Measuring Privacy Operations 2019

Cookies, Local vs. Global Compliance, DSARs and more

iapp

TrustArc
Privacy Compliance

Measuring Privacy Operations 2019

Cookies, Local vs. Global Compliance, DSARs and more

Introduction

In Measuring Privacy Operations 2019, the IAPP and TrustArc offer privacy professionals around the globe a look at how their colleagues are implementing privacy requirements. This is the latest in a series of reports designed to help companies benchmark their own privacy practices against those of their partners and competitors.

In this report, we explore whether and how a company's size, location, sector and geographic reach affect their approach to data protection. We look at whether companies have adopted a single global data protection strategy or are segmenting data subjects by jurisdiction, as well as the factors influencing that choice. We identify current areas of focus for privacy professionals and consider how legal requirements are affecting data processing practices. We also consider how the guidance offered by outside attorneys and consultants differs from the practices adopted by the companies they serve.

Our survey data demonstrates, once again, that the majority of companies are thinking globally. Fifty-six percent of survey respondents are working toward a single global data protection strategy. The appeal of a global strategy that allows companies to offer the same rights and recourse to all their customers is clear, but with more than a third of respondents complying with six or more laws, it is also complex.

Our findings show that complying with this multitude of laws leads to continual change to policies. In the past 12 months alone, 80% of survey respondents updated their website privacy policies, and almost half updated their cookie policies. The percentages were even higher among EU-based companies, suggesting that the effect of the General Data Protection Regulation continued well into 2019.

In the past 12 months alone, 80% of survey respondents updated their website privacy policies, and almost half updated their cookie policies.

We drilled down further on organizations' cookie consent policies, given new guidance from EU regulators in this area, and found that there is still a lot of variance across industry. Approximately equal percentages of companies reported having no cookie manager, deploying an "opt-out" cookie tool and using an "opt-in" system. This is one area where we saw significant differences between geographies, with EU respondents much more likely to have a cookie banner than their U.S.-based counterparts. Outside counsel and consultants were also more likely to recommend a conservative approach, with the majority advising their clients to require "opt-in" consent for non-essential cookies.

We saw some evidence of better data hygiene, though the results were mixed. About a third of companies reported collecting less data and retaining it for shorter periods and even more indicated that they regularly delete personal data. A slightly smaller percentage chose to store data but deidentify it for analytics or business intelligence. A small percentage of companies reported a decrease in user tracking, but more reported an increase.

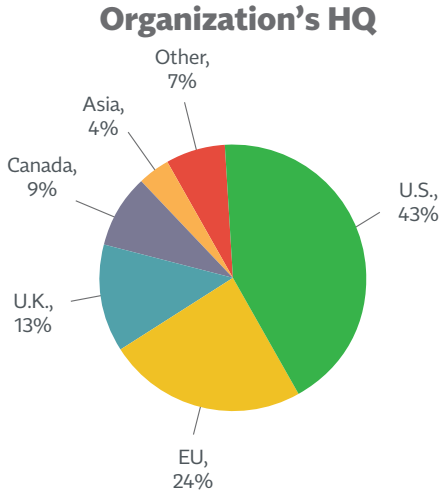
Privacy assessments of all types continued to be a key feature of companies' data governance programs. This year, vendor/third-party risk assessments ranked first among privacy assessments conducted globally, just beating out data protection impact assessments, which topped the chart in 2018. This change in priority may have been driven by high-profile enforcement actions that demonstrated regulators' willingness to hold companies accountable for lack of due diligence concerning third-party data handling. Regional differences were evident in this area, with U.S. companies more likely to conduct vendor/third-party risk assessments and their EU-based counterparts favoring DPIAs. We noted significant geographic differences with legitimate interest assessments (more common among EU organizations) and data breach readiness assessments (favored by U.S. organizations), as well. These geographic discrepancies can be tied directly to differences in the EU and U.S. legal regimes governing privacy. For instance, the GDPR requires companies conducting a DPIA to describe the legitimate interest pursued, where applicable. The U.S. legal regime does not. U.S. state law, on the other hand, has long required data breach notifications, necessitating readiness programs. Data breach notification is a more recent addition to the EU data protection regime, having been added as a new requirement under the GDPR.

