Preparing for the GDPR: DPOs, PIAs, and Data Mapping

iapp

TRUSTe

Preparing for the GDPR: DPOs, PIAs, and Data Mapping

Introduction

We know that organizations with mature privacy programs have internal privacy leadership and data management expertise, conduct privacy assessments for new and ongoing projects, and involve privacy in all facets of the product life cycle. These organizations are also more likely to conduct data inventory and mapping exercises. One-third of the members of the International Association of Privacy Professionals have reached this maturity stage with their programs.

So if a new regulatory regime codifies these practices, we should expect to see many organizations, especially those with privacy professionals on board, already well prepared for compliance.

With the General Data Protection Regulation coming online in the European Union by May 2018 — by its own terms affecting organizations worldwide that collect or process EU citizens' personal data — we have an opportunity to test how ready privacy professionals are for a contemporary and comprehensive privacy regulation that makes obligatory many of the last decade's "privacy-on-the-ground" practices.

The IAPP-TRUSTe 2016 study on privacy practices asked 244 privacy professionals about their organizations' progress toward GDPR compliance, such as whether they have a data protection officer, as well as questions about data hygiene habits like privacy assessments and data inventory and mapping exercises.

As this report demonstrates, organizations expecting to fall under the GDPR's jurisdiction are already preparing for and in many cases engaging in privacy practices codified in the GDPR. Regardless of geography or size, most organizations – 80 percent – believe they are going to need a DPO. More than 70 percent already regularly conduct privacy assessments, confirming the same finding from the IAPP-EY 2016 Privacy Governance Report. And although data inventory and mapping projects are not as common as privacy assessments, they are on the near horizon for many organizations as their privacy programs mature.

Despite mainstream media reports indicating lack of GDPR awareness, more than 90 percent of organizations with privacy professionals in place have begun preparations and many of them are well on their way toward implementing their GDPR compliance plans.

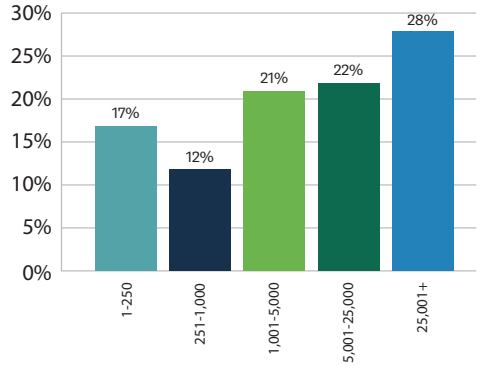
The IAPP-TRUSTe 2016 study on privacy practices asked 244 privacy professionals about their organizations' progress toward GDPR compliance.

Methodology

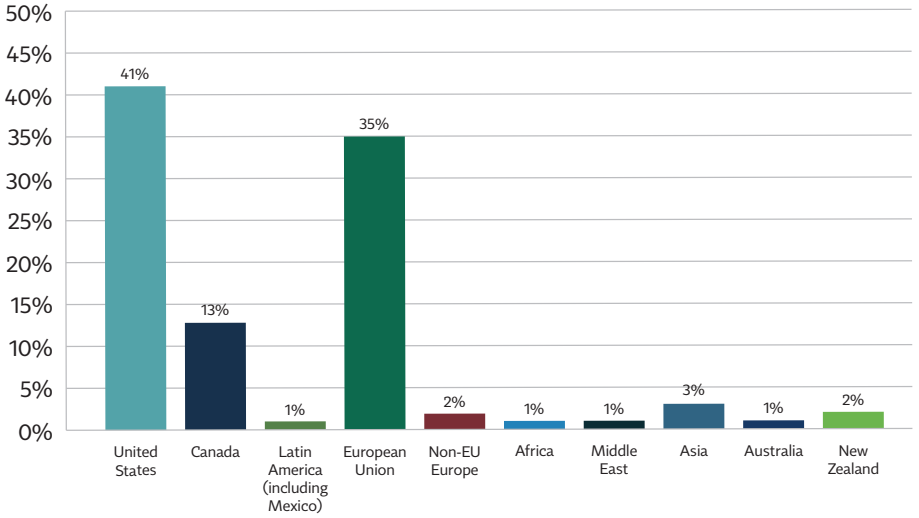
The IAPP emailed a survey to IAPP members and others who receive the IAPP's Daily Dashboard email newsletter, which provides privacy and data protection news. The 244 respondents who completed the entire survey primarily represent organizations in the United States (41 percent) and the European Union (35 percent), with respondents from Canada (13 percent) and other jurisdictions. Organizations of all sizes are also evenly represented in the survey with the largest organizations (more than 25,000 employees) submitting around 28 percent of the responses, companies with either 1,000-5,000 employees or 5001-25,000 employees each comprising roughly 20 percent, and companies under 1,000 sharing the remaining responses.

Respondents reflect a wide variety of industries as well, including around 13 percent from software and services, 12 percent from government offices, and 9 percent working in health care.

