IAPP-EY Annual Privacy Governance Report 2019

iapp

EY

Building a better
working world

Introduction

Regulators flexed their muscles in 2019, sending shock waves into corporate boards with announcements of the largest privacy and data protection fines in history.

The U.S. Federal Trade Commission's $5 billion settlement with Facebook is more than double the total of all privacy fines, globally, to date.. It comes years after the Cambridge Analytica scandal was revealed, and underscores the FTC's determination to be seen as a strong privacy regulator. It was accompanied by a less-grand but no-less-legally-significant fine by the U.S. Securities and Exchange Commission, which slapped Facebook with $100 million for failing to accurately disclose to investors privacy risks in its public filings with the SEC.

In addition to the fine, Facebook was also required to create an independent privacy committee of the board of directors, comprising independent members and charged with oversight, responsibility and accountability for the company's privacy program.

In the weeks prior to the Facebook settlements, the U.K. Information Commissioner's Office announced notices of intent to fine nearly $230 million against British Airways and $125 million against Marriott for inadequately safeguarding personal data in their systems. Earlier this year, France's data protection authority, the CNIL, fined Google more than $50 million for its consent collection practices.

And yet even among the privacy experts (those who took this year's IAPP-EY Privacy Governance Survey), compliance with comprehensive privacy law and regulation is proving very difficult indeed. More than 50% of those taking the survey who are responsible for compliance with the EU General Data Protection Regulation report their firms are at best "moderately" compliant and at worst not at all compliant. Only 9% report full compliance, while 36% optimistically call themselves "very compliant."

J. Trevor Hughes
CIPP,
CEO and President,
IAPP

Angela Saverice-Rohan
CIPP/US,
EY Americas Leader
for Privacy

The study was sponsored by EY. All copyrights remain those of the IAPP and the IAPP retained all editorial oversight.

This is not a sign that respondents don't take privacy seriously — we know that firms invested heavily in their privacy teams in 2017 and 2018. In lockstep, IAPP membership eclipsed 50,000 members in 2019 , reflecting 100% growth in just under two years. Instead, it demonstrates that even one year after the GDPR took effect, privacy and data protection pros are still struggling to keep up.

The task is monumental. The consequences of failure are significant.

The good news is that as regulators work to clarify how the law should be implemented and to flex their enforcement muscles, executives and boards increasingly engage in privacy program management and data governance.

Meanwhile, even though GDPR compliance is a task that is never complete, we see privacy professionals start to shift their attention from the GDPR to the California Consumer Privacy Act, which comes into effect January 2020. Although many have waited to see if the law would be pre-empted by a comprehensive federal law in the U.S., as the year winds down with no legislation, it's time for organizations to take the CCPA seriously.

All this means more work for in-house privacy pros, as well as the outside counsel, consultants and tech vendors that support them.

Contents

Executive Summary

Now in its fifth year, the IAPP-EY Privacy Governance Report has evolved over time, along with the privacy profession itself.

This year, almost as many of the 370 respondents to the survey hailed from the European Union as from the United States. This reflects the growth of the privacy and data protection profession in the EU in reaction to the GDPR. The GDPR has driven growth in privacy-pro ranks in the U.S., as well.

And yet, have we seen a leveling-off of business investment in privacy post-2018? Budgets and staffing are flat this year, even though GDPR compliance has not yet been widely achieved.

One GDPR responsibility most have met, in response to Article 37, is to appoint a data protection officer — nearly three out of four organizations subject to the regulation have appointed a DPO, whether obligated by the law or not. Indeed, one-third of all survey respondents hold the DPO title. Among those DPOs from the EU, most (69%) hold the top privacy role for their firm. They often have direct reporting lines to the board of directors, as well.

High on the list of privacy concerns for the board — following data breach — is legal and regulatory compliance, especially with the GDPR. The regulation has had such a massive impact on data management practices globally that it has become, in many respects, the de facto global standard for privacy. Compliance with privacy laws and regulations tops privacy professionals' priority list — 41% of respondents name it as their highest priority. GDPR compliance is far and away the top priority for those in the EU (58% chose it), whereas only 11% of U.S. respondents selected it as number one. On the flip side, 46% of U.S. respondents named "compliance (beyond the GDPR)" as their highest priority, with only 30% of EU respondents selecting it.

With all this attention to compliance, fewer than half of all respondents report being "very" or "fully" compliant with the GDPR. Among EU respondents alone, 43% report they are only "moderately compliant" with the GDPR, even when GDPR compliance is their primary responsibility. One in 10 admit they are only "somewhat" compliant with the GDPR.

Privacy pros in the U.S. are less likely than their EU counterparts to be DPOs and more likely to have multiple privacy responsibilities beyond GDPR compliance. They report working on vendor management and even "ethical decision making" more often than those in the EU.

Other major takeaways from this year's report:

- Among respondents whose organizations must comply with the GDPR, 38% have reported a breach this year (compared to just 16% in 2018), and 22% have reported more than 10.

- Nearly all respondents (90%) report their firms rely on third parties for data processing, and the top method for ensuring vendors have appropriate data protection safeguards is "relying on assurances in the contract" (named by 94% of respondents). More than half (57%) use questionnaires, while only one in four conduct on-site audits.

- The most popular method, by far, for data transfers outside the EU is use of standard contractual clauses (88% of respondents), followed by compliance with the EU-U.S. Privacy Shield arrangement (60%).

