MEASURING PRIVACY OPERATIONS

BENCHMARKING INFORMATION ON THE USE OF DATA INVENTORIES, ASSESSMENTS, DPIAS, DSARS, AND BREACH NOTIFICATIONS

iapp | TrustArc

EXECUTIVE SUMMARY

In this newest piece of an ongoing series of research that has looked at privacy operations and the use of privacy technology, the IAPP and TrustArc here examine the factors, including geographic region, organizational size, and sector, that are correlated with the current state and development of organizations' response to various operational demands upon their privacy programs. We focused on certain core operational responsibilities required for compliance with most privacy regulations and the European Union's General Data Protection Regulation (GDPR) in particular.

At the minimum, we establish a baseline of raw metrics, by which organizations can measure themselves, for how many of these kinds of activities privacy programs around the world are engaging in as part of their overall program efforts.

> ***"Our survey found that more respondents conduct DPIAs than any other form of risk assessment, including vendor vetting and even privacy impact assessments"***

Our research shows that foundational privacy program activities like data inventory and mapping are well established and common throughout the globe, in both the European Union and the United States, and among large and small organizations across sectors. These practices are managed largely with internal tools, and less often with commercially available software.

The GDPR, which applies to roughly 80 percent of our nearly 500 survey participants, encourages a risk-based approach to privacy, and specifically requires organizations to conduct risk assessments including "Data Protection Impact Assessments," or DPIAs, for high-risk processing activities. Our survey found that more respondents conduct DPIAs than any other form of risk assessment, including vendor vetting and even privacy impact assessments (PIA), an older cousin to the DPIA.

Among survey respondents subject to the GDPR, we found that many organizations have not yet been forced to engage with some of its major obligations. A majority of respondents have created fewer than five (or even zero) DPIAs since the GDPR took effect. Around one-quarter of respondents have prepared between one and five Article 30 records of processing reports, while another 15 percent have prepared none, and a full 19 percent simply don't know.

Data subject access requests have not yet come pouring in (generally speaking) either. Most respondents field fewer than 10 data subject access requests per month, and 22 percent have yet to receive any. Meanwhile, 30 percent of respondents have notified a supervisory authority of at least one data breach, which is in line with prior research that around 4 in 10 organizations report having experienced privacy incidents in a previous two-year period. The firms most likely to report data breaches are in the banking, insurance and telecommunications sector; software and services industries (the typical data processor roles) report the least often.

We've even created a fun new ratio: The median organization receives 7 DSARs per million data subjects per month.

In terms of tools used to conduct their jobs, most respondents continue to use informal internal means for data inventory and mapping, DPIAs, and other privacy operations. For mapping and inventory, just 10 percent use commercial software tools developed specifically for the task but this number grows to 20 percent for DPIAs and for records of processing. We also find that, while there is some overlap, organizations are generally investing in tools for specific tasks, rather than buying or adapting one piece of software to handle the whole suite of privacy program management tasks we investigated with this research.

These results showing an uptick in number of operational tasks completed by organizations that have used outside consultants and counsel, and have invested in privacy technology, also create a big of chicken-and-egg conundrum: Do organizations using privacy technology and outside firms create more DPIAs, for example, because the technology helps them be more efficient, or are organizations that create more DPIAs more likely to invest in privacy technology because there's more clearly a potential return on investment?

INTRODUCTION

A "COUNT"-DOWN TO COMPLIANCE

As privacy programs mature, they begin to focus on more than simply making sure the organization isn't breaking the law. This is well documented by IAPP research over the years.

We know that employees begin to have privacy responsibilities within the individual business units, that privacy by design becomes a business imperative, and that organizations begin to outfit their privacy teams with the tools and resources they need to be proactive, rather than reactive, with privacy considerations.

We also know that mature privacy teams begin to report more often to the board of directors. And every board of directors worth its salt asks about return on investment.

Answering those questions about effort and spend vs. results can be difficult for compliance-focused operations. How do you quantify a bad thing not happening? But as privacy teams get more operational, they develop metrics that can be used to benchmark against other, similar organizations and to document trends over time.

To help with both of those efforts, we offer this new study that looks at certain tasks regularly completed by privacy teams, and a few of those mandated by the EU's General Data Protection Regulation. Just how many data subject access requests are coming through on a monthly basis? Just how many data protection impact assessments are being completed and filed with data protection authorities?
What's normal?

Well, it's still early, but the returns we see in the following research suggest that privacy teams are managing well, but certainly have plenty of work on their hands. They are increasingly investing in tools to help themselves, but they still largely make do with standard business software and a good deal of ingenuity. And there is a wide range of experiences in the marketplace: What can seem like an avalanche to some is producing not a flake for others.

Regardless of your experience, we hope these numbers provide a yardstick by which to measure your workload as well as some ideas for evaluating your program's performance as a whole.

Chris Babel, CEO, TrustArc

J. Trevor Hughes, CIPP, CEO, IAPP

MEASURING PRIVACY OPERATIONS

BENCHMARKING INFORMATION ON THE USE OF DATA INVENTORIES, ASSESSMENTS, DPIAS, DSARS, AND BREACH NOTIFICATIONS

The IAPP-Trust Arc 2018 Survey on Privacy Program Metrics looked to establish some baseline metrics by which privacy programs around the world can benchmark themselves. How many business processes are organizations mapping? How many reports are they creating in order to comply with Article 30 of the EU's General Data Protection Regulation? How many privacy or data protection impact assessments are necessary? How many incidents rise to the level of breach reporting?

Are people being overwhelmed by subject access requests?

Further, we examined the factors, including geographic region, organizational size, and sector, that are correlated with the activity of organizations' privacy programs. We sought to provide data touching upon a range of questions: Why are some organizations mapping/inventorying more business processes than others? Which types of privacy assessments are most popular in the United States, Europe, and elsewhere around the world? What factors lead organizations to perform greater or fewer DPIAs? Is there a greater need to perform more DPIAs in certain sectors than in others? Does the way in which an organization develops its DPIA process (i.e., with the participation of outside legal counsel, outside consultant, or an in-house team, or through the use of a template provided by a regulatory/government agency or bundled with an assessment tool) affect how often they are performed?

> ***"We examined the factors, including geographic region, organizational size, and sector, that are correlated with the activity of organizations' privacy programs."***

This study provides insight into each of these questions, while also examining numerous other key components of a GDPR-compliant privacy program.

METHODOLOGY

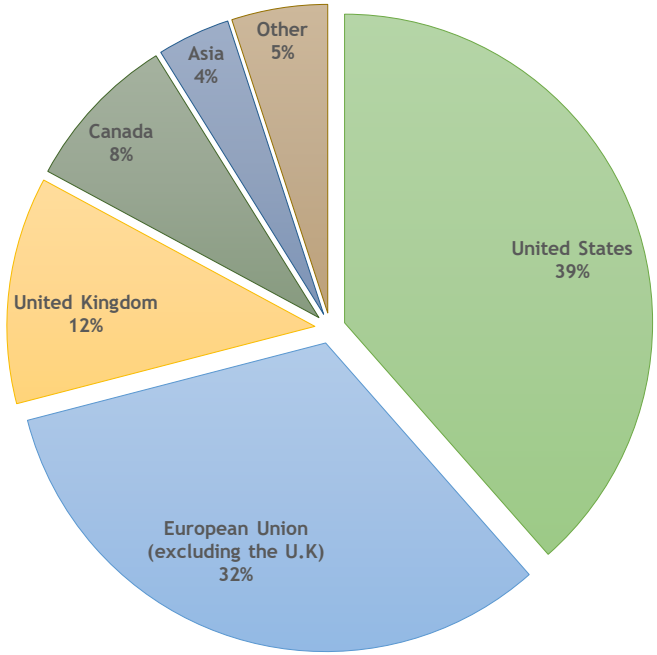
AS IT DOES WITH MOST OF ITS SURVEYS, THE IAPP USED THE DISTRIBUTION LIST FOR THE DAILY DASHBOARD TO SELECT RESPONDENTS FOR THE SURVEY. ONE INITIAL AND ONE FOLLOW-UP EMAIL INVITATION WITH A LINK TO THE SURVEY WAS SENT TO 41,000 DAILY DASHBOARD SUBSCRIBERS. SUBSCRIPTION TO THE DAILY DASHBOARD IS FREE, AND MOST OF ITS SUBSCRIBERS WORK IN PRIVACY AND ARE INTERESTED IN PRIVACY ISSUES. WHEN SIGNING UP, SUBSCRIBERS ARE NOTIFIED THAT THEY MAY SOMETIMES BE ASKED TO RESPOND TO IAPP SURVEYS. INVITATIONS TO TAKE THE SURVEY WERE SENT BETWEEN OCTOBER 23 AND NOVEMBER 6, 2018.