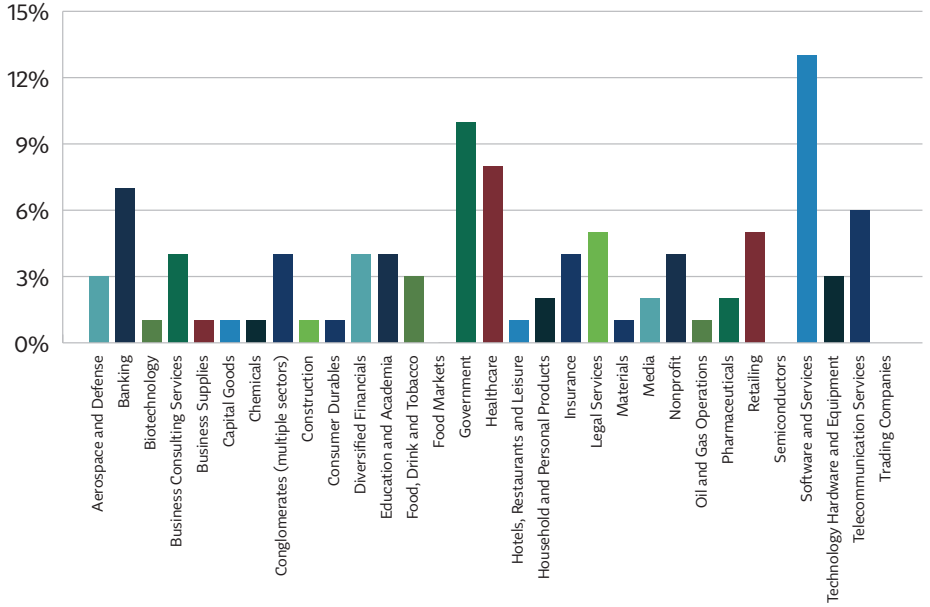
How many people are employed where you work?



What is the primary location of your employer's headquarters?



In what industry do you work?

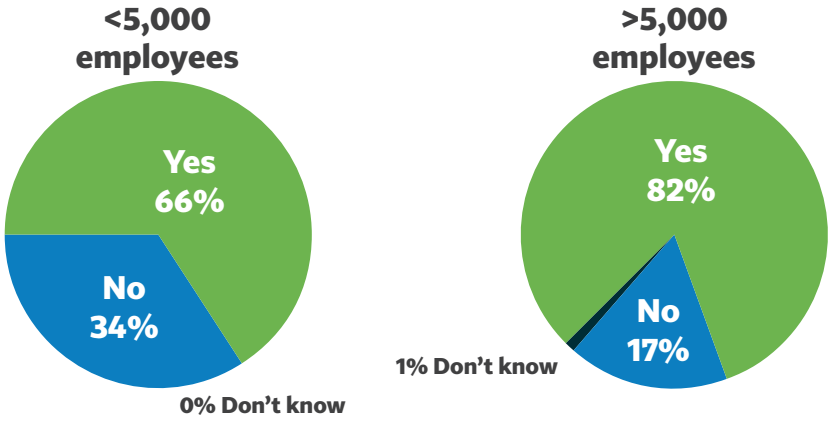


Organizations busily preparing for the GDPR

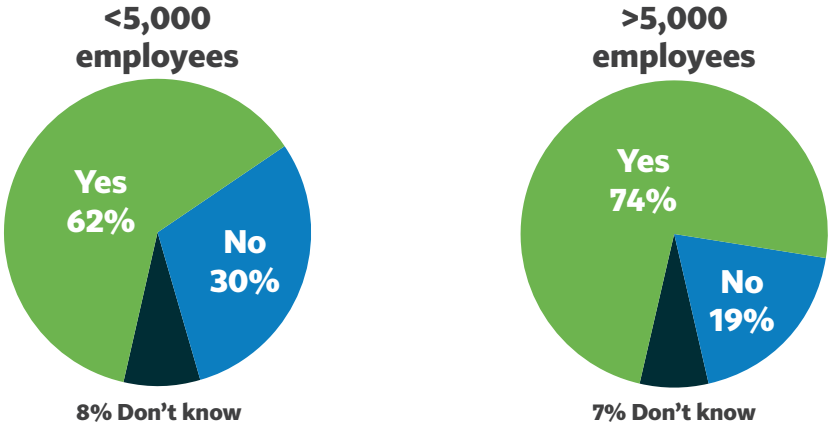
More than 73 percent of respondents have customers or employees in the European Union. Slightly fewer – around 68 percent – acknowledge their organization will have to comply with the GDPR, but 8 percent admit they do not know. Not surprisingly, larger organizations – those with more than 5,000 employees – are 16 percent more likely than smaller companies (<5,000 employees) to have employees or customers in the EU, and 11 percent more likely to fall under the scope of the GDPR.

One out of four organizations responding to our survey does not anticipate needing to comply with the GDPR. Those respondents, along with those who answered "do not know," were not asked to answer any additional questions about the GDPR. Notably, a vast majority of the Canadian respondents – more than 80 percent – say either the GDPR doesn't apply to their organization or they aren't sure.

Does the organization you work for have customers and/or employees in the European Union?



