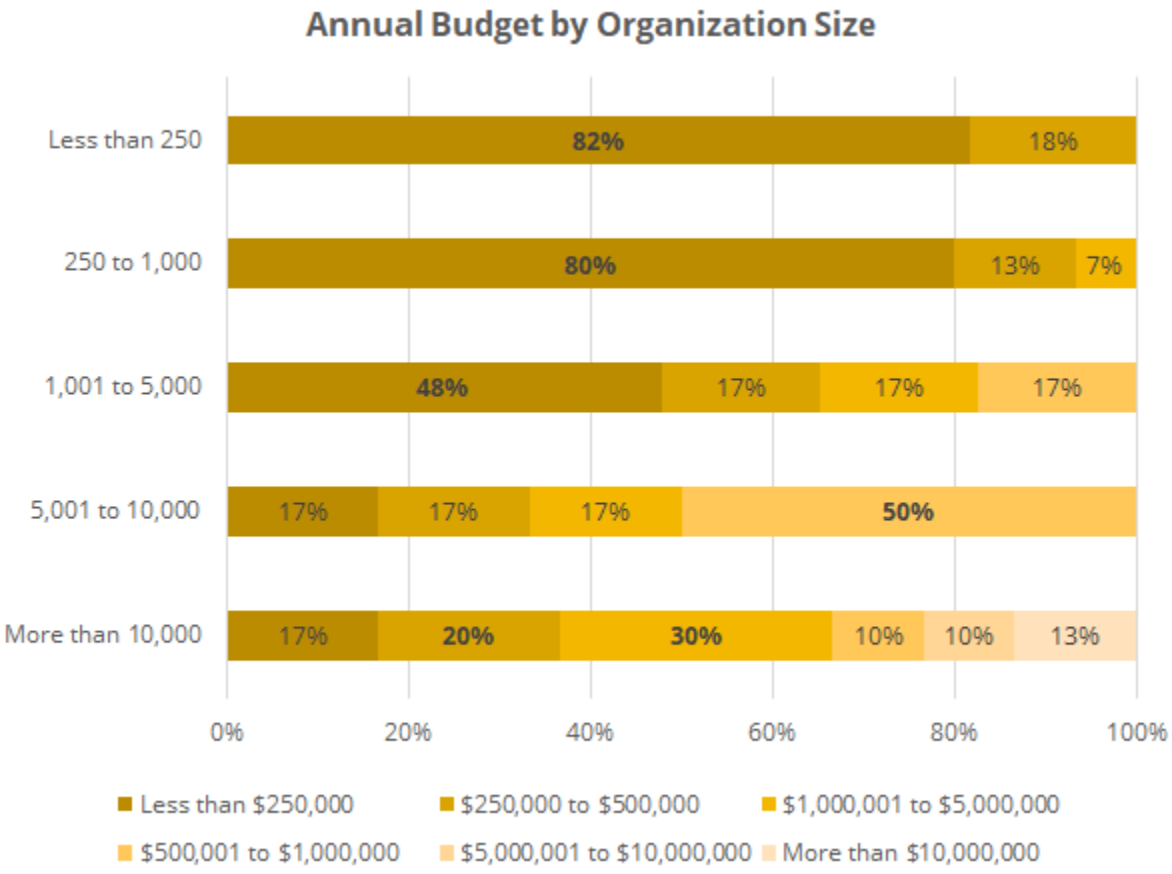


Limited spending by organizations with less than 1,000 employees

Approximately 80% of enterprises with less than 1,000 employees spend less than $250,000 annually on data protection and privacy activities. Almost half (48%) of enterprises with 1,001 - 5,000 worldwide employees spend less than $250,000 annually on data protection and privacy activities. And 17% of enterprises with more than 5,000 worldwide employees spend less than $250,000 annually on data protection and privacy activities.