While assessments are keeping privacy professionals busy, data subject access requests generally are not. DSARs have remained relatively low since the GDPR went into effect. More than 60% of respondents reported receiving 10 or fewer access requests per month. Only 7% reported receiving more than 100 per month. These percentages aligned closely with what we saw in 2018.

The limited number of DSARs likely provides breathing room for privacy professionals who only recently implemented new GDPR requirements and are now looking ahead to implementation of the California Consumer Privacy Act. It will be interesting to see whether and how CCPA changes companies' focus moving forward.

Methodology and demographics

Our survey was sent to subscribers to the IAPP's Daily Dashboard, which reaches more than 60,000 people globally. Among the 327 people who filled out the short survey — which took, on average, six minutes to complete — 43% were from the United States, 37% were from the European Union (including the U.K.), and 9% were from Canada.



Company-sizes were well represented, with one in four respondents from a firm with fewer than 250 employees, while 19% work for companies larger than 25,000 employees. In general, the largest companies were far more likely to be headquartered in the United States, while the EU organizations tended to be smaller in size.

In general, the largest companies were far more likely to be headquartered in the United States, while the EU organizations tended to be smaller in size.

Respondents represent a variety of industries, as well, nearly evenly split between sectors traditionally regulated for privacy (e.g., health care, financial services and banking, insurance) at 35% and sectors traditionally not subject to privacy regulation (e.g., technology and software, manufacturing) at 33%. Those working in legal or consulting services made up 16% of respondents, with another 11% representing governmental or non-profit organizations.

Employer size

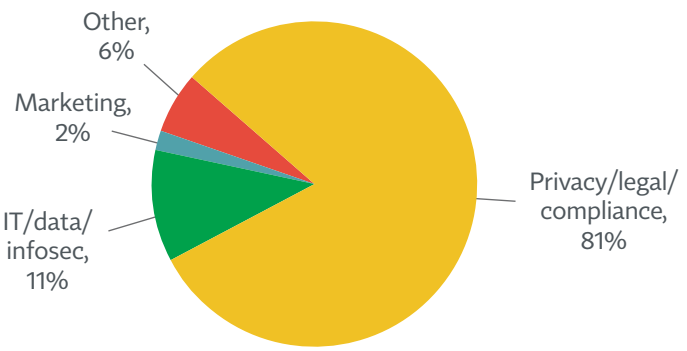
1–250	25%
251–1,000	17%
1,001–5,000	20%
5,001–25,000	19%
25,000 +	19%

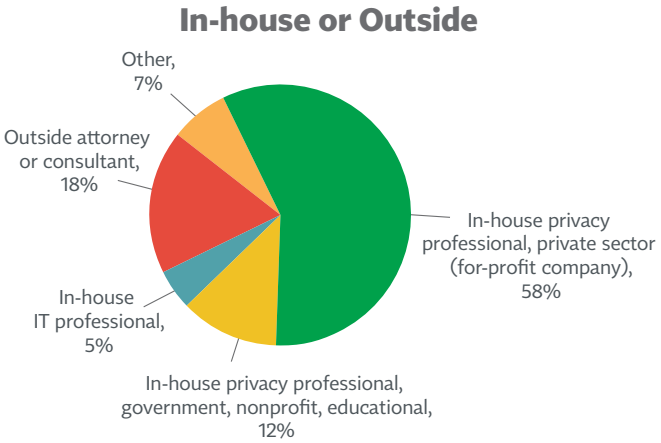
Sector/industry

High-regulated industry (e.g., health care, financial services, insurance, pharma)	35%
Unregulated industry (e.g., technology and telecommunications, manufacturing, software)	33%
Legal or consulting services	16%
Government/education/nonprofit	11%
Other	5%

As is typical of privacy professionals in the IAPP network, a vast majority — 81% — of survey respondents work in the privacy, legal or compliance functions within their organization, while only 11% work in IT, data or information security. In this survey, we also asked respondents whether they work in-house or as outside consultants, shifting them to different question sets based on their response. Approximately 8 out of 10 respondents work inside an organization.