Does your organization fall under the scope of the General Data Protection Regulation?



While there have been some reports in the mainstream media that organizations in large part lack awareness of the GDPR, among the organizations surveyed here that anticipate GDPR compliance by May 2018, nearly 43 percent already have a preliminary plan in place. Approximately 36 percent not only have a plan but have already begun implementation, while another 13 percent are well into implementing their GDPR compliance plan.

In total, a full 92 percent of respondents have at least begun preparations for GDPR compliance.

Not surprisingly, EU-based respondents are more likely to report they have begun to implement their GDPR plans (43 percent), and one in five is well into implementation. Thirty-one percent of EU organizations report having only a preliminary plan.

Their U.S.-based counterparts are slightly behind, with a full 54 percent of U.S. organizations at the preliminary plan stage, and 32 percent part of the way into implementing their plan. Only a tiny number of U.S. organizations – almost too small to be statistically relevant – report they are well underway.

In total, these numbers should prove encouraging to data protection authorities. Before the one-year anniversary of the GDPR's first publication, and over 18 months before it takes effect, privacy professionals are taking it seriously and building toward compliance. As if the GDPR were a hurricane, building offshore and with plenty of warning before landfall, organizations of all sizes and geographic locations are not sitting idly by but instead are busy making preparations.

Which of the following best describes your organization's preparation for the GDPR?

	US-only	EU-only
What is the GDPR?	2%	2%
We have a preliminary plan.	**54%**	31%
We have a plan and have begun implementation.	32%	**43%**
We have a plan and are well into implementing it.	4%	20%
We are fully compliant already.	4%	4%
Don't know.	4%	0%

Adding a Data Protection Officer

One GDPR requirement organizations are already anticipating is the mandatory Data Protection Officer appointment. This obligation, set out in Article 37, applies to public authorities and to companies whose "core activities" involve "regular and systematic monitoring of data subjects on a large scale." Without guidance yet on how broadly authorities will interpret this requirement (expected to arrive in December), organizations of all sizes are likely uncertain whether the DPO requirement applies.

The GDPR allows organizations to share a DPO amongst subsidiaries or associated business units, and even permits them to outsource the role. We therefore asked survey respondents whether the DPO requirement even applies to their organization, and if so what their plans are to appoint from within, hire someone new, or outsource the position.

Fewer than 10 percent of respondents who fall under the scope of the GDPR generally believe the DPO requirement does not apply to their organization; approximately 13 percent said they did not know. This means roughly 80 percent of survey respondents interpret the GDPR as requiring their organization to appoint a DPO. Very few organizations, at least currently, plan to outsource the DPO responsibilities.

The IAPP has estimated – based largely on company size – that as many as *75,000 DPOs may need to be appointed globally* in response to the GDPR.

With regard to the GDPR's requirement that certain organizations appoint a Data Protection Officer (DPO), which of the following best describes your organization?

This requirement does not apply to us.	10%
We already have a DPO.	**46%**
We do not have a DPO but we will be appointing someone internally to fill the role.	22%
We intend to hire a new employee to serve as our DPO.	3%
We intend to outsource the DPO role.	4%
One of our affiliates has a DPO that we will share.	2%
Don't know.	13%

Perhaps the GDPR readiness should not be surprising from this group: Forty-six percent of those who think they'll need a DPO already have that person in place. Privacy professionals are already operating in these organizations and accomplishing many of the responsibilities the GDPR requires of the DPO.

Another 22 percent plan to make an internal appointment to fill the position, which may mean a senior privacy professional has decided the role is not for her, while a very small number will hire a new person, outsource, or even share the DPO position with a sister organization.

Smaller companies (those with fewer than 5,000 employees) are more likely than larger companies (16 percent vs. 4 percent) to duck the DPO obligation all together, but among small and large companies approximately the same number – 80 percent – plan to have, or already have, a DPO. Where they differ is in current versus future appointments. Larger companies are more likely (52 percent vs. 38 percent) to have already appointed a DPO, while the smaller companies still have to find and train up an internal employee to fill the DPO role (19 percent), or outsource the job.

The same holds true comparing EU respondents to U.S. organizations. Among those EU companies obliged to appoint a DPO, 55 percent already have one while only 35 percent of U.S. companies already have a DPO, and 25 percent of U.S. companies have yet to appoint someone internally. U.S. companies are also 10 percent more likely (18 percent vs. 8 percent) to be unsure whether the DPO requirement even applies.

With regard to the GDPR's requirement that certain organizations appoint a Data Protection Officer (DPO), which of the following best describes your organization?

	U.S.	EU	<5,000	>5,000
This requirement does not apply to us.	9%	10%	16%	4%
We already have a DPO.	**35%**	**55%**	**38%**	**52%**
We do not have a DPO but we will be appointing someone internally to fill the role.	25%	19%	26%	19%
We intend to hire a new employee to serve as our DPO.	5%	2%	0%	6%
We intend to outsource the DPO role.	5%	4%	5%	2%
One of our affiliates has a DPO that we will share.	3%	2%	4%	1%
Don't know	18%	8%	11%	16%

The DPO role

Four in 10 organizations that already have identified a DPO have the privacy leader or CPO serving that role; this holds true for both U.S. and EU organizations. Around 20 percent report that someone other than the privacy leader, but still within the privacy department, has been trained to be the DPO, while another 7 percent have recruited internally from outside the privacy team. A handful of organizations – 16 percent – have more than one person performing DPO duties, and another 12 percent have a DPO in each EU Member State where they collect personal data.