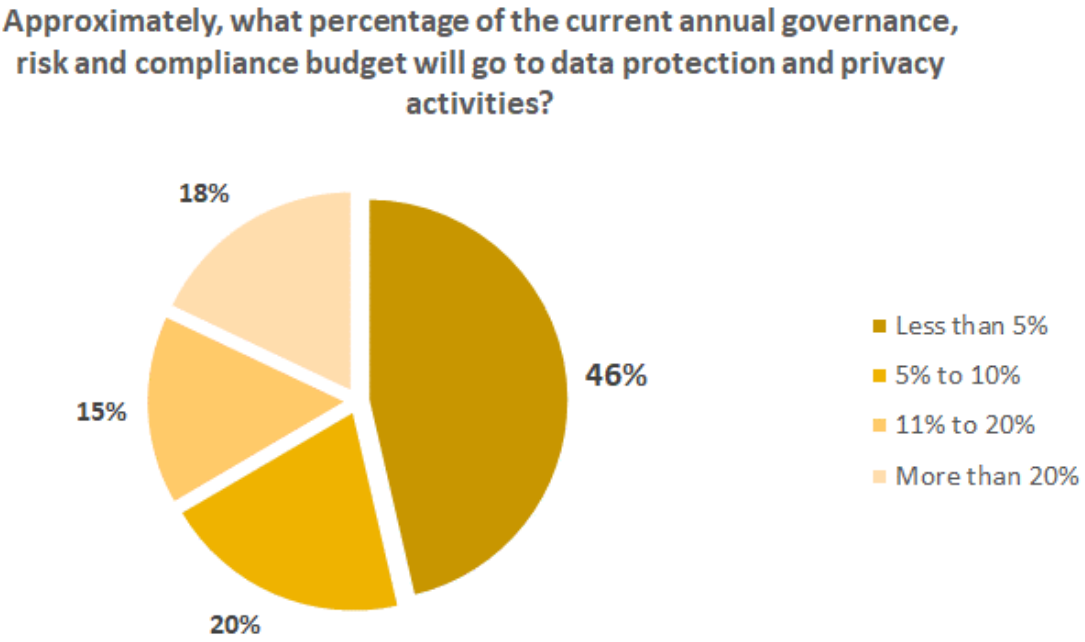
On the high end of the spending scale, 23% of enterprises with more than 10,000 worldwide employees spend more than $5 million annually on data protection and privacy activities. Only 13% of the very largest enterprises (those with 10,000+ employees) spend more than $10 million annually and only 10% spend more than $5 million on data protection and privacy activities.

Based on these figures, a total worldwide headcount of 5,000 employees appears to be the point when enterprises begin to significantly ramp up their spending on data privacy.



Spending relatively low compared to overall compliance budget

On a relative basis, the amount of spending on data protection and privacy also comprises a very small percentage of the current annual governance, risk and compliance budget. Almost half of all organizations (46%) allocate less than 5% of their annual governance, risk and compliance budget to data protection and privacy activities. Another 20% of organizations allocate between 5% to 10% of their annual governance, risk and compliance budgets to data protection and privacy activities. Thus, it is possible to make the statement that a majority of organizations (66%) allocate less than 10% of their annual governance, risk and compliance budgets to data privacy programs.



Of course, there are some organizations spending more than this benchmark 10% figure on data protection and privacy activities. For example, 15% of respondents in the survey said they allocate 11% to 20% of their annual governance, risk and compliance budget to data protection and privacy activities. And another 18% of organizations allocate more than 20% of their annual governance, risk and compliance budget to data protection and privacy activities.

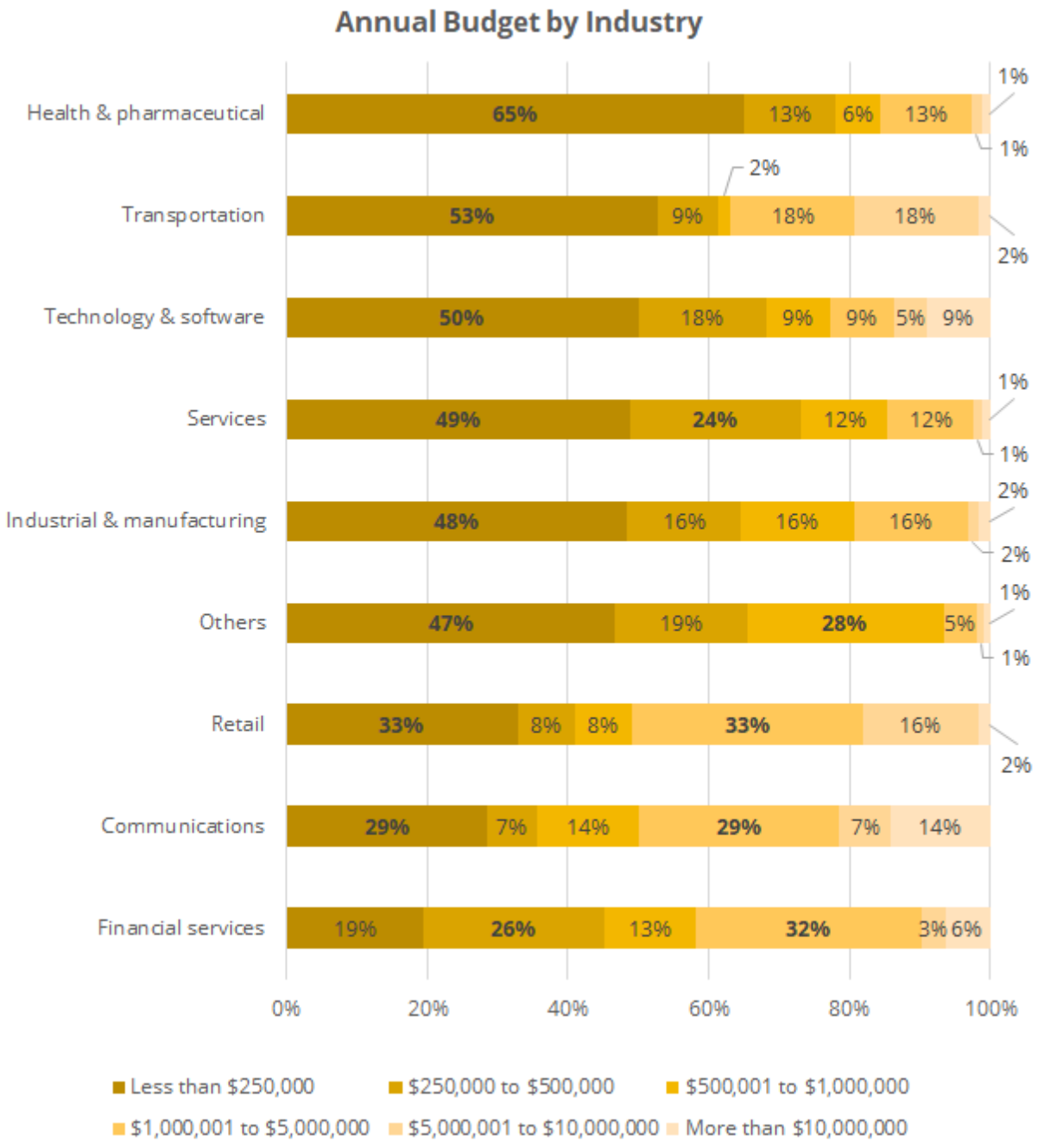
Given this variation in spending, it was worth exploring whether certain high-risk industries (such as financial services) might be allocating a greater proportion of their budgets to data privacy spending. After all, given the high visibility data breaches at financial services and healthcare companies, the expectation is that these companies are spending the most to keep their customers' data safe.