Core function within the organization





Think globally, act globally?

Many corporate IAPP members serve customers all over the world, and many individual privacy professionals who belong to the IAPP work for multinational organizations. This is especially true of members whose organizations are headquartered in the U.S. Of the respondents to our survey, just 17% reported their employers' customers or employees (collectively, data subjects) are primarily in one geographic location.

We know the 80% who are responsible for data subjects in multiple jurisdictions often grapple with whether to (a) create a single data protection program that attempts to give all of their customers, worldwide, a common privacy experience whether or not they live in a country with comprehensive privacy laws; or (b) segment their customers geographically and manage personal data according to the laws of their customers' residence.

Among survey respondents, well over half — 56% — answered "yes" to the question: "Is your organization working toward a single, global data protection/privacy strategy for data subjects' rights?" This number holds true across geographies.

Overall, approximately one in four (24%), selected: "No, we categorize data subjects by jurisdiction and geography and handle each data subject's data according to the laws that apply to him or her." A slightly higher number of U.S. respondents tended to select this answer (28%) than those from the EU (21%). Although overall 17% of respondents do business in only one region, those from the EU were much more likely (21%) to do business in one region than those from the U.S. (11%). When we isolate the "unregulated" companies — principally software, tech and telecom — we see that six in ten have a single global strategy for data subject rights' compliance, while only 8% report they have customers in just one region.

Do you have a single, global privacy strategy?

	Overall	U.S.	EU + U.K.	Regulated	Unregulated
Yes	56%	56%	55%	51%	**61%**
No, segment by geography	24%	**28%**	21%	27%	27%
No, customers in only one region	17%	11%	**22%**	19%	8%
Don't know	3%	5%	1%	3%	4%

When we asked outside counsel and consultants to share how they advise clients on this issue, we found they tended to advise their clients to segment by geography or serve clients in only one region in approximately the same proportions as our overall survey respondents. Where they differed, however, was that we gave them a chance to answer "it depends" to the question. Accordingly, only about 40% said they advise their clients to follow a single global privacy strategy, while 14% selected "it depends."

The gist seems to be that a global strategy is advised but tailored to individual jurisdictional requirements where appropriate. Typically, the "global" strategy is to follow the GDPR and ePrivacy Directive for all regions and role out geographic-specific nuances if needed.

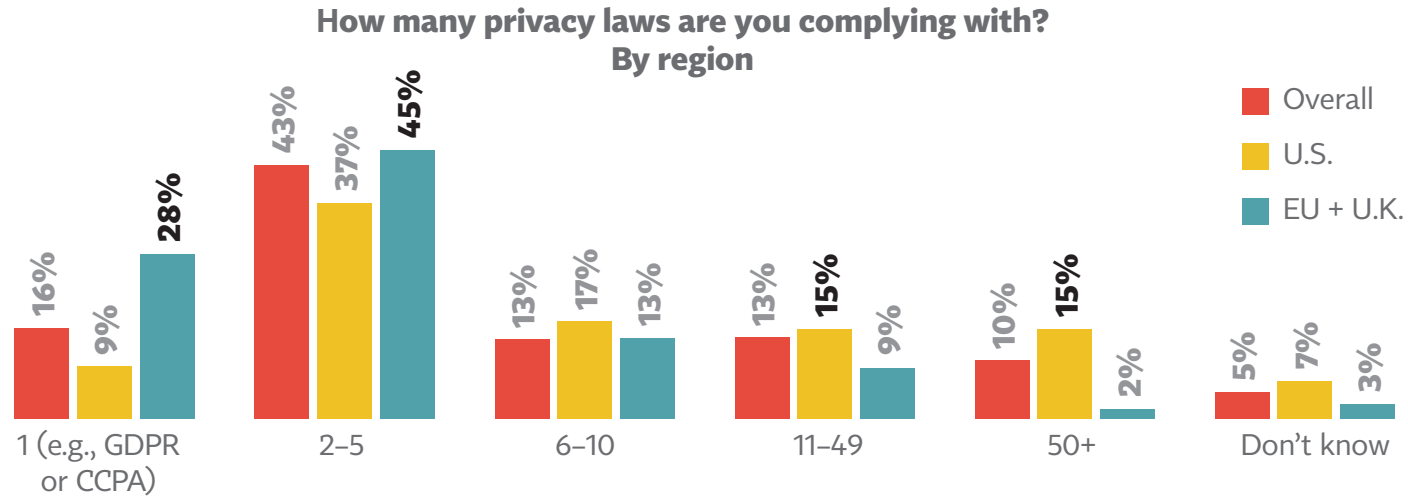
Consistent with their efforts to create a uniform data protection or privacy strategy globally, we find that many organizations — 79% — are complying with two or more privacy laws, while only 16% are focused on just one. Indeed, while the largest segment of respondents (43%) report actively working to comply with between two and five privacy laws, a solid 13% are working on six to ten laws, another 13% are grappling with 11 to 49 laws, and 10% report actively working to comply with 50 or more privacy laws at once.