In other words, while some organizations are asking their strategic privacy leader to hold the DPO role, just as many are giving the DPO tasks to someone other than the CPO or privacy lead.

When we ask about DPO reporting structures, the findings are consistent. Those DPOs who are privacy leaders or CPOs (46 percent) tend to report to a position higher on the corporate ladder, while the others report either to the privacy lead (36 percent), someone with equivalent status as the privacy lead (7 percent), or even to a position below the privacy lead (11 percent).

Four in 10 organizations that already have a DPO appointed have the privacy leader or CPO serving that role.

THOSE WITH DPO IN PLACE

With regard to the DPO position, which of the following is true?

Our privacy leader is our DPO.	**42%**
Someone in our privacy department (other than the privacy leader) is our DPO.	21%
We have trained someone who was not already filling a privacy function to serve as our DPO.	7%
We have more than one person serving in a DPO role.	16%
We have a DPO in each EU Member State where we have an office or collect personal data.	12%
Don't know.	3%

Your organization's DPO reports to:

The Chief Privacy Officer/privacy leader	36%
A position higher up the corporate ladder from the CPO/privacy leader.	**46%**
A position on the same organizational level with the CPO/privacy leader.	7%
A position lower on the organizational ladder from the Chief Privacy Officer/ privacy leader.	11%

THOSE WHO INTEND TO APPOINT A DPO

With regard to the DPO position, which of the following is true?

The Chief Privacy Officer/privacy leader will be the DPO.	**41%**
Someone in our privacy department other than the CPO/privacy leader will be the DPO.	16%
We will train someone who is not already serving a privacy function to be the DPO.	14%
We will have more than one person serving in the DPO role.	11%
We will have a DPO in each EU Member State where we have an office or collect personal data.	5%
Don't know.	13%

Your organization's DPO will likely report to:

The Chief Privacy Officer/privacy leader.	21%
A position higher up the organizational ladder from the Chief Privacy Officer/privacy leader.	**33%**
A position on the same organizational level as the Chief Privacy Officer/privacy leader.	10%
A position lower on the organizational ladder from the Chief Privacy Officer/privacy leader.	7%
Don't know.	29%

For those organizations that do not have a DPO but are planning to appoint someone internally, 40 percent of them, too, expect their privacy leader to be the DPO, while 46 percent are planning to train up someone from the privacy department or elsewhere in the organization. Understandably, companies that have yet to make the appointment are somewhat less certain about reporting structures.

Amid much speculation around whether or not DPOs will be hired or appointed at all, and to what extent they will hold leadership positions, this study suggests that organizations are certainly planning to err on the side of having someone hold the DPO title and role. That person is just as likely to be the privacy leader as a lower position within the company, and the DPO is far more likely to be an internal appointment than a new hire.

Almost no organizations surveyed are expecting to outsource the role.

Still, if one out of five organizations has yet to appoint the DPO, many new in-house privacy professional positions stand to be created across the globe. For CPOs as well as privacy professionals interested in more duties and career growth, the DPO role presents a new opportunity and challenge.

Privacy assessments

Motivations

Among privacy professionals' primary duties is conducting data protection impact assessments or privacy impact assessments. Seventy-one percent of survey respondents report their organizations conduct DPIAs or PIAs. This number is precisely consistent with the numbers reported in the annual IAPP-EY Privacy Governance Report.

Larger organizations report a 78 percent likelihood of conducting privacy assessments, while just 64 percent of smaller organizations (fewer than 5,000 employees) tend to do them. This correlates strongly with findings in governance surveys that show large companies are more likely to have mature privacy programs.

Of the 25 percent of respondents who do not conduct regular privacy assessments, the primary reason given was lack of time or bandwidth, followed closely by lack of internal support from leadership. Other reasons include lacking the right tools or inadequate budget. Some respondents suggest that their assessments are informal, or that they are just beginning to implement more structured privacy assessment processes.

Which of the following are barriers to completing privacy assessments (select all that apply)?