New Year Resolution

Educate executives of what facets make up a privacy program.

Manager
Entertainment & Media Company

In general, other than Financial Services, Communications and Retail, about half (47-65%) of all other enterprises spend less than $250,000 annually on data protection and privacy activities.

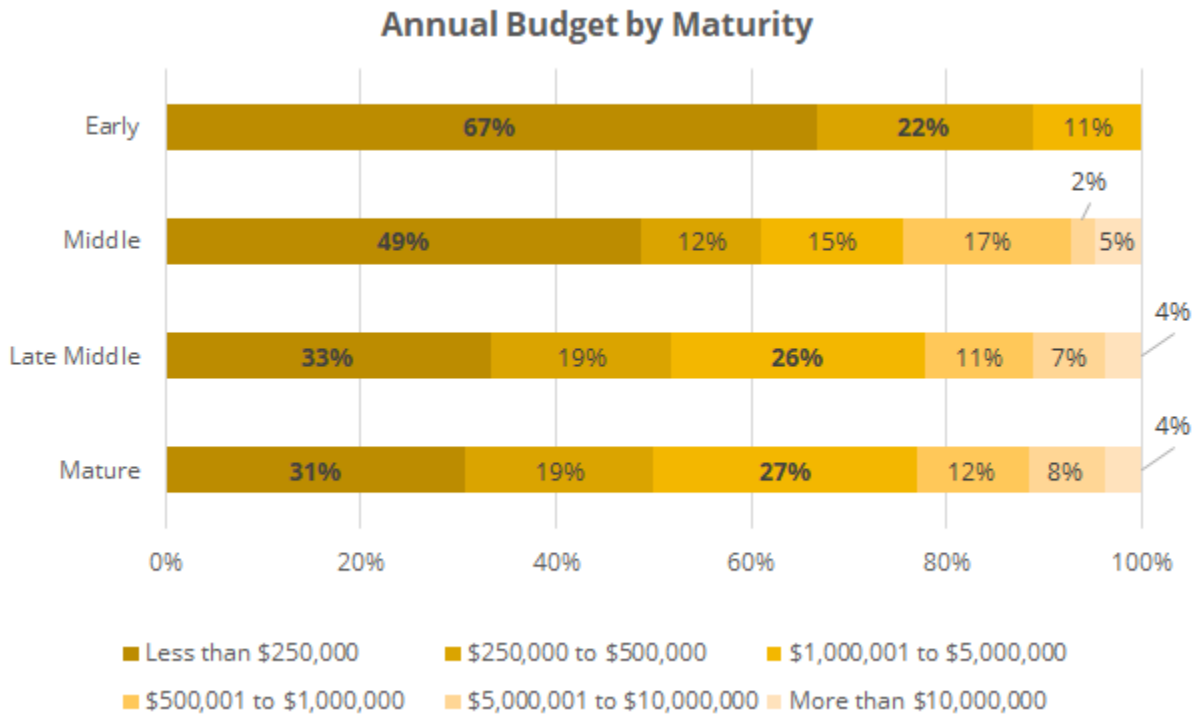


Interestingly, despite the sensitivity of personal data in the Health & Pharmaceutical industries, 65% of enterprises in the sector spend less than $250,000 annually on data protection and privacy activities.