EU respondents were more likely to report actively working to comply with five or fewer privacy laws, while U.S. respondents were more likely than their EU counterparts to be complying with 11 or more laws. This may reflect either the sectoral nature of privacy law in the U.S., the prevalence of multinational organizations employing U.S. respondents or both.

ONE GLOBAL STRATEGY? IT'S NOT 'YES' OR 'NO' BUT A HYBRID.

As a privacy professional located in the EU explained:

> We heavily debated this "global versus local" approach internally a while ago and made the decision to follow a "hybrid" approach. This means that we are clearly working toward a single global strategy to make our global privacy program effective and the usage of our support tooling scalable, but that we reflect the local law where necessary. These local rules can lead to bigger strategic deviations, e.g., in markets with data localization requirements, such as China or Russia, but in most of the cases, it is only a smaller implementation/operationalization issue that requires local policies, processes and/or modifications of otherwise global IT tools.
>
> We wanted to have one strong global strategy in place instead of scattered local strategies but also wanted to be able to deviate where necessary. To support this, we carefully drafted our strategy and chose high-level language to address cases in which there are local deviations (e.g., DSR response timelines under the GDPR, CCPA and LGPD). With that, the local deviation is only an implementation issue and doesn´t necessitate a local strategy.



Benchmarking cookies practices

For many, addressing cookies consent post-GDPR implementation has been time consuming and complicated. To recap, the ePrivacy Directive — as implemented by EU member state laws, such as the U.K.'s Privacy and Electronic Communications Regulations — prohibits placement of a file on an end user's terminal equipment (typically in the form of a cookie or another tracking technology) without the user's consent.

Prior to the GDPR, many organizations complied with this rule by posting a notice on their website announcing that the site uses cookies and that continued use of the site constituted consent to or acceptance of those cookies.

But "consent" is defined under GDPR Article 4 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." Furthermore, guidance from prominent EU data protection authorities indicates consent for nonessential cookies must be "opt-in" rather than passive or tacit acceptance of a site's cookies policy.

Accordingly, many privacy professionals worked with their organizations to come up with a new approach to cookies. Our survey asked what approach they are taking today, and here are the results:

21% do not have a cookie banner or cookie manager at all.

25% have a cookie banner on their site indicating continued use of the site constitutes consent.

19% use an "opt-out" cookie tool (nonessential cookies are "on" unless declined).

20% use an opt-in system (non-essential cookies are "off" unless accepted).

15% other/don't know

When we dig deeper, we find noticeable differences by geography. Respondents working for EU-based companies were far less likely to report that their site has no cookie banner (10% for the EU versus 24% for the U.S.). At the same time, respondents from U.S.-based organizations were more likely to select "don't know" or "other," with some explaining that their company has multiple websites and tends to have a different policy based on the customer's location.

Outside counsel and consultants were decidedly more conservative when they advise clients on cookies compliance. A full 59% — nearly 6 in 10 — reported they advise their clients to use an "opt-in" system, with a tool that doesn't drop nonessential cookies until after the user affirmatively agrees. Another 14% recommend a cookie notice with an opt-out system (cookies are set unless the user does not agree), while just 9% advise their clients to use a cookie banner that considers consent to involve continued use of the website.