- For those respondents transferring data from the EU to the U.K. (52%), 91% report they intend to use SCCs for data-transfer compliance after Brexit.

- More than half of respondents (56%) named "locating unstructured personal data" as the most difficult issue in responding to data subject access requests (including access, deletion, and rectification requests), far ahead of "monitoring data protection/privacy practices of third parties" (36%), data minimization (28%), or developing a centralized opt-out tool (25%).

- Manual methods are still common for activities like data inventory and mapping and responding to subject access requests, with spending on privacy technology significantly higher among U.S. respondents than those from the EU.

All in all, we find privacy professionals happy in their jobs. In our first-ever "happiness indicator," 33% of privacy professionals assigned the highest satisfaction score to their jobs ("very satisfied"), with another 49% selecting the next highest score ("satisfied"). Only 8% said they were either unsatisfied or very unsatisfied.

Nearly half of all respondents (45%) expect privacy to bring them new opportunities, while another 38% are at the peak of their careers.

With all this attention to compliance, fewer than half of all respondents are "very" or "fully" compliant with the GDPR.

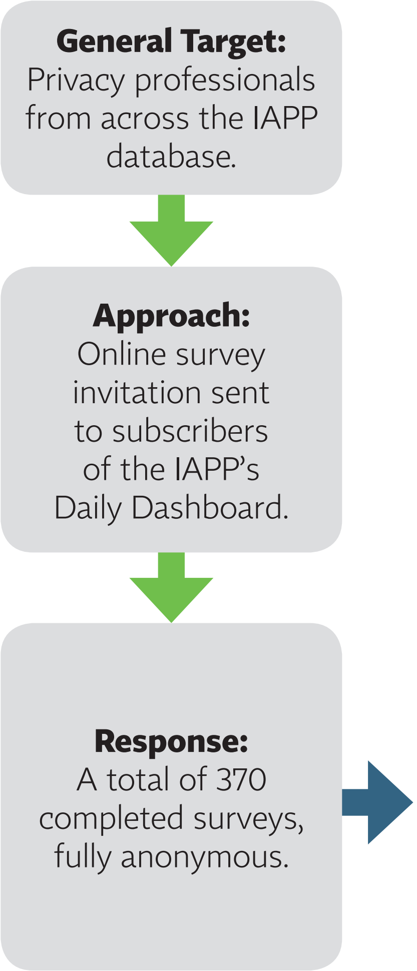
Contents

Research Objectives

The overarching goals of this research are to:

- Understand privacy program structures (e.g., budget, staffing, career development) within various organizations.
- Measure compliance with the EU General Data Protection Regulation, with special attention to data-subject requests and data transfers.
- Examine potential responses to Brexit, preparedness for legal obligations, and factors influencing an organization's decisions on data use.
- Identify recent trends in the daily routines of privacy and data protection professionals.

Method



General Target: Privacy professionals from across the IAPP database.

Approach: Online survey invitation sent to subscribers of the IAPP's Daily Dashboard.

Response: A total of 370 completed surveys, fully anonymous.

The survey asked a variety of detailed questions about privacy budgets, staffing, leadership and team responsibilities. Moreover, general questions on GDPR compliance, data transfers, the potential impact of Brexit on privacy operations, and DSARs were included.

WEIGHTING: The 2019 results were statistically weighted to match the employee size distribution of firms answering the 2018 survey. This matching allows us to make better comparisons between findings from the two years.

SEGMENTS: Segments of the sample with fewer than 30 respondents have been flagged as "small sample size." Results from these segments should be considered directional and suggestive, rather than statistically definitive.

SIGNIFICANT DIFFERENCES: Some findings in the report are flagged as "statistically different" from either 2018 or from other segments. A significant difference is one that is large enough (taking account the base size of respondents) that we can feel at least 95% confident that it's the results of an actual difference in the marketplace (versus mere sample fluctuation).

Glossary

CIPM: Certified Information Privacy Manager — a certification offered by the IAPP.

CIPP: Certified Information Privacy Professional — a certification offered by the IAPP.

CISO: chief information security officer.

CISSP: Certified Information Systems Security Professional — a certification offered by (ISC)2.

Customer target: For the purposes of comparison, we ask respondents to categorize themselves as primarily business to-business, business-to-consumer, or a blend of both sales channels.

Director-level: Certain question sets in the survey were only shown to those respondents who identified themselves as "directors" or higher within their organization. "Director" was defined as a level in the organization between the standard manager level and vice presidents or the C-suite.

Full-time versus part-time: You will see references to "full-time" and "part-time" privacy employees. This is not intended to mean that "part-time" employees are not full-time employees of the organization. Rather, it means that they spend only part of their time on privacy matters.

In-house privacy professional: With this terminology, we are referring to those doing the work of privacy as an employee of an organization that controls or processes data. We are excluding those who sell outside privacy services, such as attorneys, consultancies or privacy tech vendors.

ISO 27001/2: The International Standards Organization has developed these standards for information security management and controls.

Mature: We ask respondents to self-report where they are on the privacy program maturity curve. They answer "early stage," "middle stage," or "mature."

PIA: Privacy impact assessment — this should be thought of as synonymous with data protection impact assessment, but not specific to the DPIAs as outlined in the GDPR.

Privacy leader: We ask respondents to self-report whether they are the "privacy leader," that is, the most senior officer responsible for privacy in an organization, having responsibility for oversight of the privacy program. As we demonstrate in the report, this could be anyone from the CEO to a CPO or a DPO.