We don't have enough time/bandwidth	**56%**
We lack internal support from leadership or other departments.	49%
We lack the right tools.	37%
We don't have the budget.	34%
We don't have the training or knowledge.	29%
We don't see the need or value	12%
Other (please elaborate):	20%

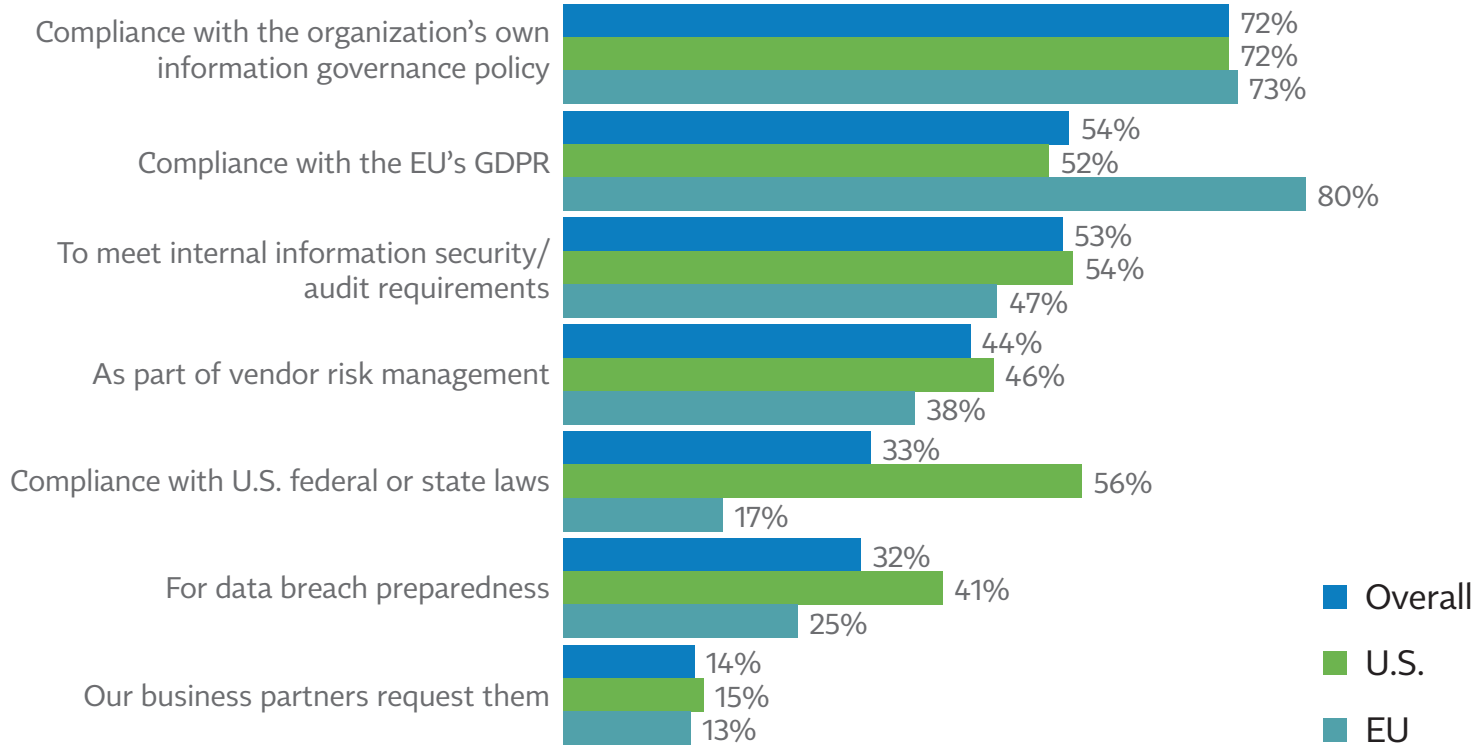
Some of the reasons given for not conducting privacy assessments include:

- **"We don't have a process in place to enforce this but are producing one in time for the GDPR implementation."**
- **"No need at this time, but 2017 may be a different matter."**
- **"There are no internal barriers, it has just not been something that has been a focus in the U.K. before."**

Although legal compliance certainly motivates organizations to conduct privacy assessments, it is not the only motivator. Overall, the number one motivation for privacy assessments among survey respondents was far and away internal information policy compliance, cited by seven out of 10 respondents who conduct such assessments. This number is consistent among both U.S.- and EU-based organizations.

Perhaps because Article 35 of the GDPR expressly requires DPIAs, 80 percent of EU organizations cite GDPR compliance as their top reason for conducting them. Nonetheless, privacy assessment activity takes place even without regulatory mandates. Among the 60 organizations that report the GDPR will not even apply to them, 78 percent (more than the overall average) conduct privacy assessments anyway. This is a classic example of "privacy on the ground" at work.

Which of the following, if any, describe your organization's motivations for conducting privacy assessments (select all that apply)?



Canadian respondents selected "other" often (52 percent) when outlining why they conduct privacy assessments. Among the illustrative explanations for privacy assessment motivations were the following comments: "Currently conducted for Canadian operations because of PIPEDA. Have conducted U.S. and starting EU PIAs using similar Canadian methodologies"; and, "We have only just started to implement PIAs as a result of the number of projects/initiatives starting within the organization seeking Data Protection Authority compliance advice but also in preparation for the GDPR."

Mechanics

Privacy professionals, having toiled for years with less than adequate budgets, are resourceful. So while some of them (17 percent) conduct privacy assessment using governance, risk management and compliance tools, and a handful (6 percent) use specifically-designed privacy assessments software, the vast majority (66 percent) rely upon manual or informal processes that might include email, spreadsheets, and other bootstrapping means. While more than a third have built their own internal systems for privacy assessments, the recent influx of vendors offering software tools will likely lower that percentage in the future.