Spending increases as program maturity increases

In order to calibrate the overall findings, survey responses were also analyzed according to the maturity of the data protection and privacy programs of the organizations. The expectation was that enterprises with Early stage privacy programs would be spending the lowest percentage of their budget on data protection and privacy activities, while enterprises with Late-middle or Mature stage programs would be spending the most.

As expected, as maturity increases, spending increases. Interestingly, about 90% (1 in 10) of enterprises with Early stage programs spend less than $500,000 annually on data protection and privacy activities. However, only 50% of organizations with mature stage data protection and privacy programs are spending less than $500,000 annually on data protection and privacy activities.



With maturity comes executive support and a more entrenched organizational privacy culture that values spending on data privacy. For that reason, some analysts have suggested that mature stage enterprises might be able to develop a competitive advantage over their rivals who have less developed privacy programs.

Key Finding 5

75% of enterprises have less than ten employees responsible for data protection and privacy

Approximately 1 of 4 enterprises have just one employee responsible for data protection and privacy

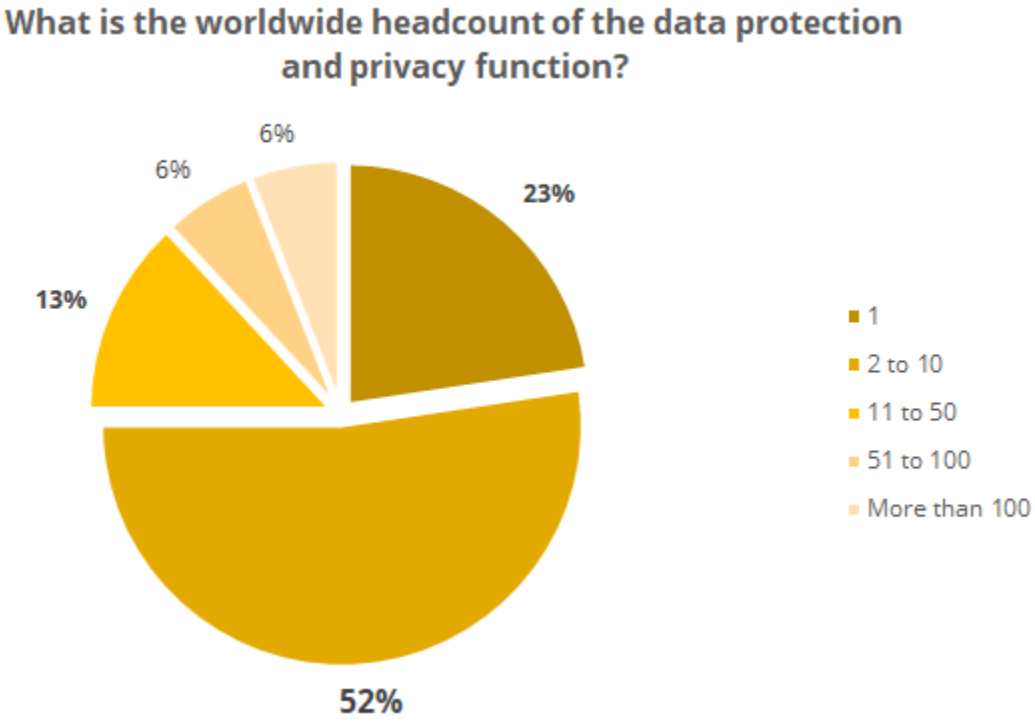
As organizations look to improve and expand their data protection and privacy programs, it only makes sense that they will be hiring more employees in specific functional roles. This is especially true for large, multinational corporations that must deal with a variety of legal jurisdictions and cross-border issues around the world. And yet, one surprising finding of this survey was that, even though organizations are more aware than ever of their data privacy responsibilities, they still have not started to staff up to meet those responsibilities.

In fact, nearly one in four (23%) of enterprises surveyed have just one employee in the data protection and privacy function. Even when accounting for enterprise size, it is striking how many organizations have only 1 employee responsible for data protection and privacy. For example, approximately 50% of organizations with less than 1,000 employees have a privacy function with only 1 employee. And even for organizations with as many as 5,000 employees, nearly one-quarter of them (23%) only have a single employee within this function.

New Year Resolution

Use privacy champions embedded in the business more effectively.

Director
Financial Services Company



Approximately 75% of enterprises have 10 or fewer employees in the data protection and privacy function. Moreover, even in the very largest organizations, the size of the data privacy team is likely to be very small. Approximately 40% of organizations with more than 5,000 employees have a privacy function with fewer than 10 employees.