Operationalizing privacy and data protection

Policy and practice changes

Those familiar with GDPR compliance always knew much work remained after May 25, 2018, and indeed that the job of compliance is never really done. We wanted to know, in the last year, what privacy-related operational changes have organizations made?

With all the flurry around cookie notices and consent, overall, 80% of respondents reported updating their website's cookie policy in the past 12 months. Nearly half (47%) updated their organization's privacy policy. Another 4 in 10 worked on deleting data more frequently, while 36% invested in decreasing data retention time. Interestingly, in the age of artificial intelligence and business intelligence, organizations were directionally more likely to increase (20%) versus to decrease (12%) data analytics and user tracking over the past year, showing that privacy laws may have raised awareness about the impact of such techniques but haven't slowed their adoption.

These policies reflect, in part, the significance of the ePrivacy Directive in the EU and U.K. data protection landscape, and the fact that U.S. companies are more likely to be outside the scope of the directive — or, in some cases, less concerned about its enforcement

These figures hold essentially true across geographies, as well as between regulated and unregulated industries, with a few exceptions. Respondents in the EU and U.K. were more likely than their U.S. counterparts to update their website's cookie policy (56% EU versus 44% U.S.) and to delete personal data more frequently (52% EU compared to 39% U.S.). Those from the EU and U.K. were also far more likely (30%) than those in the U.S. (13%) to convert from an opt-out to an opt-in email marketing strategy across all geographies. These policies reflect, in part, the significance of the ePrivacy Directive in the EU and U.K. data protection landscape, and the fact that U.S. companies are more likely to be outside the scope of the directive — or, in some cases, less concerned about its enforcement.

Privacy-related operational changes made in the last 12 months

(Select all that apply.)

	Overall	U.S.	EU + U.K.
Updated website's privacy policy one or more times	80%	77%	85%
Updated website's cookie policy one or more times	47%	44%	**56%**
Deleted personal data more frequently/regularly	42%	39%	52%
Decreased data retention time	36%	35%	44%
Collected less data (implemented minimization)	32%	27%	34%
Continue to store data but deidentified it for analytics and BI	25%	24%	24%
Increased use of data analytics and user tracking	20%	22%	17%
Converted from an opt-out to an opt-in email marketing strategy across geographies	21%	**13%**	**30%**
Decreased use of data analytics and user tracking	12%	13%	14%
None of the above	7%	6%	7%
Don't know	4%	4%	2%

Privacy assessments

Drilling down specifically on privacy assessments, we asked which of several types of assessments organizations currently conduct. The GDPR's data protection impact assessments — mandated in high-risk processing situations as set forth in Article 35 — was the second-most-common assessment overall with 61% of respondents selecting this option.

The most common type of risk assessments selected (overall by 63% of respondents) were those built to vet the privacy and security practices of vendors and other third parties handling personal data. This top ranking was influenced largely by U.S.-based respondents for whom vendor/third-party risk assessments was by far the number one risk assessment by far — 78% selected this response. Meanwhile, for privacy pros in the EU and U.K., this type of assessment ranks third behind conducting DPIAs (81%) and legitimate interest assessments (53%).

We also see big differences in the role privacy professionals in the U.S. play in data breach readiness assessments — 38% of U.S.-based respondents said their organization currently conducts them, while only 26% of respondents from the EU and U.K. selected that answer. As well, with regard to security, the EU and U.K. respondents were more likely to follow the ISO standard 27001, whereas alignment with the U.S. National Institute of Science and Technology assessments were far

more common in the U.S (28% of U.S. respondents do this assessment) than in the EU and U.K. (where only 5% follow this guideline).

There's less of a difference between highly regulated and unregulated firms when it comes to the types of privacy assessments they conduct, other than a slight up-tick in GDPR-related assessments among unregulated firms, which are more likely to be doing business in the EU regardless of where they are located.