Regulated versus unregulated industries: For the purposes of comparison, we categorize traditionally "regulated" industries as those in health care or financial services.

SOC2 Privacy: Service Organization Controls are reporting platforms developed by the AICPA. SOC2 are reports "relevant to security, availability, processing integrity, confidentiality, or privacy," for which AICPA has developed "Trust Services Criteria."

Contents

How the Job of Privacy Is Done

Profile of a privacy pro: 2019

The IAPP eclipsed 50,000 members globally in 2019. Responses to our annual Privacy Governance survey reflect the global and professional diversity of our community.

We identify the following trends:

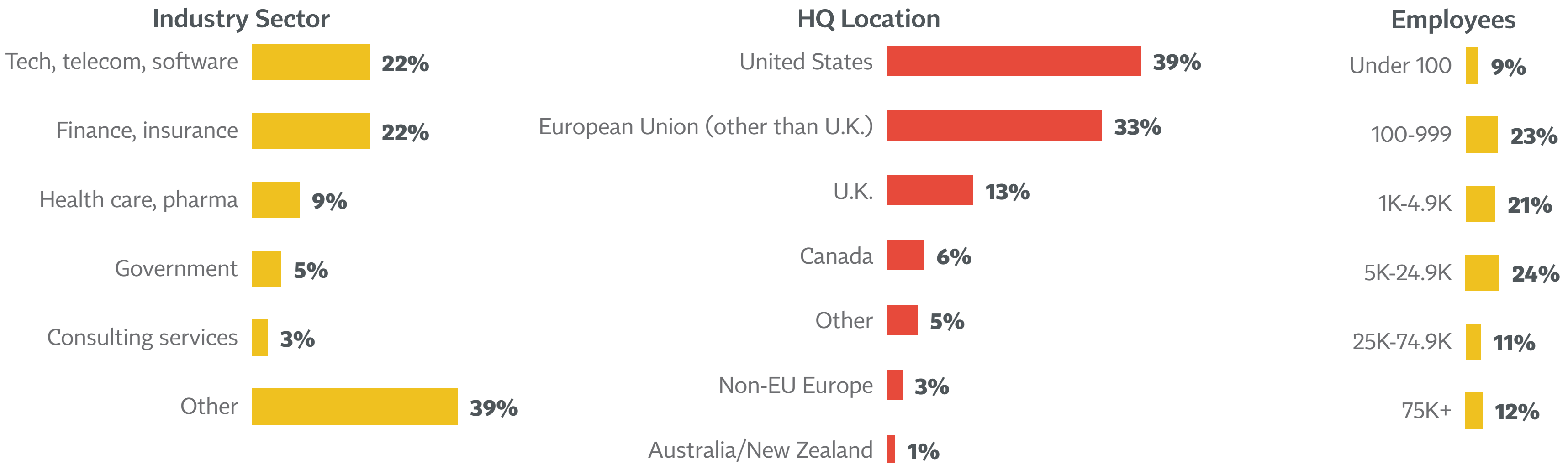
- The GDPR, which took effect in May 2018, has been a massive driver of growth in the privacy and data protection profession not only in the EU — our fastest-growing region — but also in the United States and around the globe.

- Although some privacy professionals have used the growing regulatory pressure on companies to leap ahead professionally (more on that coming up next), the greater growth areas are in the "meaty middle" of the corporate hierarchy. Managers are the largest segment of respondents to our survey this year, with a small dip in the number of directors.

- Lawyers, general counsel in particular, are responding to our survey more often than in past years, signaling either promotion of privacy pros to the GC role or (more likely) adoption of privacy responsibilities by GCs who previously did not pay as much attention to this issue.

- As is typical of past years, we see respondents from a range of industries in this year's survey, and they tend to represent companies of all sizes. Financial institutions have long faced regulatory pressure for data handling practices, but tech companies (such as software and hardware producers, cloud providers, etc.) have not. The GDPR changes that, as does the soon-to-be-implemented CCPA. As comprehensive, omnibus laws, they target all sectors of the economy, and we see that distribution in our rank and file.

Company Profiles

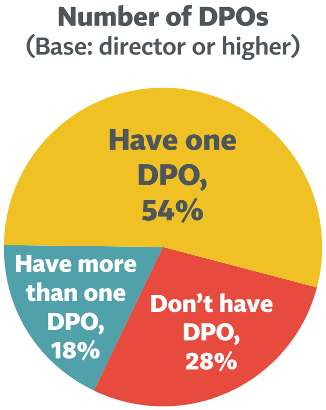


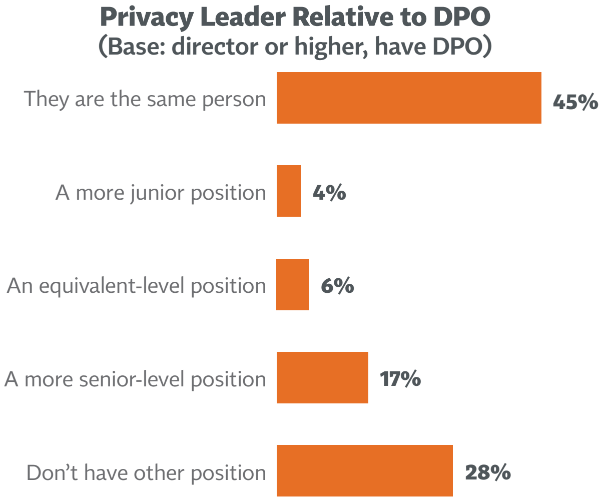
Growth in DPO ranks

By the one-year anniversary of the GDPR's implementation date, the IAPP estimated that about 500,000 organizations have already registered DPOs with data protection authorities in the EU. This staggering number far exceeded pre-GDPR estimates and demonstrates the enormous economic impact of the GDPR, as well as the explosive growth in privacy and data protection as a valued professional role.