What tools do you use to conduct or record the results of your privacy assessments (select all that apply)?

	Overall	<5,000	>5,000
We do it manually/informally with email, spreadsheets, and in-person communication.	**66%**	**72%**	**62%**
We use a system developed internally.	36%	32%	40%
We use governance, risk management and compliance (GRC) software that we customize for privacy assessments.	17%	10%	22%
We outsource our assessments to external consultants/ law firms.	7%	12%	3%
We use a commercial software tool designed specifically for privacy assessments.	6%	9%	4%
Don't know.	1%	1%	0%

Regardless, these organizations are doing a lot of privacy assessments.

Most organizations (60 percent) conduct privacy assessments at the project or product launch stage, or when a project or product changes (53 percent). The next most common points are at the idea stage (46 percent), with almost half saying they're conducting these assessments an ongoing basis for projects or products collecting PII (45 percent). Few organizations (only 15 percent) conduct these assessments on a regular or ongoing basis for all projects or products.

Regarding frequency, there is no rule of thumb. One out of five organizations conducts privacy assessments between three and 10 times per year, while another one out of five conducts them between 11 and 50 times annually. After that, privacy assessment frequency ranges from 51-100 times per year (15 percent) to 101-500 times per year (14 percent) to as few as one or two times (12 percent) per year. When we filter by organization size, we find that larger organizations (more than 5,000 employees) in general conduct privacy assessments with more frequency than smaller ones and indeed are almost 10 percent more likely than the overall population to conduct privacy assessments between 101 and 500 times per year.

All of which conforms with common sense. Larger organizations have more products, which need more assessments as they launch.

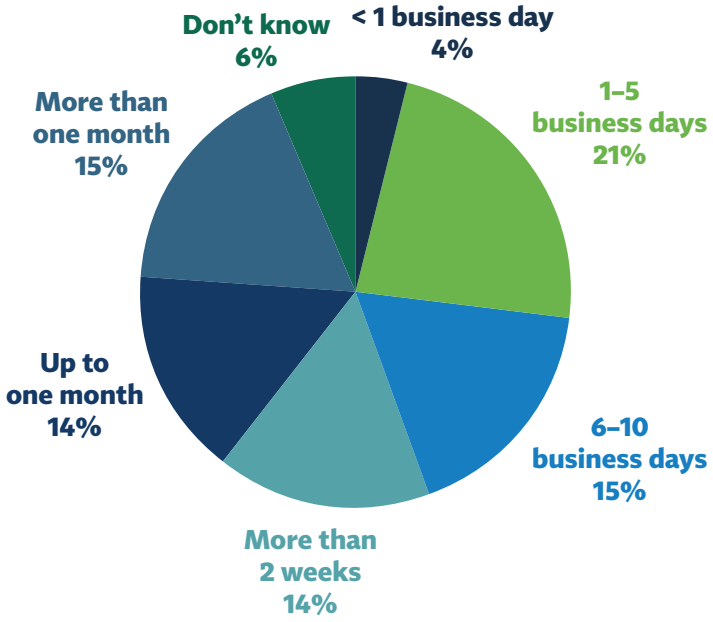
Approximately how many privacy assessments (including DPIAs, PIAs, etc.) does your organization conduct annually?

	Overall	<5,000	>5,000
1-2	12%	22%	3%
3-10	**22%**	**27%**	18%
11-50	21%	26%	18%
51-100	15%	13%	17%
101-500	14%	3%	**23%**
501-1,000	2%	1%	2%
1,001+	3%	0%	5%
Don't know	12%	1%	14%

Why are software vendors beginning to offer privacy assessment tools? Survey findings of "don't have enough time/bandwidth" as the leading barrier to PIAs and "we do it manually/informally" as leading method of conducting PIAs would indicate demand for automation tools.

How long does it typically take your privacy assessment to be completed?

<1 business day	4%
1-5 business days	**21%**
6-10 business days	15%
More than 2 weeks	14%
Up to one month	14%
More than one month	15%
Don't know	6%



The most common duration for a privacy assessment is within one week, as 20 percent of respondents – both in the US and the EU – report taking between one and five business days to conduct an assessment. Beyond that, once again assessment times vary widely from up to two weeks, to more than a month, and durations in between. Larger organizations tend to take longest, probably because of the number of staff involved; organizations with more than 5,000 employees are more likely to take up to two weeks (instead of one) to complete privacy assessments.

In general, of course, how long an organization takes to complete a privacy assessment depends on the assessed project as well as the assessment process. Here are some sample responses:

"There is a lot of 'it depends.' If the PIA is being done in conjunction with procurement then the PIA term mirrors the procurement process term, plus the implementation phase."

"While it takes one or two business days to finalize a privacy assessment, the privacy assessment is only the first step in the privacy review process. Additional activity may occur as what's been assessed/reviewed is being implemented or operationalized."

"Delays are typically due to obtaining required details from subject matter experts. PIAs are not 'priority' operational work."

"Only just started to conduct PIAs and procured a PIA toolkit from our solicitors which includes an Addendum for compliance with articles in GDPR. Currently undertaking our first PIA."