There's less of a difference between highly regulated and unregulated firms when it comes to the types of privacy assessments they conduct.

Which of the following types of privacy assessments does your organization conduct?

	Overall	U.S.	EU + U.K.	Regulated	Unregulated
Vendor/third party risk assessments	63%	**78%**	52%	69%	69%
Data protection impact assessments	61%	53%	**81%**	60%	65%
Privacy impact assessments	53%	55%	45%	57%	49%
Legitimate interest assessments	34%	24%	**53%**	32%	**41%**
Data breach readiness assessments	30%	**38%**	26%	33%	30%
International data transfer assessments	30%	27%	37%	29%	35%
Alignment with ISO 27001 assessments	27%	26%	33%	25%	31%
Alignment with NIST assessments	15%	**28%**	**5%**	19%	15%
Privacy threshold assessments	15%	16%	15%	14%	17%
Don't know	6%	4%	3%	5%	3%
Other	4%	4%	2%	3%	5%

DPIAs

GDPR Article 35 requires data controllers to "carry out an assessment of the impact" of processing activities that use new technologies or otherwise create high risks to the rights and freedoms of data subjects. EU member states can further designate situations in which DPIAs are required. DPIAs must be conducted prior to engaging in the data processing activity and should involve the advice of a designated data protection officer.

Because external counsel and consultants are engaged more often in DPIA assistance than in any other privacy-related risk assessment, it follows that they find DPIAs to be either "very important" or "extremely important" for their business clients. More than 6 in 10 (61%) ranked DPIAs a 4 or 5 on a 5-point importance scale.

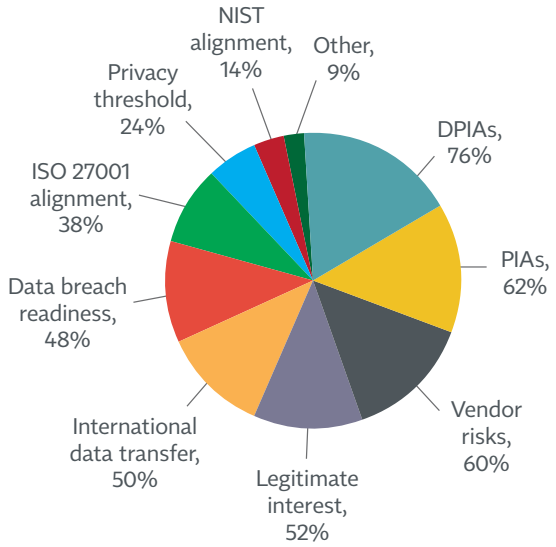
Lawyers and Consultants: How important is conducting DPIAS for clients?

Not at all important	5%
Slightly important	12%
Moderately important	22%
Very important	**39%**
Extremely important	22%

With GDPR-mandated DPIAs serving a prominent role in compliance activities, we wondered just how many of them firms have completed in the past 12 months. The most likely answer this year was "between 1 and 5," selected by 26% of respondents. Another 12% have conducted between 6 and 10 DPIAs, while