Of the 370 respondents to this year's survey, 72% report that their firm has a DPO. Among those who do, 75% have just one DPO, while 25% have more than one.

Indeed, one out of three respondents is a DPO. Most of them (28% of all respondents) hold this title because it's mandated by Article 37 of the GDPR, but some (5% of all respondents) have the title even if it's not required for their organization.





If an organization has a DPO, it's more likely than not (62%) that that person is also the organization's privacy leader. If we isolate EU respondents, it's even more likely (69%) that the DPO is the privacy leader, whereas in the U.S. only 43% of privacy leaders are also the DPO, while 31% of privacy leaders are senior to the DPO.

DPOs are privacy leaders more often in smaller firms (by employee and by budget), work in less-mature privacy programs, and have more responsibility for GDPR compliance but much less CCPA responsibility, than in firms where the DPO is not the leader.

Significant rise in reported breaches

The GDPR defines "breach" very broadly to include any unauthorized disclosure of personal data. It requires notification to the supervisory authority unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects. This broad definition of personal data breach, combined with notification-by-default, is likely the reason for the growth in reported breaches in this year's report, rather than, for example, an increase in cyberattacks.

The number of respondents indicating they have reported a breach more than doubled this year — 38% compared to 16% in 2018 — among respondents whose organization must comply with the GDPR. A majority of respondents

Reported security breach to lead authority

U.S. HQ	22%
EU HQ	52%

continued on xiii

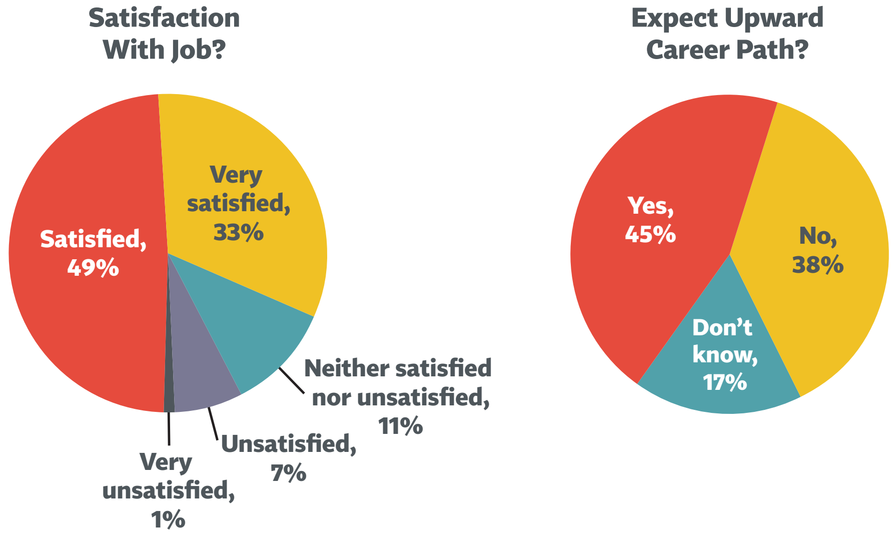
Privacy Leadership

As a career, privacy offers upward mobility to many individuals. Among respondents, 45% expect advancement in their career paths.

If you're already a privacy leader, you more likely than not hold the title of chief privacy officer. Among respondents with privacy leader responsibilities, 35% are CPOs; another 35% are "other." DPO is the title of just 25% of privacy leaders.

Privacy leaders are also likely to be the chief privacy counsel (31% of privacy leaders have this role), assuming the organization has one (42% of respondents don't). They are unlikely to be the chief information security officer; it is the same person in only one in 10 cases. But privacy leaders tend to look horizontally on the corporate ladder at the CISO position (in 39% of cases they are an equivalent level position). By contrast, privacy leaders are almost never filling the chief technology officer role (only 4% do), and they very commonly (51%) serve in a role junior to the CTO, with one in four holding an equivalent-level position.

Privacy pros generally happy in their jobs and expect promotion



This tells us that information security merges slightly better with the privacy role than a pure technology function, and yet neither is more likely than not coupled with privacy, and privacy still (generally speaking) is not yet reaching the same corporate ranks as its older professional "cousins."

continued from xii

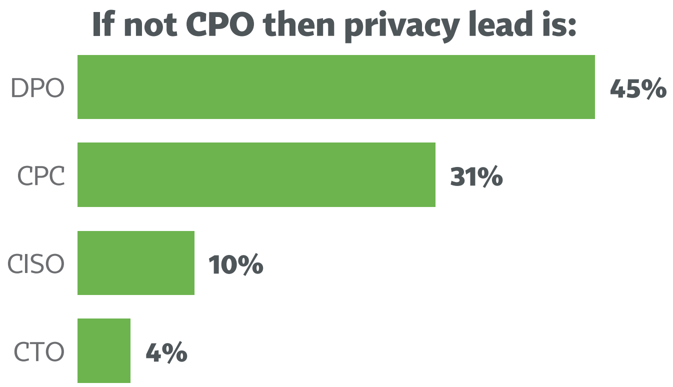
from firms with EU headquarters admitted they have notified their lead supervisory authority of a personal data breach in the last year.