THE SURVEY CONTAINED 27 QUESTIONS, INCLUDING DEMOGRAPHIC QUESTIONS. A TOTAL OF 496 PEOPLE TOOK THE SURVEY, WHICH TOOK AN AVERAGE OF SEVEN MINUTES TO COMPLETE.

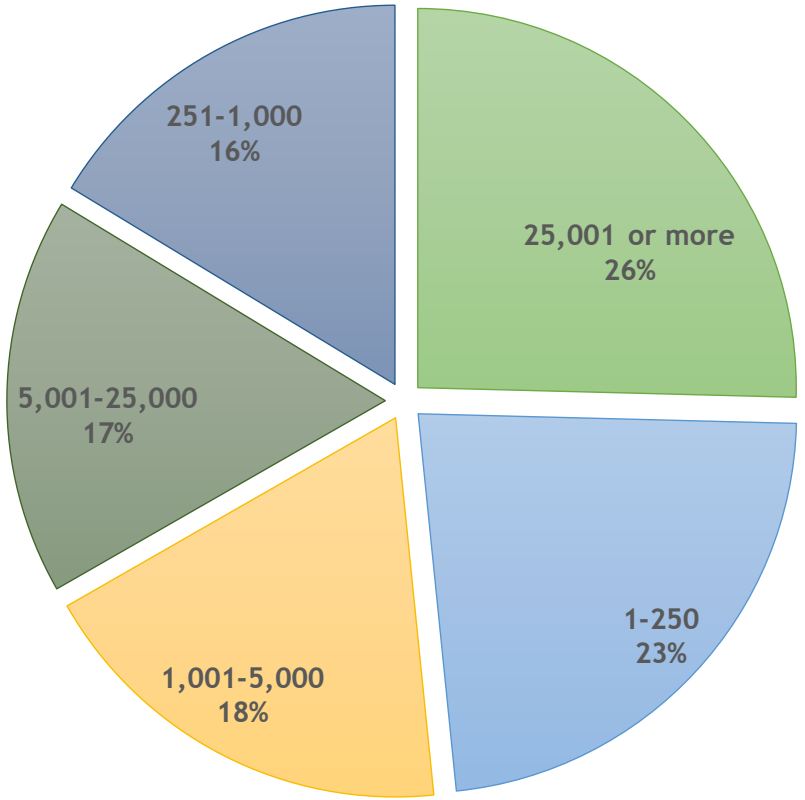
DEMOGRAPHICS

The largest group of respondents works in the U.S. (39 percent), followed by the European Union, excluding the U.K. (32 percent), the U.K. (12 percent), and Canada (8 percent).

IN WHICH OF THE FOLLOWING REGIONS ARE YOU CURRENTLY BASED?



HOW MANY PEOPLE ARE EMPLOYED GLOBALLY BY YOUR ORGANIZATION?

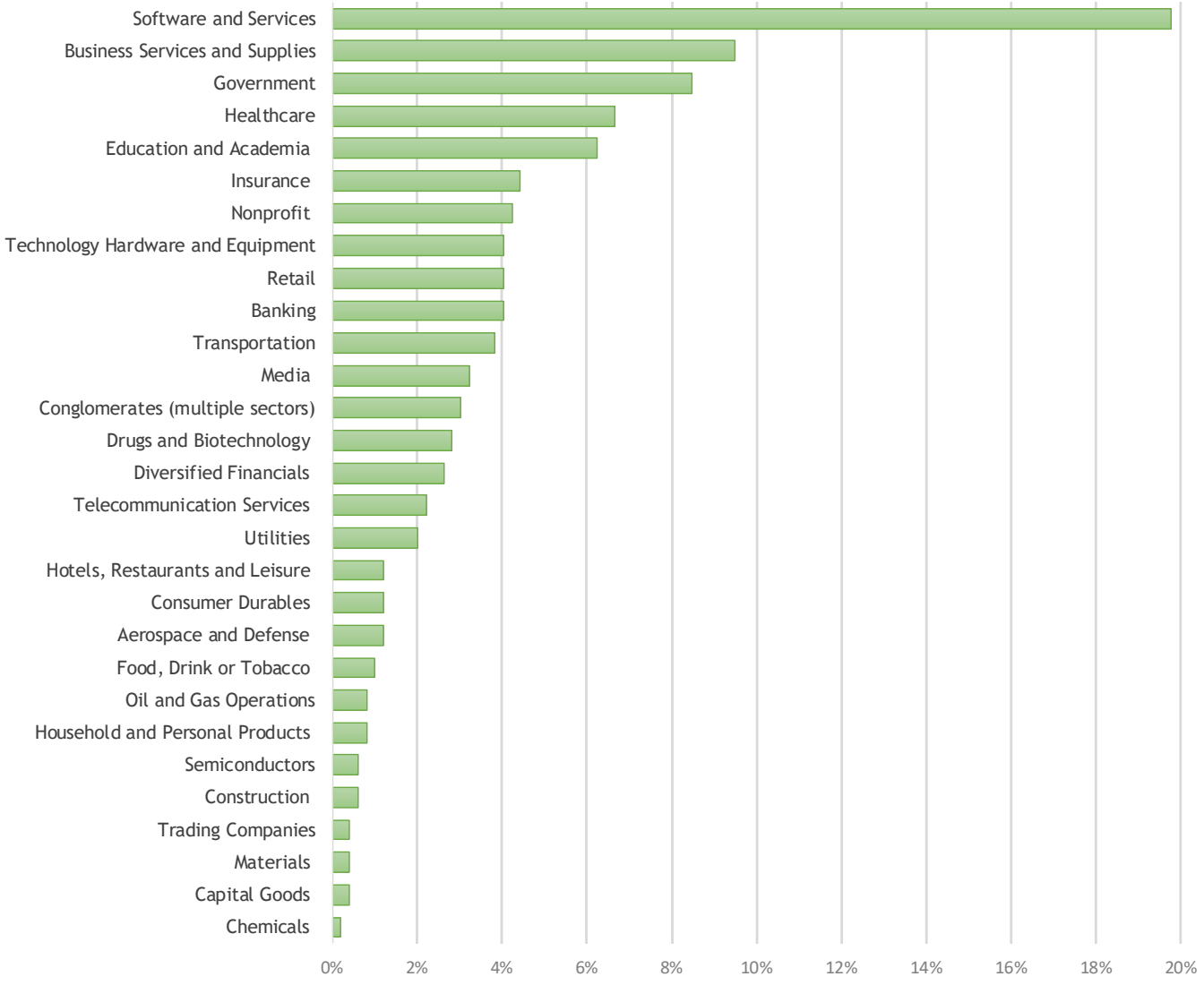


Respondents were evenly distributed throughout the range of company sizes, with organizations that employ 25,001 people or more representing 25 percent of survey respondents, followed next by organizations that employ 1-250 people (23 percent).

DEMOGRAPHICS

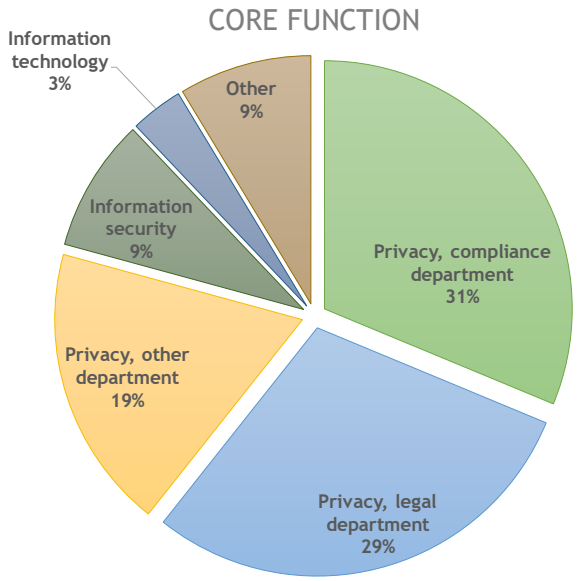
WHICH OF THE FOLLOWING BEST DESCRIBES YOUR COMPANY?