Less risky projects might permit a limited self-assessment that can be completed in a day, while higher-risk projects may involve higher-level sign-off, or start with a project lead and require privacy or legal department final approval.

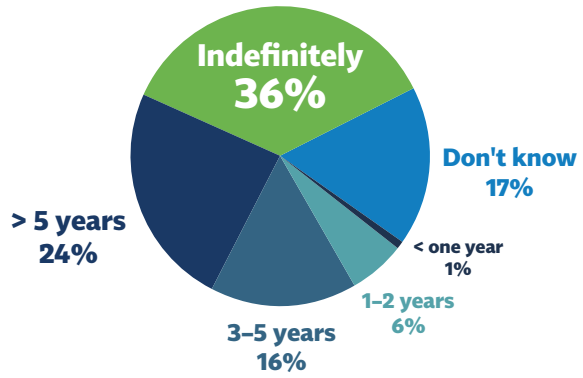
Not surprisingly, nearly nine out of 10 organizations involve the Privacy department in privacy assessments. The next most commonly consulted team is Information Security/Cybersecurity (68 percent) followed closely by the Legal department (66 percent). Information Technology departments are involved slightly more than half of the time, while Compliance departments get included in fewer than half of all privacy assessment exercises.

For now, the Data Protection Officer role is asked only about one-third of the time to weigh in on privacy assessment exercises. This is likely to increase as organizations add a DPO position. Indeed, Article 38(1) of the GDPR requires controllers and processors to "ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data."

Which of the following departments are involved or consulted in your organization's privacy assessments (select all that apply)?

Privacy	**87%**
Information Security/Cybersecurity	68%
Legal	66%
IT	57%
Compliance	42%
DPO	36%
Product Development/Engineering	25%
Human Resources	22%
Marketing	16%
External Law Firm	10%
C-Suite/Management	9%
Regulators	6%
R&D	6%

HOW LONG DO YOU MAINTAIN RECORDS OF PRIVACY ASSESSMENTS?



If anyone is looking for an old privacy assessment, chances are good it is still on hand. One out of three organizations maintains privacy assessment records indefinitely, while one in four keeps them for more than five years. Everyone else is as likely to keep them for fewer than five years as they are to have no idea how long such records are maintained.

Data inventory and mapping

Motivations

Organizations are more equipped to manage personal data if they know what they are collecting, where it is stored, who shares it, and how long it is retained. Data inventory and mapping exercises are common in both privacy and security functions, but how common?

According to our study, fewer organizations engage in routine data inventory and mapping for privacy management purposes – only 43 percent of the overall respondents – than conduct regular privacy assessments. This is also consistent with findings from the annual Privacy Governance Report.

Just over 30 percent, however, say they plan to begin within the next 12 months, for some a nod to GDPR compliance but for others just the logical next step in a maturing privacy program. Indeed, 40 percent of those companies who do not need to comply with the GDPR already conduct data mapping and inventory exercises and 23 percent (with admittedly a small sample size) intend to get started on them soon. One out of five companies overall does not do them or plan to, and this number rises to 30 percent when the GDPR is not a factor.

For those one in four respondents who eschew data inventory and mapping now and for the foreseeable future, the most likely reason is lack of internal resources or staff, followed by its low status on the organization's priority list.

EU (47 percent) and U.S. (46 percent) organizations are directionally more likely than the average organization to conduct data inventory regularly, and these numbers are consistent across company size. So what is pulling down the overall numbers? Canadian organizations, of which only 25 percent (directionally, given the small sample size of 32 total) conduct data inventory and mapping, while over 50 percent do not and have no plans to start. Governmental organizations are also disproportionately represented (20 percent) among those who do not perform data inventory and mapping.

Which of the following are barriers to completing a data inventory/ mapping project for privacy purposes (select all that apply)?

Lack of internal resources/staff	**58%**
It's a low priority for the organization	48%
Too busy; focused on other projects	32%
These projects are done by others (e.g. IT/security)	30%
Lack budget for external consultants or suppliers	30%
It cannot be maintained so no reason to start	12%
Don't know	10%

Mechanics and Participation

With the same resourcefulness used for privacy assessments, privacy professionals engaged in data inventory and mapping generally construct their own forms and processes from whatever they have on hand. Given a menu of options from which they can select multiple answers, 62 percent of respondents who conduct data inventories say they do them manually using email, spreadsheets and the like, while 36 percent may use an internally-developed system. Only 12 percent report using a GRC software system and even fewer (10 percent) use a commercial product developed exclusively for the inventory and mapping tasks.

The Privacy department (74 percent) and the IT department (70 percent) are the most active participants in data inventory and mapping projects. Both departments play a greater role than Information Security (62 percent) or Legal (41 percent), which are much more engaged in privacy impact assessments. The Compliance department is involved for only one out of three organizations. This logically suggests that the inventory and mapping process is a precursor to risk and regulatory compliance analysis, and thus is much more likely to involve departments that gather and handle data in the first instance, and much less likely to involve departments responsible for assessing organizational risks of data use – Privacy department excluded, of course.