Most respondents who have reported a breach (63%) reported fewer than five; but a remarkable 22% have reported more than 10 breaches. As discussed in the IAPP's "GDPR at One Year" white paper, EU DPAs collectively received more than 89,000 data breach notifications during the first year of GDPR implementation. This might be a sign of over-compliance by organizations fearful of fines and investigations.

To date, however, very few of these breaches have resulted in fines. Only 2% of survey respondents — statistically insignificant at this point — report having been fined for a reported security breach. Indeed, with all the things DPAs have to deal with, they must set enforcement priorities. Perhaps the British Airways and Marriott fines are outliers. As discussed in the white paper, some DPAs, such as the ICO, have "chosen to focus on working with the business community to address potential problem areas rather than automatically resorting to fines and enforcement actions."

That said, privacy leaders also tend not to report to CISOs or CTOs. Their bosses hold a variety of titles, nearly evenly split among general counsel (25%), chief executive officer (23%), chief compliance officer (22%) or a director (22%), with another one in five reporting to "other" (21%).

Noticeably, those who seek positions closest to the top (or at least with the most prestigious titles) will have the best luck in the U.S. C-Suite and General Counsel (GC) titles for privacy professionals also are most likely in firms with the smallest privacy budgets.



Role of the Board

The role of the board of directors has always been important to privacy governance. But the FTC further elevated the board's privacy role in its recent settlement order with Facebook over the Cambridge Analytica matter.

In that case, the FTC not only levied on Facebook a $5 billion fine, but also required the company's board to create a special independent privacy committee to oversee and take responsibility for the company's privacy program. At the same time, the SEC reprimanded Facebook for not disclosing to its investors the risk that its customers might suffer privacy harms and ordered payment of $100 million as a fine.

Although such numbers are not as significant to a company with annual revenue exceeding $50 billion, as they might

The controller/processor relationship

One of the GDPR's compliance complexities is its bifurcation of the world between controllers and processors, with contractual obligations and shifting liabilities depending on one's role.

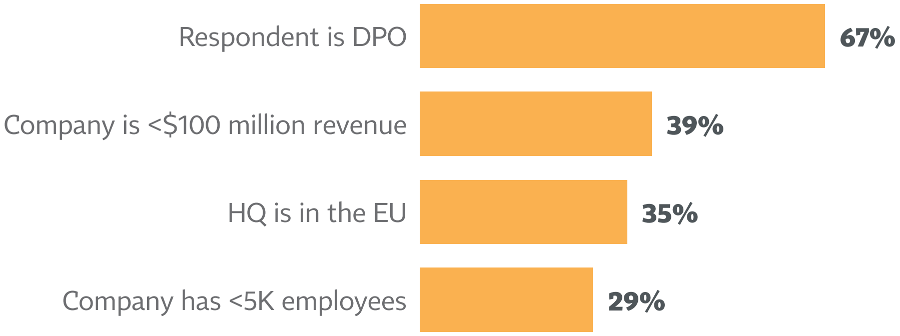
A controller determines the purposes and means of data processing. The quintessential controller is the organization that has the direct relationship with customers and collects personal data from them. Traditional B2C businesses are nearly always controllers and are rarely strictly processors. B2B organizations, however, often play the processor role, such as a cloud storage provider, but not necessarily for all purposes. They remain controllers with respect to their client's business contact information and with data of potential leads, as well as with employee data.

Blended companies (B2B and B2C) are often challenged with defining their role, and it can change depending on what deal is on the table. This requires expertise, negotiation, and contract-drafting skills and thus often requires a larger privacy team. Our research shows that "blended companies" have the highest reported numbers across the board on privacy team responsibilities, as well as budgets and staffing. They also tend to receive the most DSARs.

Outsourcing data processing is by far and away the norm. Nine out of 10 companies use another company to process data. For years, organizations have vetted their

continued on xv

Privacy lead most likely reports to the board if:



otherwise be they are eye-catching nonetheless and should result in greater attention to privacy issues at the highest corporate levels.

Article 37 of the GDPR requires the DPO to have reporting lines to the highest levels of management. Even within organizations where the DPO is not the privacy leader, 20% of DPOs nonetheless report directly to the board of directors. Consistent with that finding, our data suggests that boards in the EU are more likely to have direct oversight of privacy issues than those in the U.S. (35% versus 10%).

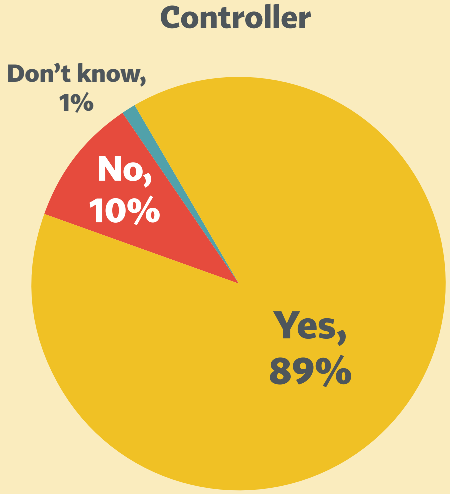
In the IAPP's annual Privacy Risk Study, we identified that risk of data breach is the highest privacy concern disclosed in companies' annual filings with the U.S. SEC (Form 10K). This matches our survey respondents' top choices of topics reported to their boards, with 68% noting that data breach is the number-one issue. A close second is the status of compliance with the GDPR, with 64% reporting to the board. This issue too is starting to be disclosed in Form 10K filings. Indeed, the past two years' Privacy Risk Study reports show marked increase in concern over regulatory enforcement for privacy noncompliance, as well as the threat of litigation.