Based on the results of the survey, the low headcount total does not appear to be by design, but rather, due to the challenge of obtaining sufficient budgetary or organizational resources.

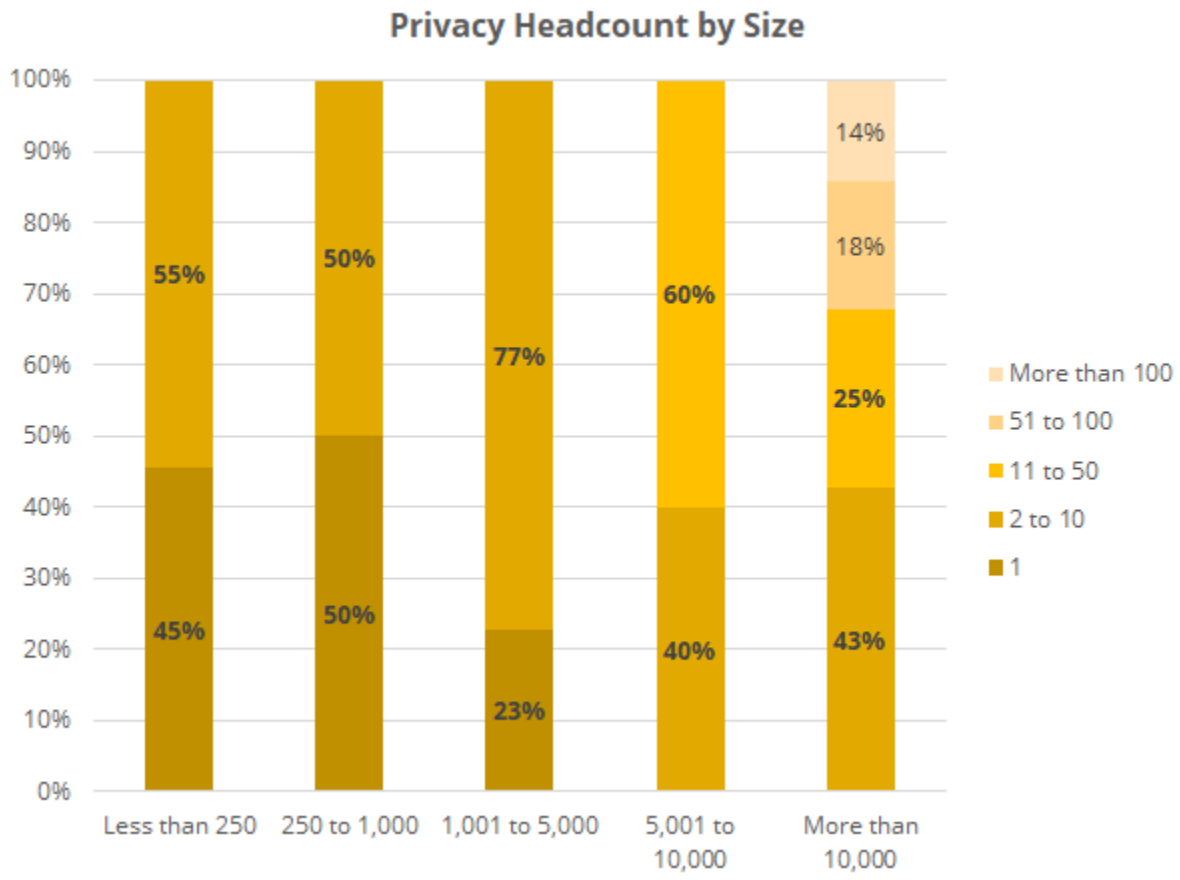
For example, just 13% of respondents said that hiring/retaining staff is a challenge. So if hiring more employees for the data protection and privacy function is not the issue, why aren't more organizations doing so? In the

New Year Resolution

To provide regular updates to the business to ensure that there is a general awareness of what the Data Protection Department are doing to achieve compliance.

Senior Executive/VP
Defense & Aerospace Company

post-GDPR era, requirements are more onerous and penalties are higher, so it's clear that budgetary and other resource constraints might pose a risk to organizations.



Conclusion and Recommendations

Many organizations could be doing much more to build and implement data protection and privacy programs.

On a worldwide basis, organizations are waking up to the realities of the post-GDPR world. In response to the challenges facing them, they are now tasked with prioritizing the appropriate responses. This includes serious thinking about how much of their annual risk and compliance budgets should be allocated to data protection and privacy measures, how many data privacy professionals should be specifically hired into a functional role, and what types of technological solutions they should be implementing in order to automate (or, at least, streamline) many of their data protection and privacy processes.