Among the many industry sectors represented in the survey, software and services sector had the largest percentage (20 percent), followed by business services and supplies (9.5 percent) and government (8.5 percent). Health care (7 percent) and education/academia (6 percent) rounded out the top five representative sectors.



WHICH OF THE FOLLOWING BEST DESCRIBES YOUR CORE FUNCTION WITHIN YOUR COMPANY?

To ensure our survey reached the expected audience, we asked respondents to report on their location within the organization. As expected, nearly a third of respondents described their role as privacy, compliance department (31 percent), followed closely by privacy, legal department (29 percent), and privacy "other" (19 percent). Only around 20 percent work in a function not principally dedicated to privacy.



HOW RISK ASSESSMENT IS DONE

The substantive questions of the survey examined practices related to data inventory and mapping; privacy assessments, with a focus on data protection impact assessments; records of processing pursuant to Article 30 of the GDPR; data subject access requests; and data breach notifications. These time-intensive tasks are crucial to maintaining an ongoing privacy program. Building systems for these tasks can take many employee hours, involve investments in specialized tools, and even engagement of outside consultants or legal assistance.

But how often, once these systems are in place, are they used now that the GDPR is in effect? This next section explores risk-based foundational exercises undertaken by organizations, regardless of their need to comply with the GDPR, followed by a discussion of certain time-intensive GDPR-specific compliance tasks.

DATA INVENTORY IS A WIDESPREAD PRACTICE, STILL MANAGED ON SPREADSHEETS

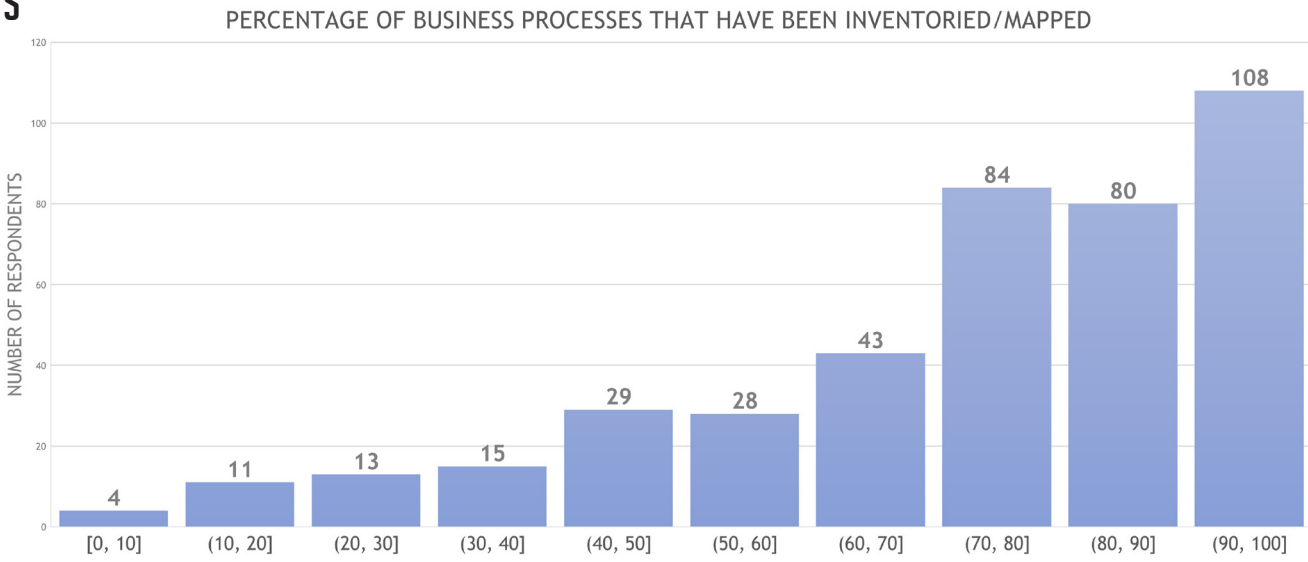
Respondents were first asked whether their company has created a data inventory of its business processing activities. About 83 percent of respondents said yes, 13 percent said no, and 4 percent were unsure. This is dramatically different from the results of a 2016 IAPP report, in which only 43 percent of respondents overall reported engaging in routine inventory and mapping exercises. In that report, 30 percent promised they were planning to begin inventory exercises, a nod to GDPR compliance. Somewhere between that survey and this one, even more organizations have seen the prudence of data inventory and mapping exercises. As well, the IAPP has added more survey respondents from the EU.

Predictably, respondents from the EU (excluding the U.K.) were more likely to have created a data inventory of their businesses practices, whereas respondents from Canada were less likely to have done so.

These results are not surprising. To comply with many privacy and data protection responsibilities – including transparency regarding data processing activities, assigning a lawful basis for processing, responding to data subject access requests, confirming data processing and security obligations with a business partner, etc. – an organization must first understand what data it processes, how, where and why.

Those who conduct data processing report they have, on average, mapped 75 percent of their business processes (the median number was 80 percent). On average, respondents from the EU (excluding the U.K.) reported mapping more of their business processes (79 percent on average). Those who used customized GRC (short for "governance, risk management and compliance") software and internally-developed systems to perform data inventory and mapping also reported mapping higher percentages of their business processes (77 percent and 80 percent respectively) than others.

The least likely to have conducted data inventory/mapping? Those who work in education/academia, which is somewhat surprising in light of the sensitivity of the data processed at such institutions (e.g. student health records and transcripts, financial information of students and donors, etc.), but perhaps understandable given general budget constraints in the education arena.



HOW RISK ASSESSMENT IS DONE

Mapping and inventory operations are most commonly conducted using manual/informal tools, such as email, spreadsheets, and in-person communication, with almost half (45 percent) primarily using these basic business tools. This is down from 62 percent using this system in the 2016 survey.

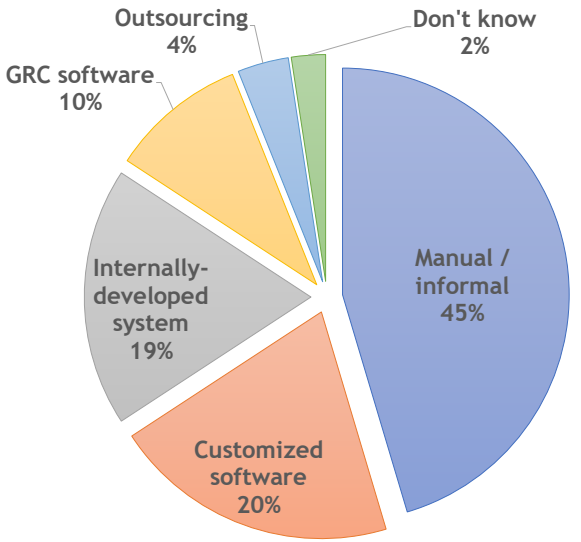
WHAT TOOLS DO YOU USE TO PERFORM DATA INVENTORY AND MAPPING?	2018	2016*
MANUALLY/INFORMALLY USING EMAIL, SPREADSHEETS ETC.	45%	62%
SYSTEM DEVELOPED INTERNALLY	18%	36%
COMMERCIAL SOFTWARE TOOL DESIGNED SPECIFICALLY FOR INVENTORY/MAPPING	20%	10%
GRC SOFTWARE CUSTOMIZED FOR INVENTORY/MAPPING	10%	12%
OUTSOURCE TO EXTERNAL CONSULTANTS/LAW FIRMS	4%	8%
DON'T KNOW	3%	2%

* IN 2016, RESPONDENTS COULD SELECT ALL THAT APPLIED.