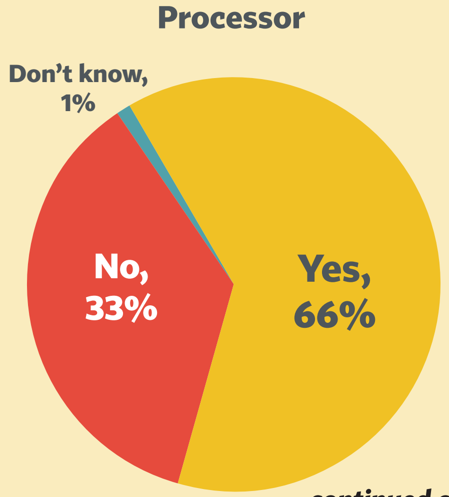
Plans and strategies to prepare for the CCPA prior to its January 2020 implementation rank far lower as board-level issues (just 23% of respondents named them) in the first year that the Governance Survey has queried this issue. We anticipate growth in CCPA compliance as a board-level concern in 2020, especially if no federal law is passed to pre-empt the CCPA and if the California Attorney General launches enforcement actions. This is an area to watch in the coming months.

continued from xiv

data processors according to attention to privacy and security concerns, but these obligations are never more important than now. Article 28 of the GDPR requires careful selection of a processor, contractual provisions providing assurances about data safeguarding and cooperation with DSARs, and ongoing monitoring for compliance.

Visiting a vendor, and even just conducting phone conversations, is labor intensive and potentially cost prohibitive. Only around one in four respondents (26%) report





continued on xvi

Privacy Pro Responsibilities

Organizations often hire privacy professionals not just to safeguard data because it's the right thing to do, but also because laws and regulations require them to offer consumers transparency, control, rights of access and deletion. It is compliance with privacy laws and regulations that tops privacy professionals' priority list, with 41% of respondents naming it as their highest priority. Next on this year's priority list is compliance with the GDPR specifically, named by 31% of respondents as their top priority overall. Far less likely to be a top priority — with only 11% selecting it first — is meeting business partners' expectations, followed by safeguarding data from attacks and threats, which was listed first by only 10% of respondents.

When we compare respondents in the EU to those in the U.S., we find that GDPR compliance is far and away the top priority for those in the EU (58% chose it), whereas only 11% of U.S. respondents selected it as number one. On the flip side, 46% of U.S. respondents named "compliance (beyond the GDPR)" as their highest priority, with only 30% of EU respondents selecting it as number one. U.S. respondents are significantly more likely than their EU counterparts to put business partner expectations on the priority list (14% to 7%), and the gap is even wider — 16% for U.S. respondents to just 3% of those in the EU — when prioritizing safeguarding data from threats.

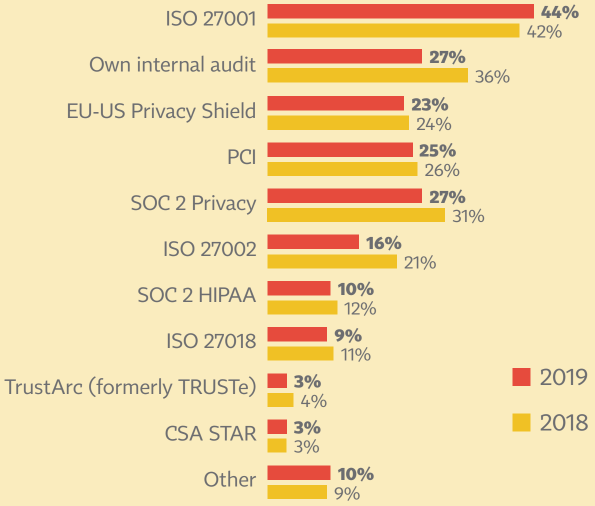
Looking at it another way, we see that 88% of EU respondents rank "compliance" with a law (GDPR or otherwise) as their top priority compared to just 57% of those in the U.S. At the same time, it's three times more likely that a U.S.-based privacy pro (36% U.S. to 12% EU) will have as a top priority something other than legal compliance (such as satisfying business clients, helping with security, or even enhancing reputation and brand).

Regional distinctions can also be found in privacy team responsibilities. For the most part, privacy professionals globally must engage in bread-and-butter duties, like

continued from xv

conducting on-site vendor audits to vet their data-processing programs. Nearly all respondents (94%) list "relying on assurances in the contract" as their method to ensure processors live up to their GDPR and other privacy and security obligations.

More than half of our survey respondents (57%) require completion of questionnaires addressing data handling practices, and nearly half (48%) require third party attestations or certifications. For third-party certifications, ISO 27001 remains the year-over-year favorite.



The top consideration for processor selection is the existence of data protection and information security warranties in the contract — 88% of respondents say this is either "important" or "very important." The next most important considerations are carrying out due diligence of the vendor and limiting how much personal data a vendor receives.

drafting and updating privacy policies, conducting privacy training, addressing privacy issues with products and services, following legislative developments, conducting risk assessments, addressing incidents, and communicating with customers and others about privacy issues.