Based on the responses of 252 data privacy professionals worldwide, it is clear that many organizations could be doing much more to build and implement data privacy programs. For example, 45% of organizations are spending less than $250,000 annually on data protection and privacy and 23% of organizations have only a single employee within the data protection and privacy program. Considering that some of these organizations have more than 10,000 employees worldwide, it would appear that much more could still be done to build a world-class data privacy organization.

The good news is that there are several basic steps that all enterprises can take to improve the quality and effectiveness of their data protection and privacy programs that would not necessitate a radical increase in either spending or hiring:

- **Make the business case for data protection and privacy.** Data protection and privacy does not have to be a cost center for an organization – it can also be a source of competitive advantage. This would help to alleviate the two major challenges faced by organizations of all sizes – working with various business functions to integrate data protection and privacy programs, and obtaining sufficient resources and budget for new programs.

- **Whenever possible, choose data protection and privacy solutions that are scalable.** One major focus of this report was the shifting challenges and priorities of companies as their data protection and privacy programs migrate through different maturities. Companies still in the early stage of data privacy need to make sure that they are implementing programs that can scale with the overall growth and expansion of new business opportunities.

- **Empower employees to do more with less.** This is especially important for organizations hiring only a single employee to handle all data protection and privacy issues. For example, the report specifically points out opportunities for companies to implement technological solutions earlier, rather than later, during the launch and implementation of a data privacy program. This might reduce the burden on solo employees.

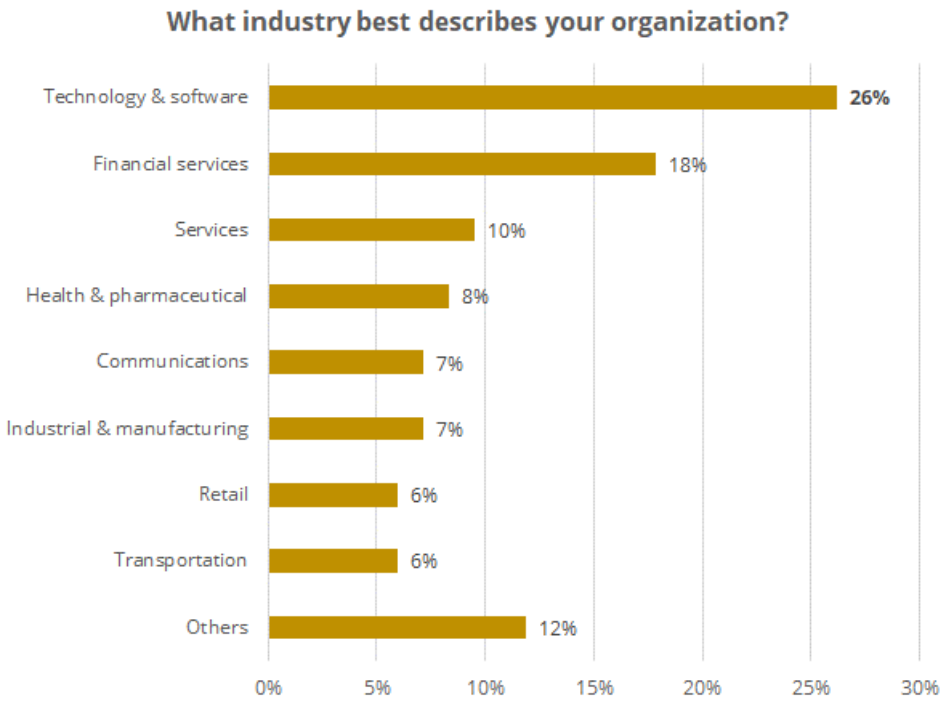
Obviously, there is still significant uncertainty in the post-GDPR landscape. Already, the first GDPR penalties have been made public, and the expectation that 2019 will likely see much more action on the legal and regulatory front. So are companies really doing enough to protect themselves from potential liability? Simply spending more money and hoping the problem goes away will not work. Instead, organizations need to create a privacy-aware culture that makes it easier to integrate privacy measures into every functional unit of the business. Moreover, new products and services should come with the expectation that they are conforming to the highest data privacy principles.

The hope is that this survey of data protection and privacy officers can point organizations in the right direction for addressing their own priorities and challenges, and give them some useful benchmarks for evaluating their own performance.