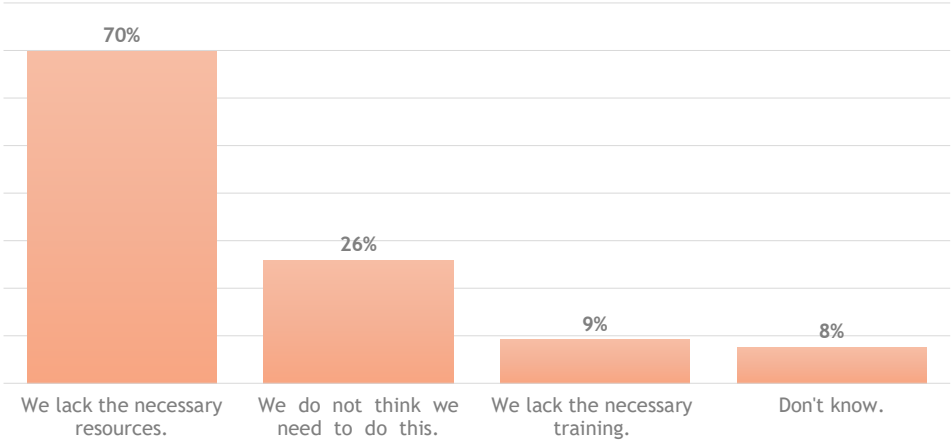
Approximately one in five respondents uses a commercial software tool designed specifically for data inventory/mapping, double the 10 percent who did so in 2016. Whereas 36 percent used an internally developed system in 2016, this year only 18 percent do. Almost 12 percent use governance, risk management and compliance software that is customized for data inventory/mapping purpose, on par with the 10 percent reporting such programs two years ago. Finally, only about 4 percent outsource their data inventory/mapping to an external consultant or law firm – half of the percentage who did so in 2016.

Meanwhile, respondents who admitted they had not conducted mapping exercises were most likely to cite a lack of necessary resources, with 70 percent of respondents giving this answer (up from 58 percent saying so in 2016). "We do not think we need to do this" was the second most-common response (26 percent), while a lack of training came in third at just 9 percent. Among Canadians and respondents from the EU, lack of training was a more common answer. Those least likely to cite lack of resources as an excuse were respondents from the U.S. and those in the retail sector.

PRIMARY TOOL USED TO PERFORM DATA INVENTORY AND MAPPING



REASONS FOR NOT INVENTORYING BUSINESS PROCESSES



HOW RISK ASSESSMENT IS DONE

DPIAS/PIAS AND VENDOR MANAGEMENT MOST COMMON RISK PROGRAMS

Many privacy regulations – and the GDPR in particular – take a risk-based approach to data protection. And, of course, risk lurks throughout the data processing life cycle.

While privacy impact assessments, often called data protection impact assessments in the EU, have long been integral parts of effective privacy programs, DPIAs are now legally required in some circumstances by the EU's GDPR, which has brought focus to the spectrum of impact assessments, from initial impact assessments and targeted assessments against certain frameworks all the way to formal DPIAs delivered to EU data protection authorities.

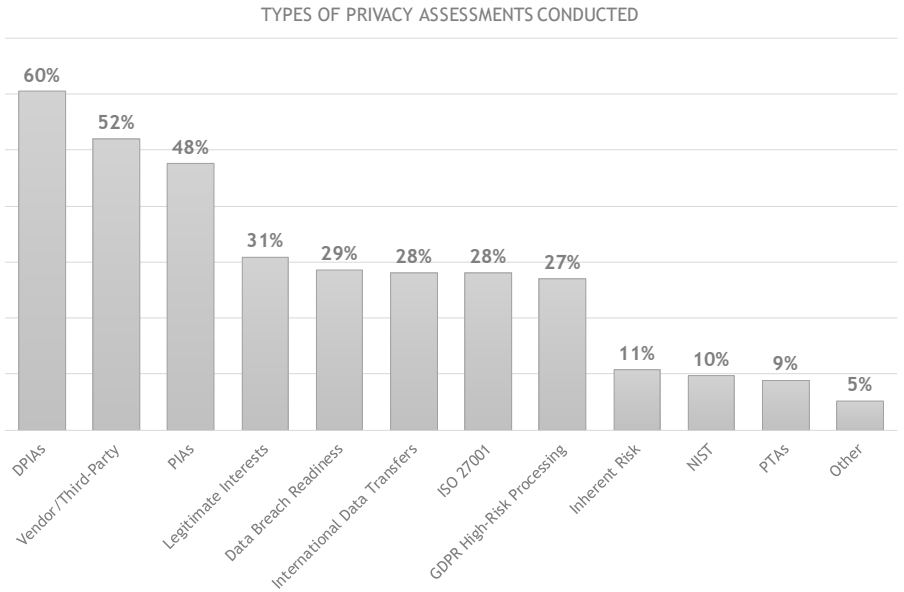
Thus, we explored with respondents the types of privacy assessments their organizations currently conduct. A list of 11 different kinds of assessments, from which respondents could select multiple answers, as well as an open-ended "Other" answer choice, were presented (see full list in chart, this page).

DPIAs were the most common privacy assessment, with 60 percent of respondents reporting that they conduct them. Privacy Impact Assessments (PIAs) were also conducted by about half (48 percent) of respondents. This presents an interesting question about nomenclature. We know that if we simply ask an up-or-down question about whether an organization uses privacy impact assessments at all, as we did in the 2017 IAPP-EY Governance Report, 70 percent say, "yes." Further, 78 percent of respondents in the 2018 Governance Report say that PIAs are part of a privacy team's remit. Yet, here, we see a clear distinction between PIAs and DPIAs. It would appear that in some cases "DPIAs" is synonymous with "PIAs," but not all PIAs rise to the level of formal DPIAs.

Not surprisingly, given that DPIA is a European term, respondents from the U.K. and the EU were more likely to report conducting DPIAs, while those from the U.S. and Canada were less likely to report doing so. Respondents working in the consumer durables sectors were also more likely than other to conduct DPIAs, while those working in the government sector were less likely to.

Coming in as the second-most common risk assessment are Vendor/Third-Party Risk Assessments, which about slightly more than half (52 percent) of respondents reported conducting. Always an important aspect of privacy and security risk analysis, vendor vetting is legally required under GDPR as well. Article 28 not only obligates controllers to select vendors that offer appropriate technical and organizational safeguards for personal data, it also compels controllers to bind processors to certain key contractual requirements as well. This has elevated the importance of vendor vetting and contractual requirements to the privacy office and in particular to the role of the DPO.

In the next tier of common assessments, we find targeted tasks: Legitimate Interest Assessments (31 percent) for organizations looking to establish a legal basis for processing; Data Breach Readiness Assessments (29 percent), for those undergoing data breach prep; International Data Transfer Assessments (28 percent); ISO 27001



HOW RISK ASSESSMENT IS DONE

Assessments (28 percent); and GDPR High-Risk Processing Assessments (27 percent), which would then trigger the formal DPIA process. These should in many respects be the same as Privacy Threshold Assessments (9 percent), but it's clear that name hasn't taken off for the process of deciding whether an official DPIA is appropriate.

Organization size was positively correlated with conducting various kinds of privacy assessments. More specifically, the more people an organization employs, the more likely it is to conduct PIAs, vendor/third-party assessments, international data transfer assessments, GDPR high-risk processing assessments, inherent risk assessments, ISO 270001 assessments, and NIST assessments. We have seen this throughout our surveying over the years: Larger organizations, as you might expect, are more likely to have mature privacy programs that engage in a variety of privacy-related operational tasks.

This is a function of having more resources available, yes, but also a function of large companies being more likely to have customers from a variety of jurisdictions around the world, and thus subject to a variety of privacy and data protection laws. The complexity of creating a privacy program that is compliant with a wide range of obligations, including those surrounding cross-border data transfer, generally necessitates a quick ramp-up in maturity and sophistication.

As we look more deeply at the effect of geography in this area, respondents from the U.K. were more likely than others to conduct legitimate interests assessments, international data transfer assessments, and GDPR high-risk assessments, and respondents from the EU (excluding the U.K.) were more likely to report conducting ISO 270001 assessments, and less likely to report conducting data breach readiness assessments and NIST assessments. This should be unsurprising given the long history of breach notification in the United States and NIST's prominent role in creating operational frameworks in the American business community.