Not surprisingly, EU respondents (97%) are far more likely to put GDPR compliance on their list of responsibilities than those in the U.S. (72%). But while U.S. privacy professionals checked many boxes on the "responsibilities" question, those in the EU did not. We see U.S. respondents more likely to list as responsibilities "vendor management," "redress and consumer outreach," and even "ethical decision making around use of data" than those in the EU.

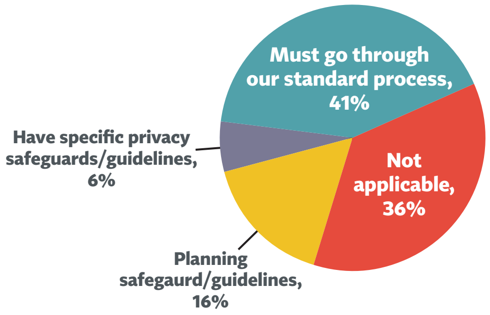
Even though the CCPA likely applies extraterritorially, similarly to the GDPR, for the most part only U.S.-based respondents listed it as a responsibility in this year's survey – 80% of U.S. respondents compared to just 17% in the EU.

Once again, this suggests that privacy pros in the U.S. tend to carry a wider range of responsibilities and expectations, well beyond GDPR compliance. Conversely, it also suggests

	U.S.	EU
Privacy Responsibilities		
GDPR compliance	72%	97%
Following privacy legislative developments	92%	80%
Vendor management	83%	64%
Ethical decision-making around data use	72%	56%
Privacy-related subscriptions and publications	60%	33%
Preparation for the CCPA	80%	17%
Redress and consumer outreach	47%	33%
Privacy-related web certification and seals	38%	21%

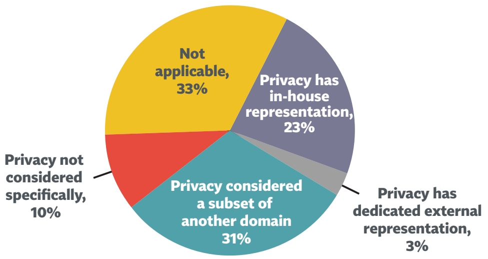
Specialized Privacy Risks

This year, for the first time, our survey asked whether privacy professionals are treating artificial intelligence or machine learning differently from other privacy risks. Specifically, we asked, "To what extent do privacy risks factor into your artificial intelligence or machine learning strategy or process?" Our goal was to explore whether AI/ML has inspired specialized risk analyses, whether privacy teams settled for standard privacy reviews deployed for other processing, or whether for now, AI /ML analysis is not a factor at all.



For 36% of respondents, AI/ML is not perceived as a unique risk factor presently. Four in 10, however, deal with AI/ML issues but use their standard privacy risk analysis. Only 6% of respondents have developed AI-/ML-specific privacy safeguards or guidelines, while another 16% are currently planning them. Is this an opportunity for law firms and consultants to provide guidance?

We also asked — here, too, for the first time — if privacy risks are factored into mergers-and-acquisitions strategies. The data shows that respondents are typically not concerned with M&As, either because it's not applicable (33%), it's viewed as the responsibility of someone else in the organization (31%), or it's simply not treated any differently from other data processing risks (10%). Approximately one in five respondents indicated their firms assign an in-house team to consider privacy issues with M&As; just 3% said it's an outside function.



that EU respondents (especially DPOs) are are laser focused on GDPR compliance as their top responsibility, and this, of course, entails a wide variety of duties and obligations.

GDPR Compliance: Still a Struggle After All These Years

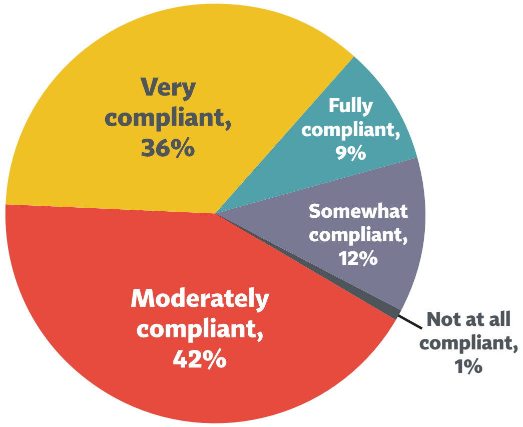
The one-year GDPR anniversary has come and gone. Already, as was mentioned above, DPAs are issuing fines, including mega penalties announced against British Airways, Marriott and Google.

And yet, fewer than half of the respondents to our survey report that their firms are “very compliant” or “fully compliant.” More than one-third report being only “moderately compliant.” Keep in mind, our survey has a selection bias, since those who take it are already specialized in privacy and data protection law and work for employers that have invested in compliance. Even among these professionals, GDPR compliance is still a struggle.