About the survey

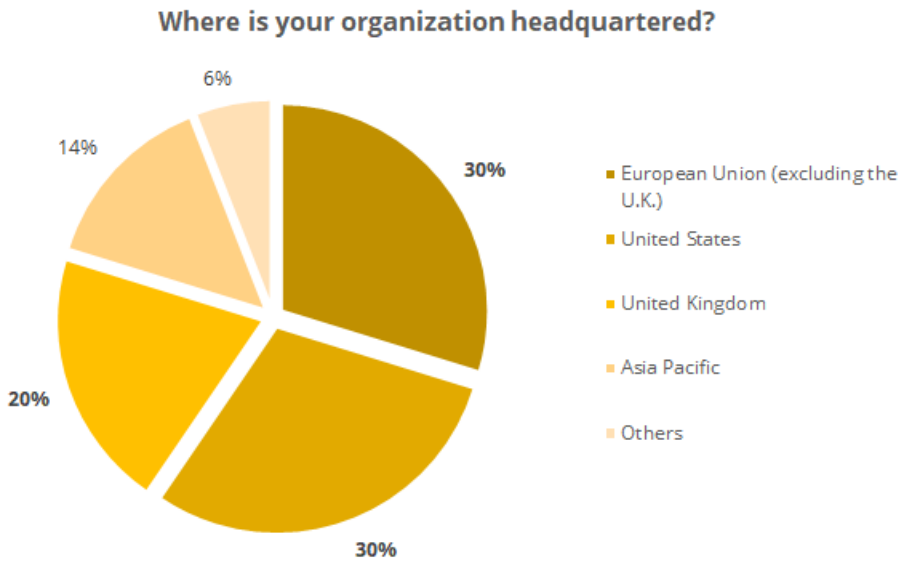
For this report, we invited professionals with data protection and privacy responsibilities in their organization to participate in a survey.

A total of 252 responses were collected and a total of 14 industries were represented. The largest sectors were Technology & Software and Financial Services.



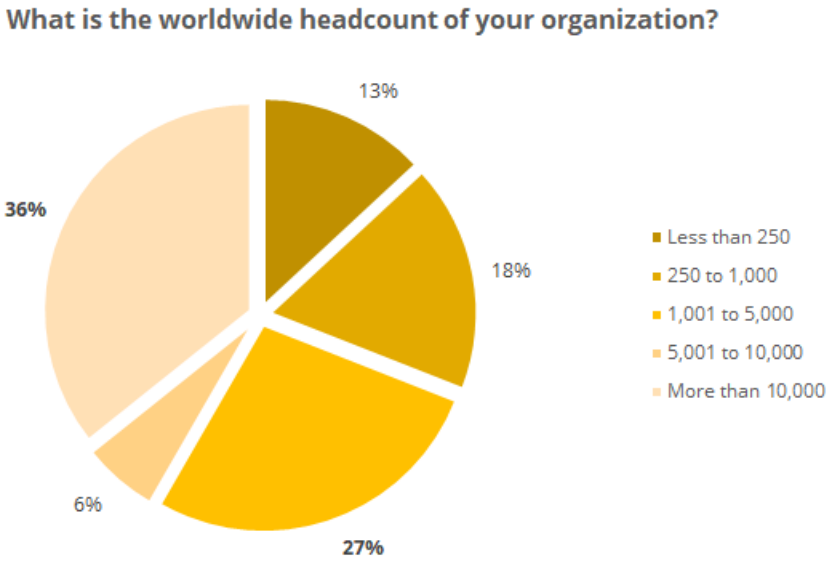
* *Others: Entertainment & media, Agriculture & food service, Consumer products, Education & research, Defense & aerospace*

Respondents are working in organizations headquartered around the world with 80% from the European Union, United States and United Kingdom.