USE OF COMMERCIAL SOFTWARE TOOLS

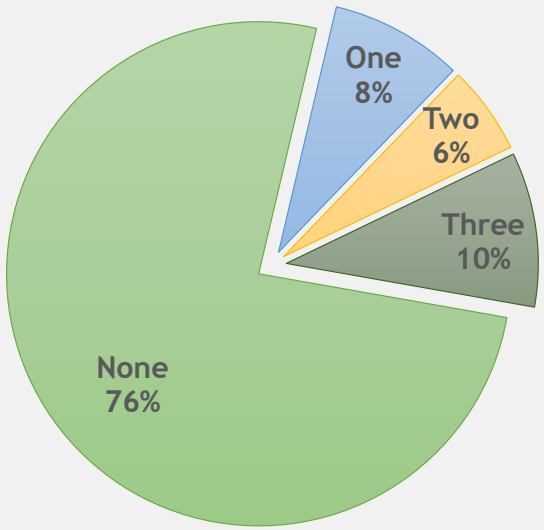
For each of the data inventory, DPIAs, and Article 30 records questions, we asked respondents about whether they use some kind of software tool designed for the privacy industry. We were also interested, however, if organizations were likely to simply buy tools for all three tasks, or if they were more likely to target specific of those tasks for tackling with some kind of software package.

In all, 24 percent of respondents use privacy tech for at least one of these tasks, but it's actually more common for an organization to use tech for all three tasks (10 percent) than for just one of the three (9 percent), with the remaining organizations using privacy tech for two of the three.

In large part, it would seem that organizations either dive in or don't.

Respondents who work at larger organizations, are based in the U.K., and are in the materials and software and services sectors tend to use more of these software tools than others, while respondents from Canada and those working in the government sector tend to use fewer of them.

USE OF COMMERCIAL SOFTWARE TOOLS FOR DATA INVENTORY/MAPPING, DPIAS, AND RECORDS OF PROCESSING



GDPR ACTIVITIES SLOW TO EMERGE,

ESPECIALLY RESPONSES TO ACCESS REQUESTS AND DATA BREACH REPORTING

Getting to the core of the research, each respondent was then asked whether they were subject to the General Data Protection Regulation (GDPR). The 17 percent of respondents who said "no" exited the survey. The other 83 percent (410 respondents), however, were given four more sets of questions that pertain specifically to their compliance with certain provisions of the GDPR and which serve to create benchmarking metrics by which organizations can measure their own programs.

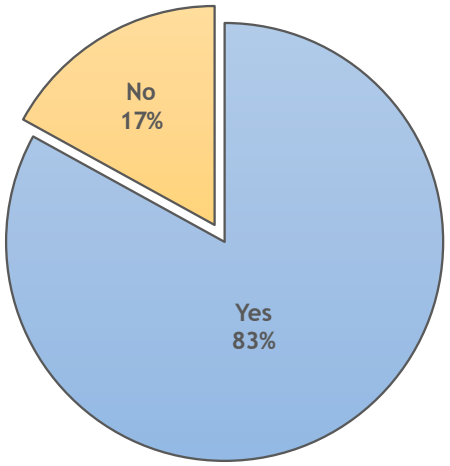
DPIAS

All respondents subject to the GDPR were asked how many DPIAs their company has completed since May 25, 2018. In large part, conducting a formal data protection impact assessment is a relatively uncommon task. DPIAs are required only when a controller is engaged in processing likely to result in a high risk to the rights and freedoms of individuals. The largest portion of respondents, 38 percent, reported having completed between one and five DPIAs since May 25. And the second largest group, comprising 17 percent of respondents, reported completing none.

Thus, more than half of all organizations subject to the GDPR have conducted five or fewer DPIAs since the GDPR came into force.

What might cause an organization to conduct more or fewer DPIAs? About 12 percent reported between 6 and 10 DPIAS, 15 percent of respondents reported having completed between 11 and 50, and an exclusive 9 percent reported having completed 51 or more. How can we explain the deviation?

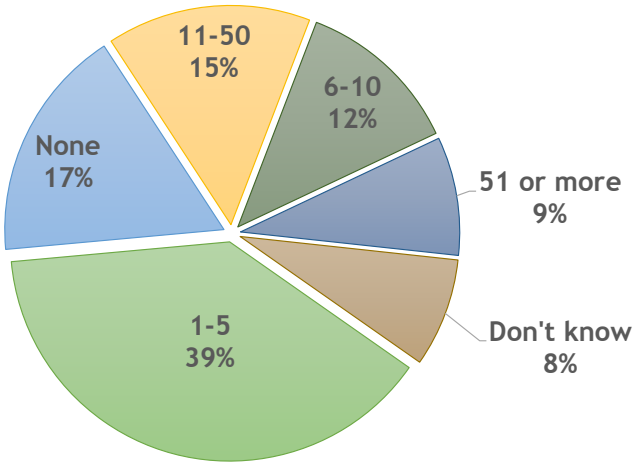
DOES THE GDPR APPLY TO YOUR ORGANIZATION?



First, organizational size is correlated with conducting DPIAs, meaning that larger organizations on average conduct more DPIAs than smaller ones. Organizations in the banking, drugs and biotechnology, and technology hardware and equipment sectors also report conducting significantly more DPIAs than others, while organizations in the education/academia, media, and nonprofit sectors report conducting significantly fewer DPIAs than others.

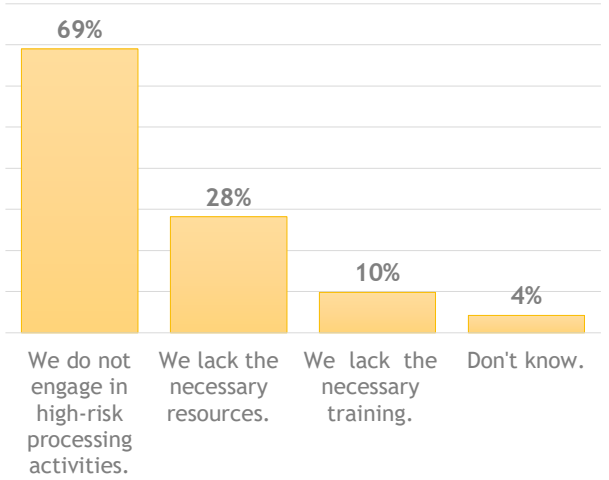
In fact, of the 17 percent of respondents who answered "None," the most common explanation for why, given by 69 percent of these respondents, was that, "We do not engage in high-risk processing activities." This would explain the correlation with the banking, drugs, and biotech industries. Another 28 percent reported lacking the necessary resources to conduct a DPIA, which might explain the education sector, which chronically suffers from lack of resources.

DPIAS COMPLETED SINCE MAY 25, 2018



About 10 percent reported that they lack the necessary training to do so, which overlaps with the lack of resources, and about 4 percent were unsure how to explain the lack of DPIAs.