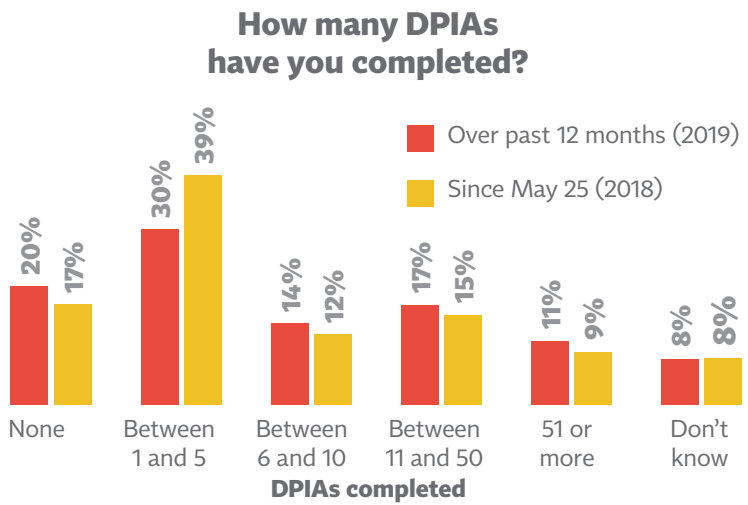
ENGAGING COUNSEL/CONSULTANTS FOR PRIVACY ASSESSMENTS

Outside counsel and consultants are more likely to be engaged by their clients for DPIAs (76%) than for any other type of assessment, including PIAs (62%). This reflects the importance of engaging external advice when processing special categories of data that might pose a higher risk to data subjects. Another area of potential risk — assessing vendors — came in third for external assistance (60%), trailed by legitimate interest assessments (52%) and international data transfer assessments (50%). These numbers are directional given the small sample size (n=58) but suggest that in-house privacy professionals are most likely to seek external guidance for managing high-impact data processing or analyzing a lawful basis for data processing or transfer.



14% have conducted between 11 and 50 such assessments in the last year. Only 9% have had to complete 51 or more DPIAs, while 17% have completed none.

When we compare these answers to a similar question asked in IAPP-TrustArc 2018 GDPR benchmarking survey, we find a similar story. In last year's survey, we first filtered out respondents whose organization does not have to comply with the GDPR to determine which percentage had prepared DPIAs since the GPDR was implemented — about five months in advance of the survey. This year, our question looks back over the prior 12 months. When we filter out those who indicated the GDPR does not apply (16%), it shows the following:



Among those completing no DPIAs, the largest percentage (62%) do not engage in high-risk processing activities, while another 23% plan to complete DPIAs in the next six months.

Article 30 reports

Organizations with more than 250 employees are obliged under GDPR Article 30 to maintain records of data-processing activities that include (among other things) the categories of data subjects and personal data processed, transfers to third countries, time limits for erasure, and technical and organizational security measures in place to safeguard the data.

The survey responses suggest that the Article 30 spigot runs either cold or hot, not warm: Companies either complete no Article 30 reports, or they do a lot of them. Few respondents report doing only a handful. For obvious reasons, respondents from organizations headquartered in the U.S. are more likely to say the GDPR doesn't apply — or that even if it does, they haven't prepared any Article 30 reports. Meanwhile, EU-based organizations are far more likely (29%) to have prepared 11 to 99 such reports or even 100 or more (22%).

Differences between companies that comply with only one privacy law and those that comply with multiple privacy laws are not significant; other than that, those complying with only one privacy law are more likely (25% to 15%) to say the GDPR does not apply.

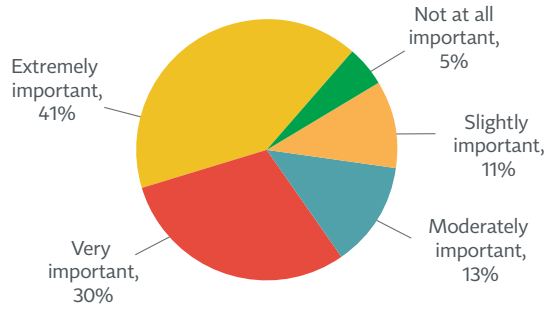
Among those completing no DPIAs, the largest percentage (62%) do not engage in high-risk processing activities, while another 23% plan to complete DPIAs in the next six months.

How many Article 30 reports has your organization created?

	Overall	U.S.	EU
GDPR is not applicable to our company	17%	**24%**	2%
None	13%	16%	7%
1–5	17%	12%	24%
6–10	5%	2%	7%
11–99	17%	12%	**29%**
100 or more	17%	18%	22%
Don't know	14%	17%	8%

Article 30 reports are not customer-facing compliance requirements like, say, a privacy notice or cookie notice on a company's website or even responsiveness to data subject requests (discussed next). So, one would assume they are lower on the priority list from the perspective of practical, cost-sensitive external counsel and consultants.

How important is it for lawyers and consultants to create Article 30 reports for clients?