What tools do you use to perform data inventory and mapping (select all that apply)?

	Overall	<5,000	>5,000
We do it manually/informally with email, spreadsheets, and in-person communication.	**62%**	**70%**	**53%**
We use a system developed internally.	36%	30%	43%
We use governance, risk management and compliance (GRC) software that we customize for our inventory/mapping purposes.	12%	9%	16%
We use a commercial software tool designed specifically for data inventory/mapping.	10%	9%	12%
We outsource our data inventory/mapping to external consultants/law firms.	8%	9%	6%
Don't know	2%	2%	2%

When we look only at EU organizations that conduct mapping and inventory, we find the IT department slightly more likely than Privacy to be involved. Notably, the DPO role is greatly enhanced relative to organizations in other geographic regions (48 percent likely in the EU vs. 27 percent overall). Because the DPO has a longer history in the EU than elsewhere, perhaps this trend may be followed by GDPR-complying organizations globally.

Which of the following departments are involved in data inventory and mapping projects?

	Overall	EU Only
Privacy	**74%**	68%
IT	70%	**73%**
InfoSecurity/Cybersecurity	62%	58%
Legal	41%	35%
Compliance	33%	38%
Human Resources	30%	30%
Data Protection Officer	27%	**48%**
Marketing	15%	20%
Product Dev/Engineering	12%	13%
C-Suite/Management	7%	8%
External Law Firm	5%	0%
Research and Development	3%	0%
Regulators	3%	5%

Process and Funding

Respondents report having very recently completed data mapping or inventory projects: Over 50 percent say they last did one within the previous six months, while 18 percent have completed one within the past year. These numbers hold firm regardless of the organization's geography or number of employees.

Once created, data inventory and mapping projects are much more likely to be reviewed regularly by the privacy team (50 percent of the time) or reviewed on an ad hoc basis (25 percent) than to be maintained automatically (4 percent) or by an external source (4 percent), or even neglected altogether (9 percent). Organizations in the EU are the most fastidious; 70 percent of EU respondents report regularly reviewing their inventory and mapping work. In the U.S., meanwhile, only 35 percent of organizations regularly maintain their data inventory/mapping projects, although 17 percent of U.S. respondents simply didn't know. Larger companies are directionally more likely than smaller ones to engage in routine updating.

Overall, Privacy team budgets are not tapped for the bulk of data inventory or mapping projects. Instead, they tend to be funded jointly by many departments (including Privacy, IT, Security or Compliance) (25 percent), or from departments other than Privacy (24 percent). The Privacy budget is tapped by fewer than 20 percent of the organizations who conduct inventory and mapping.

Overall, Privacy team budgets are not tapped for the bulk of data inventory or mapping projects. Instead, they tend to be funded jointly by many departments.

U.S. organizations tend to charge inventory and mapping projects to either the Privacy team (24 percent) or another individual department (33 percent), rather than ask the departments to share the cost (17 percent). Nearly four in 10 EU-based organizations, however, require multiple departments to chip in, while only 13 percent look to just one department.

Across the board, we should note, many respondents simply do not know how such projects are funded.

How do you maintain your data inventory/mapping projects?

	Overall	US Only	EU Only	<5,000	>5,000
Reviewed regularly by the privacy team	**49%**	**35%**	**70%**	**43%**	**55%**
Reviewed on an ad hoc basis	25%	26%	15%	29%	20%
We use external consultants to keep up to date	4%	4%	3%	4%	4%
It's not been updated since first produced	9%	9%	8%	11%	6%
We use an automated tool to maintain the data inventory	4%	9%	0%	2%	6%
Don't know.	10%	17%	5%	13%	8%

How are your data mapping/inventory projects usually funded?

	Overall	US Only	EU Only	<5,000	>5,000
From the privacy budget	19%	24%	13%	16%	22%
From the IT, security, or compliance budget	24%	**33%**	13%	20%	**29%**
It's jointly funded by privacy and the IT, security, or compliance budgets	**25%**	17%	**38%**	**29%**	20%
Don't know.	18%	20%	20%	20%	16%
Other (please describe):	14%	7%	18%	16%	12%

Conclusion

Over the past decade, as the privacy profession has grown and matured, organizations have devoted more resources to privacy staff and privacy-related tasks. Multiple departments outside the core privacy team have privacy responsibilities and even budget obligations. So when the EU's GDPR takes effect in mid 2018, many organizations will already be complying with its most routine operational requirements.

The next 18 months should see increases in privacy assessments, data mapping and inventory activities, as well as new internal appointments and hiring for the DPO role. The DPO, in turn, will likely work closely with multiple departments on a variety of projects including data inventory and mapping, as well as privacy assessments.

What's also clear is that the DPO job description will have to include "bootstrapping" and "resourcefulness" as core skills.

Even so, as these DPOs strive for compliance, it seems clear they need increased staffing and better tools if they are to be successful in implementing their plans. The coming of the GDPR in May 2018 will not take many organizations by surprise, but it will further strain what are already limited resources.

Learn More
http://iapp.org/about

Learn More
https://www.truste.com/about-truste/