REASONS FOR NOT COMPLETING DPIAS

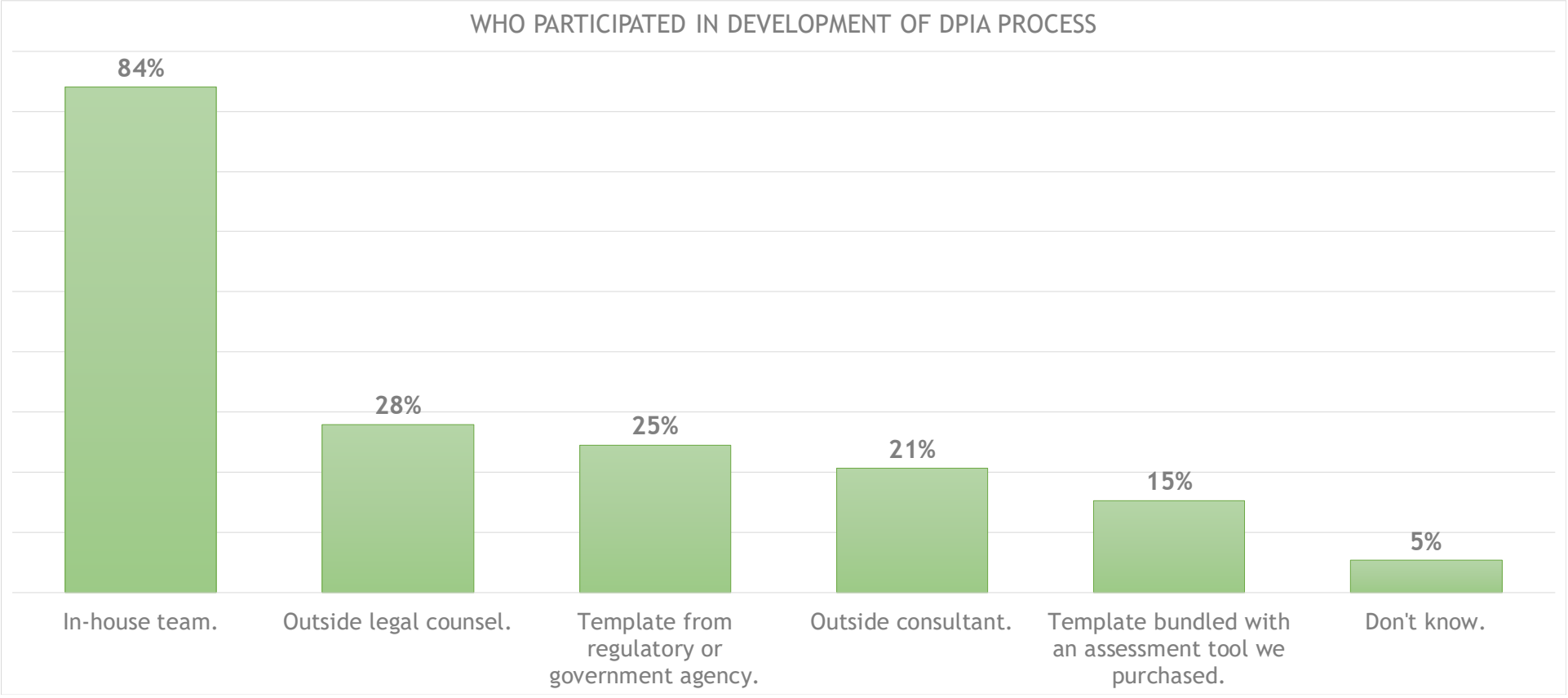


GDPR ACTIVITIES SLOW TO EMERGE,
ESPECIALLY RESPONSES TO ACCESS REQUESTS AND DATA BREACH REPORTING

Interestingly, those who reported that outside consultants and in-house teams participated in the development of their DPIA process also tended to conduct more DPIAs than others. To paraphrase from the dbuild the process, DPIAs will come.

Those who reported having completed at least one GDPR-required DPIA since May 25 were asked two follow-up questions about their DPIA process. First, they were asked who participated in its development and then the technology, if any, that's involved.

Most commonly, organizations use an in-house team to conduct DPIAs; 84 percent of respondents do. Twenty-eight percent of respondents use outside legal counsel to develop their DPIA process, and a quarter use a template provided by a regulatory or government agency (respondents could choose more than one, as teams often use a variety of inputs to create their process). About one in five respondents (21 percent) use an outside consultant, while 15 percent use a template bundled with an assessment tool they purchased.



GDPR ACTIVITIES SLOW TO EMERGE,

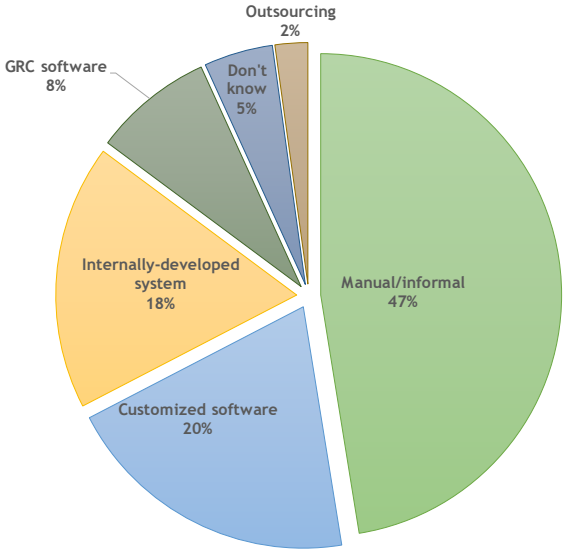
ESPECIALLY RESPONSES TO ACCESS REQUESTS AND DATA BREACH REPORTING

Regarding the primary tool used by companies to manage their DPIAs, manual/informal ones, such as email, spreadsheets, and in-person communication, were the most common, used by 47 percent of respondents. This is down considerably from 66 percent reporting using similar informal tools for privacy risk assessments in 2016.

In line with the rapid rise in technology created for privacy teams we've seen over the past three years, commercial software designed specifically for conducting DPIAs was the second most popular tool, which about one in every five respondents (20 percent) reported using as their primary DPIA tool. Again, this is a major change from two years ago, when only 6 percent of survey respondents reported using a specifically designed commercial tool for privacy risk assessments. Another 18 percent reported primarily using a system developed internally (compared to 36 percent in 2016), and 8 percent reported using GRC software customized for conducting DPIAs (compared to 17 percent in 2016).

A small portion of the respondent base, about 2 percent, reported outsourcing their DPIA process entirely (versus 7 percent two years ago), but this is clearly not a common practice.

PRIMARILY TOOL USED TO MANAGE DPIAS



GDPR COMPLIANCE REPORTS

In addition to DPIAs, the GDPR also mandates what have become known as "Article 30 reports," essentially documentation of the organization's data processing activities. Many organizations have chosen to create a separate report, or analysis, of each separate processing operation, thus creating a stockpile of "reports," which any regulator could peruse to understand an organization's activities. This is part and parcel of an accountability framework, also mandated by the GDPR. If an organization is going to prove it is GDPR compliant, it must first be able to show which data is being processed, the legal basis for doing so, and so on.

The findings of our research would suggest that this practice is still relatively in its infancy. The most common response was between one and five (24 percent) reports and another 15 percent of respondents said their company has created none. However, "Don't know" was the second most common response (19 percent). As these activities are so new, there is the obvious issue with nomenclature: Could some organizations have consolidated all of their Article 30 work into one single report that documents all of their processing operations? Might some organizations have interpreted "report" to mean a report to a data protection authority of some kind?

It's hard to say.

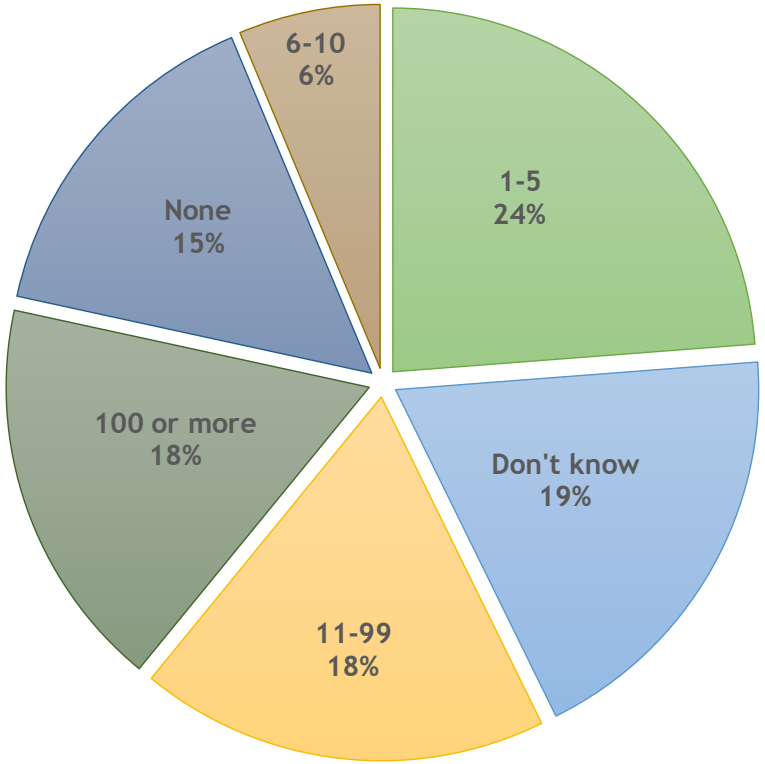
Because, on the other end of the spectrum, we have 18 percent of respondents reporting that their organization has created between 11 and 99 Article 30 Reports, and another 17 percent say they have created 100 or more. There's clearly a wide range of activities in the marketplace.