To the contrary, however, when we asked outside counsel and consultants how important it is to "create Article 30 reports on behalf of your clients," 7 in 10 answered either "very important" or "extremely important." This is likely key not only to client engagement and fee generation, but also to helping clients reduce their overall risk profile. In the event of a compliance investigation, one way to demonstrate good faith and best efforts is through having Article 30 reports in order.

Data subject access requests

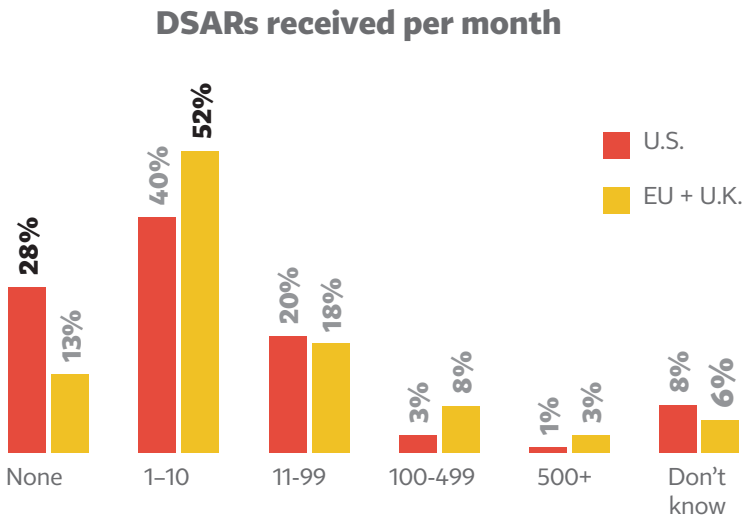
In fall 2018, IAPP and TrustArc asked privacy professionals how many data subject access requests they had received per month since the May 25 GDPR implementation date. We reported at the time that 22% had received none and nearly half of all respondents reported receiving between 1 and 10 per month, with 16% receiving 11 to 99 DSARs, only 9% receiving more than 100 monthly.

When we asked the same question in this year's survey, looking back over the prior 12 months, the numbers are much the same: 22% reported receiving no DSARs this past year, while 44% reported receiving between 1 and 10 per month. Approximately 1 in 5 (18%) reported receiving between 11 and 99 per month, only 5% received between 100 and 499 and just 2 percent received more than 550 monthly DSARs.

DSARs received per month (overall)

	2019	2018
None	22%	22%
1–10	44%	47%
11–99	18%	16%
100–499	5%	6%
500+	2%	3%
Don't know	9%	6%

When we isolate companies in the EU and U.K. from those in the U.S., we find both regions receiving relatively few DSARs each month, but organization in the UE and U.K. are more likely to get 1 to 10 requests (52%) than those in the U.S. (40%), while the U.S.-based organizations are slightly more likely to get none (28% versus 13%).



The remarkable consistency of monthly DSAR data year over year, however, may provide predictability to privacy professionals building out their internal staff for DSAR response activities, as well as setting budgets for privacy tech designed to support such requests.

Conclusion

This year's Measuring Privacy Operation's report makes clear that privacy professionals' plates are full. The evolving legal landscape and legal requirements themselves require regular assessments of data-processing operations and compliance programs. The expanding ecosystem of third parties handling data and enforcement actions in this area necessitate a focus on vendor risk assessments. New technologies, services and data uses also make continual policy reassessments a must. The data outlined here demonstrates, once again, that privacy is not a one-off endeavor.

Over the next year, the majority of companies that have implemented global privacy programs will face a decision point yet again. Will they be able to incorporate new CCPA requirements into their global privacy strategy or will they shift to a jurisdiction-based approach? Perhaps we will see an uptick in those deploying a hybrid model. While DSARs continue to be minimal for the vast majority of companies, CCPA could change this dynamic. Might the mandated visibility of "Do Not Sell Buttons" lead to an explosion of data subject requests? If so, will that lead companies to shift from manual response processes to automated ones? Will the private right of action linked to data breaches under the CCPA shift privacy professionals focus or lead to greater collaboration with their security colleagues?

While privacy professionals were busy in 2019, all signs suggest privacy programs will continue to evolve. Look for our continued monitoring of privacy programs and trends in the year to come.