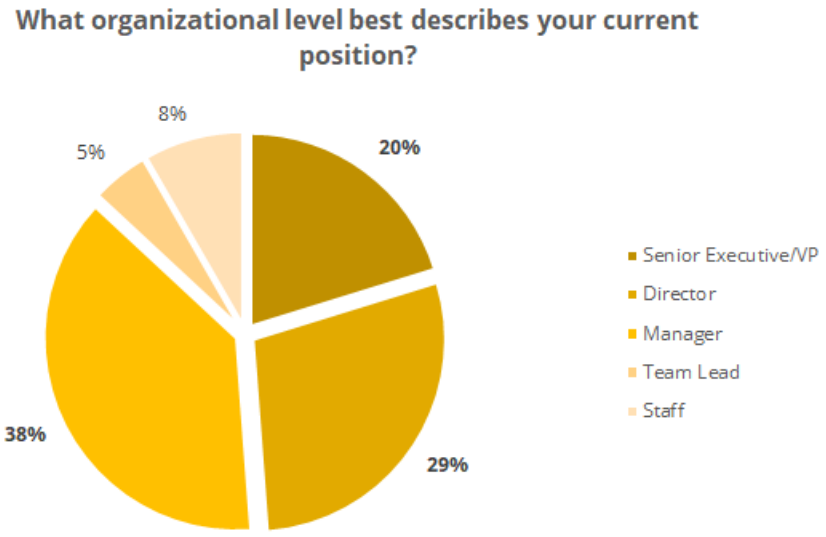


* *Others: Middle East, Africa, Canada*

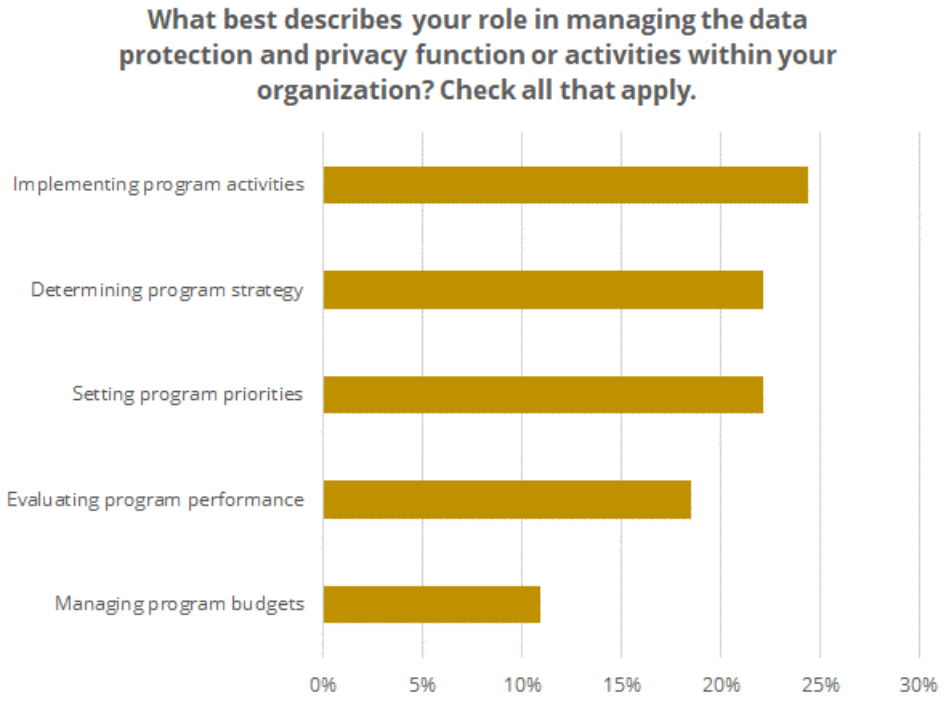
Respondents from organizations with more than 10,000 worldwide employees represented the largest segment. 69% of organizations in the survey have more than 1,000 employees.



The largest segment (38%) of respondents hold managerial positions. Almost half (49%) of respondents hold a position of Director or Senior Executive/VP.



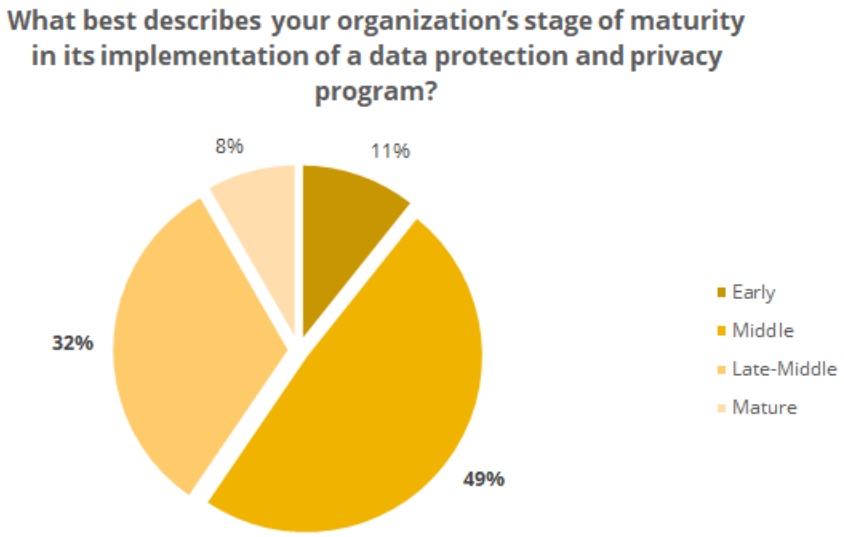
Respondents have responsibilities across all areas of a data protection and privacy program.



Respondents were asked to rate the maturity of their organization's data protection and privacy program:

- **Early stage** – Many program activities have not as yet been planned or implemented
- **Middle stage** – Program activities are planned and defined but only partially implemented
- **Late-middle stage** – Most program activities are implemented across the enterprise
- **Mature stage** – Program has successfully been implemented across the enterprise

The majority of organizations (81%) are in the Middle and Late-Middle stage. Only 11% were in the Early stage and 8% were in the Mature stage.



CPO
MAGAZINE

About CPO Magazine

We provide news, insights and resources to help data privacy, protection and cyber security leaders make sense of the evolving landscape to better protect their organizations and customers.

 enquiries@cpomagazine.com

 www.cpomagazine.com

Follow us:

 twitter.com/cpomagazine

 linkedin.com/company/cpomagazine

 facebook.com/cpomagazine