GDPR ACTIVITIES SLOW TO EMERGE,

ESPECIALLY RESPONSES TO ACCESS REQUESTS AND DATA BREACH REPORTING

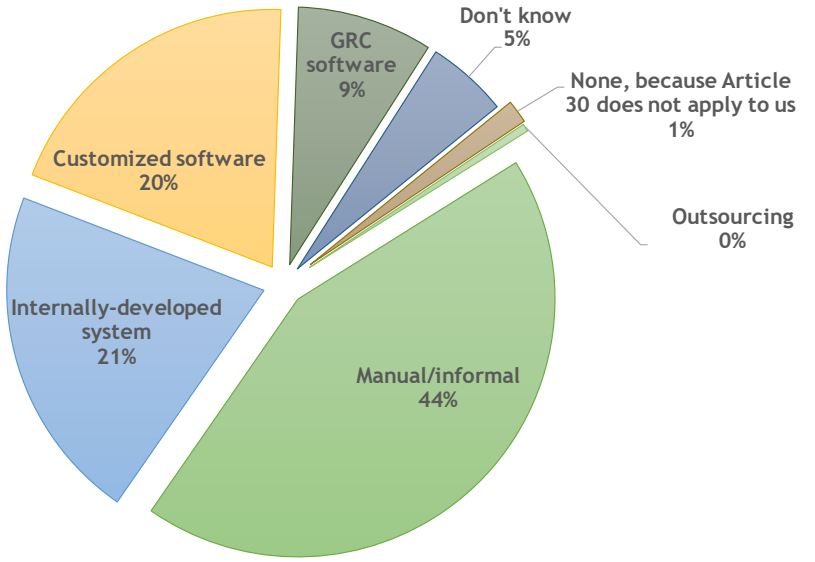
As with conducting DPIAs, organizational size is significantly correlated with creating Article 30 reports, in part because the rule exempts organizations with fewer than 250 employees. Respondents based in the EU (non-U.K.) also created more of them, whereas respondents based in Canada created fewer. Respondents who work in the semiconductors and technology hardware and equipment sectors also reported creating more Article 30 reports than others, though it's unclear why that might be.

ARTICLE 30 REPORTS



Regarding the primary solution used to maintain records of processing, responses again indicate that informal tools, such as email, spreadsheets, and in-person communication, were the most commonly used solution. After that, about one in five used either a system developed internally (21 percent) or commercial software designed specifically to maintain records of processing (20 percent). Another 9 percent reported primarily GRC software that is customized to maintain records of processing. Less than one percent of respondents outsource their maintenance of records of processing activities, and less than two percent do not maintain records of processing because Article 30 does not apply to them. Lastly, five percent of respondents were not sure what solution is primarily used to maintain their records of processing.

PRIMARY SOLUTION TO MAINTAIN RECORDS OF PROCESSING



GDPR ACTIVITIES SLOW TO EMERGE,
ESPECIALLY RESPONSES TO ACCESS REQUESTS AND DATA BREACH REPORTING

DATA SUBJECT ACCESS REQUESTS

While organizations, themselves, largely dictate how many DPIAs and Article 30 records they create, depending on the nature of their business and operations, they have less control of the volume of data subject access requests they might encounter. Obviously, the nature of an organization's operations will have some effect on the number of DSARs, as they're called, they encounter. Consumer-facing, or particularly data-driven businesses are likely to have more than those in the B2B business, but every organization has employees, and public entities might have more DSARs than many for-profit businesses.

To help organizations better understand how their own experience relates to others, and allow for the fact that many jurisdictions already had data subject access requests as a normal course of business before the GDPR, we focused on asking for the volume of DSARs organizations have experienced on a monthly basis since May 25, 2018, and what method they were using for processing those requests.

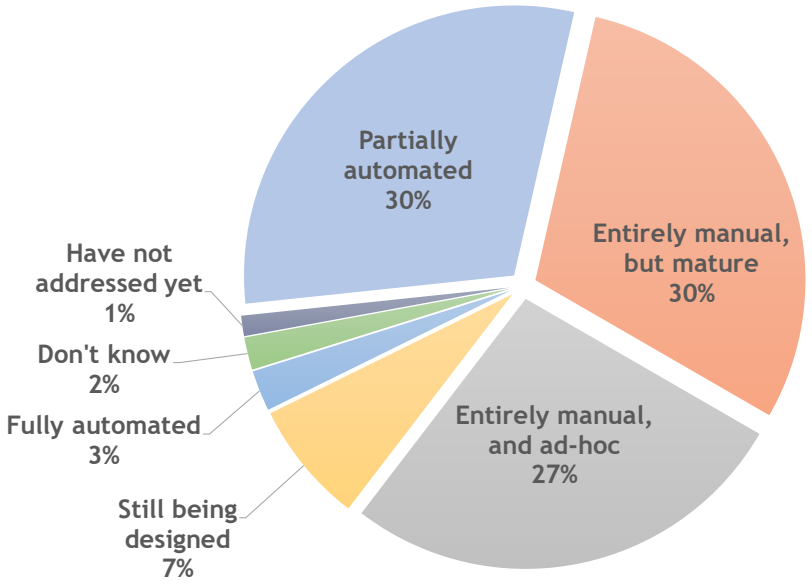
As many may have experienced, a data subject access request can be extremely time consuming, depending on its nature. An employee's request can be particularly complicated. In this research, however, we did not differentiate between employees and data subjects outside the organization.

We did find that organizations are doing their best to bring some structure to the process. Nearly a third (30 percent) have at least partially automated the process, but just two percent say the process is entirely automated. Many organizations would likely be interested in how they've accomplished that.

For most, the process is either entirely manual but mature (30 percent) or entirely manual and ad-hoc (27 percent).

This means many organizations are spending significant human capital on satisfying requests, as DSARs are not rare and most respondents are seeing a steady stream, if not an overwhelming amount.

HOW DSARS ARE ADDRESSED



Almost half of respondents (47 percent) said that they have been receiving about one to 10 per month, with another 16 percent receiving somewhere between 11 and 99 per month. However, as many as 6 percent have received between 100 and 499 thus far, and 3 percent report receiving 500 or more DSARs per month since May 25, 2018.

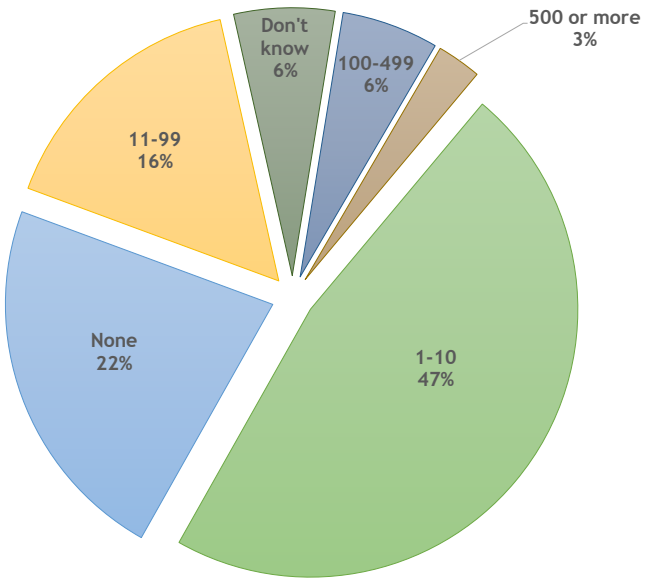
And yet 22 percent of those who say they are subject to the GDPR say they have received none whatsoever.

Continuing the trend, larger organizations reported receiving more DSARs per month than smaller organizations. We also see the expected breakdown by market sector, as respondents working in the consumer durables, media, retail, and tech sectors also reported receiving significantly more DSARs, while respondents working in the business services and supplies, education/academia, and health care report receiving significantly less DSARs than others.

GDPR ACTIVITIES SLOW TO EMERGE,

ESPECIALLY RESPONSES TO ACCESS REQUESTS AND DATA BREACH REPORTING

DSARS RECEIVED PER MONTH SINCE MAY 25



Further, those 22 percent who said they hadn't received any DSARs were asked why they thought that might be. All of these respondents reported that the reason their company has not processed any DSARs is because no one has submitted one – the options for "we don't have a process in place" or "don't know" were not selected.

In order to get some kind of baseline for how many DSARs organizations might expect to be seeing each month, respondents were also asked to estimate the number of data subjects whose data they process in their capacity as a data controller. The median number of data subjects' data processed was 87,500. The highest number was 5 billion (one response of 28.5 billion was eliminated because, well, that's impossible, unless they've found some non- Earthlings with data to process). Respondents working in the construction and software and services sectors reported processing the data of more data subjects than others.

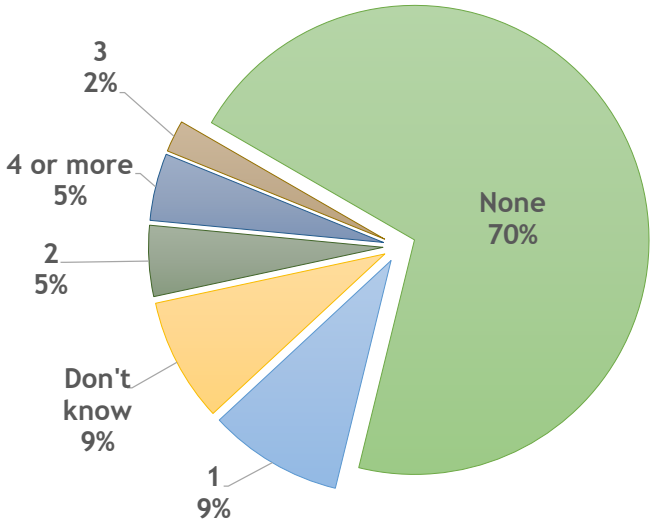
As you might imagine, this produced a wide variation in numbers of DSARs per data subject, but the median number is likely fairly representative of the experience of the average company: 7 DSARs per million data subjects per month.

BREACH NOTIFICATION MINIMAL POST-GDPR

In the final portion of our survey, respondents were asked how many data breach notifications their company has filed with an EU supervisory authority since the GDPR's go-live date. The large majority (70 percent) reported having filed none. Of the rest, about 9 percent reported having filed one, 5 percent reported filing two, 2 percent reported filing three, and 5 percent reported having filed five or more data breach notifications with an EU supervisory authority.

We know from prior research that roughly four out of 10 privacy professionals report experiencing an information security incident

DATA BREACH NOTIFICATIONS FILED WITH EU SUPERVISORY AUTHORITIES SINCE MAY 25



(defined as the "unauthorized disclosure of data") over a two-year span. Although the GDPR broadly defines security incidents as a personal data breach, it does not require notification of the supervisory authority unless the controller concludes there is a risk to individuals' rights and freedoms. We can therefore assume that some incidents – breaches – occurred that organizations determined did not merit notification.

When we further asked how many breaches rose to the level of notifying data subjects, required with the breach is likely to create a "high risk" to individuals' rights and freedoms, the response in many ways mirrored the question previous, with only slightly more respondents (75 percent) saying they had sent none.

GDPR ACTIVITIES SLOW TO EMERGE,

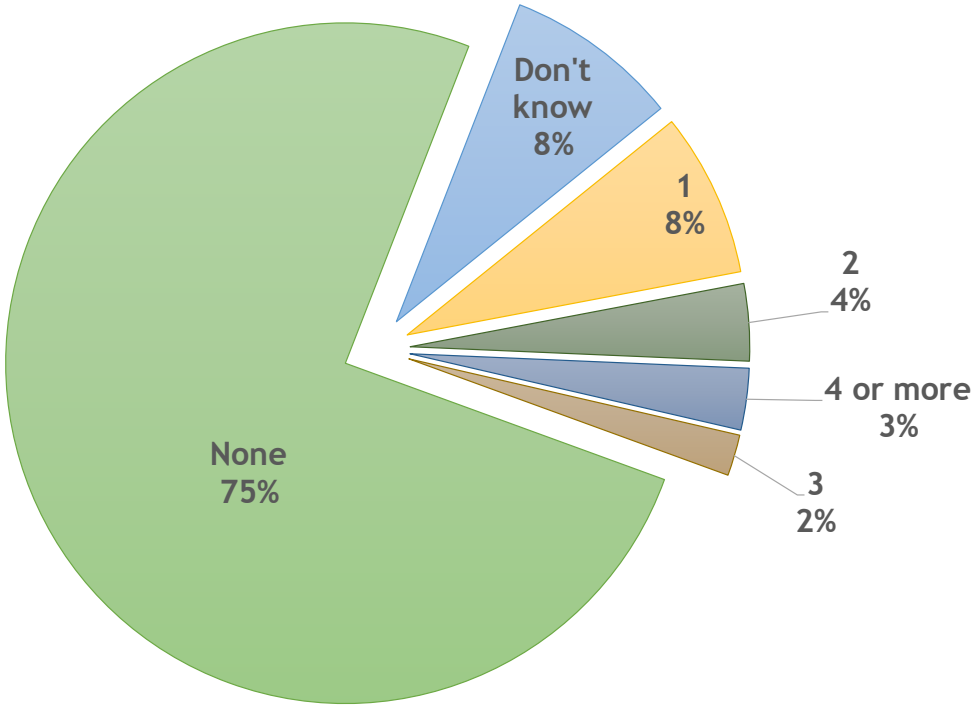
ESPECIALLY RESPONSES TO ACCESS REQUESTS AND DATA BREACH REPORTING

Eight percent said they had sent one notification to data subjects, 4 percent said they had sent two, 2 percent said they had sent three, and 3 percent said they had sent four or more data breach notifications to data subjects since May 25. Given breach notification is new to the EU, this is a significant number – as of yet we have not seen enforcement operations from DPAs in this area.

In terms of who has been affected, larger organizations were far more likely than smaller ones to file data breach notifications with EU supervisory authorities. Although about 23 percent of respondents within the overall sample reported filing at least one data breach notification to a supervisory authority, 27 percent of respondents from larger organizations (1,001 or more employees) reported filing at least one, whereas only 16 percent of respondents from small organizations (1-1,000 employees) filed one or more. Respondents working in the banking, insurance, telecommunications services, and trading sectors also report filing significantly more data breach notifications with EU supervisory authorities, while those in the software and services sector reported filing significantly fewer.

Organizations based in the EU (non-U.K.) also reported sending significantly more data breach notifications to data subjects since May 25 than others. Whereas about 18 percent of respondents in the overall sample reported sending at least one data breach notification to data subjects, 25 percent of respondents in the EU (non-U.K.) reported doing so. Organizations in the construction, government, insurance, telecommunications services, and trading sectors were also more likely than others to send data breach notifications to data subjects, while organizations in the software and services sector were significantly less likely to report sending data breach notifications to data subjects.

DATA BREACH NOTIFICATIONS SENT TO DATA SUBJECTS SINCE MAY 25



CONCLUSION

While it could likely go without saying, the data in this report makes it clear: The General Data Protection Regulation has changed the way privacy programs operate. They are completing more tasks, they have a better understanding of their data holdings, and they have invested in more technology to help them with their work.

However, the GDPR is not, as some feared, creating an unmanageable flood of work. The average organization is likely able to field the 7 DSARs per million data subjects they receive per month, and getting through a DPIA or two a month does not seem insurmountable.

But that doesn't mean privacy teams are satisfied simply to muddle through. There is a clear case to be made for some organizations that a dose of technology and automation is warranted, and we are seeing steady acceptance of privacy technology as the marketplace begins to develop.

It will be interesting to see if this trend continues, just as it will be interesting to see how operational tasks under the GDPR evolve. Will we see less DSARs as data subjects no longer feel the need to test out their new rights? Or will we see more DSARs as data subjects become increasingly aware of those rights? Will DPIAs become less common as the marketplace better understands what is meant by "high risk," or will they become more common as data protection authorities audit operations and issue more guidance on the risks to rights and freedoms.

Look for continuing research to answer these questions and more.

IAPP.ORG

TRUSTARC.COM