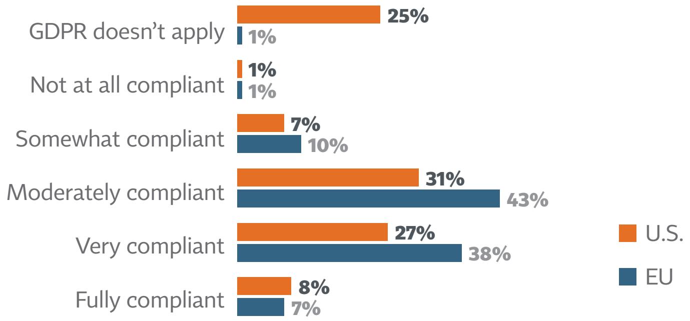
When we segregate U.S. from EU respondents, we see that one in four U.S. respondents report the GDPR does not even apply to their firm. Among EU respondents, 43% report they are only “moderately compliant” with the GDPR, even when GDPR compliance is their primary responsibility. One in 10 admit they are only “somewhat” compliant with GDPR.

These remarkable statistics likely do not indicate that respondents are lax at their jobs, but rather that the more one studies and implements the GDPR in a real-world business environment, the more one realizes that full compliance is a lofty goal. New data-processing activities are constantly created and discovered, so there is never a moment when all the work is done.

GDPR Compliance Status
(Base: must comply with the GDPR)



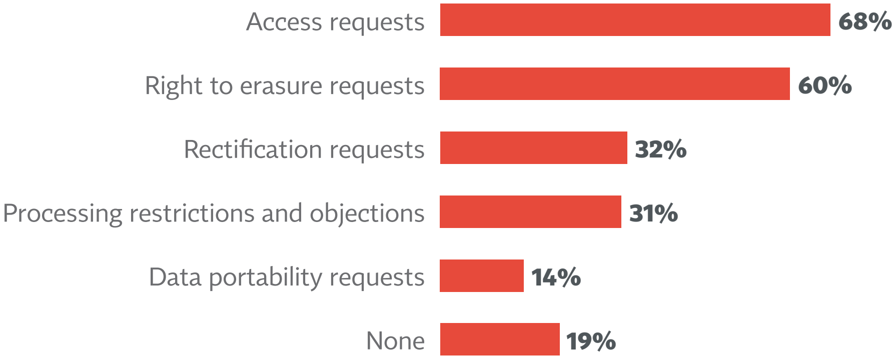
Level of GDPR Compliance among EU and U.S. firms



The silver lining is that the tasks seem less challenging now than a year ago. Across all categories of GDPR compliance tasks, the difficulty scores that respondents assigned have dropped compared to 2018. Compliance with the “right to be forgotten” still ranks first on the perceived difficulty scale, but it dropped half a point from last year (from 5.8 on a 10-point difficulty scale to 5.3). Data portability, ranked second, also dropped from 5.3 to 4.8.

U.S. respondents struggle more than their EU counterparts with all GDPR obligations, but gathering explicit consent has always been an area of significant differentiation. For U.S. respondents, it is tied for second on the difficulty scale with a 4.9 difficulty score, whereas EU-based respondents place it third (with only a 4.2 rating) behind right to be forgotten (5.0), data portability (4.6), and conducting DPIAs (4.6).

Types of DSRs Received in Past Year



The gap is even wider between U.S. and EU respondents regarding data subject requests. U.S. respondents give them a 4.7 perceived difficulty score compared to just 3.9 from those in the EU. And yet that task is one that has fallen markedly in its overall perceived complexity compared to last year, dropping 1.2 points on the difficulty scale. This is likely because firms are being forced to face actual requests and come up with efficient responses. And so, over time, the process is becoming easier.

Interestingly, those who tend to rank data subject requests as less difficult are also those receiving the most requests. These same respondents also tend to take the least amount of time in responding. Among those who found data subject requests most difficult, only 30% were able to respond within a week, whereas among those who found them less difficult than average, 56% could respond in under a week's time.

To be sure, just because practice and systems make data subject requests less complicated on a per-request basis

Data transfers

One of the reasons for growth in IAPP membership and the privacy profession generally is the increasing complexity of global privacy and data protection laws. IAPP members often work for enterprises that conduct business in many regions, if not globally. This year's governance survey for the first time has more respondents whose organizations collect data from the EU (without the U.K.) (77%) than from the U.S. (66%).

Seven in 10 respondents say their organization transfers data out of the EU to non-EU countries. The GDPR requires these transfers to go only to countries with adequate data protection laws; alternatively (only 37% of respondents rely on adequacy), controllers must put in place appropriate safeguards to ensure GDPR compliance. The most popular of these tools — year over year — are overwhelmingly standard contractual contracts: 88% of respondents in this year's survey reported SCCs as their top method for extraterritorial data transfers, followed by compliance with the EU-U.S. Privacy Shield arrangement (60%).

For respondents transferring data from the EU to the U.K. (52%), 91% report they intend to use SCCs for data-transfer compliance after Brexit.

With SCCs and Privacy Shield both under threat of invalidation by the Court of Justice of the European Union, controllers and processors alike face uncertainty in maintaining compliance with the GDPR's data-transfer requirements.

doesn't mean they are easy. More than half of respondents (56%) named "locating unstructured personal data" as the most difficult issue in data subject request response, far ahead of "monitoring data protection/privacy practices of third parties" (36%), data minimization (28%), or developing a centralized opt-out tool (25%).

The data show that data subject requests are hitting EU respondents a bit harder than those in the U.S. Blended (B2B and B2C) firms are also more likely than B2B or B2C companies to receive data subject requests. Least likely to receive multiple data subject requests are small firms by employee size (<5,000 employees) and by revenue.

Percentage of organizations that have received data subject requests by HQ location

	U.S.	EU
Access	59%	76%
Erasure	50%	72%
Rectification	22%	39%

Firms most likely to receive data subject requests:

- **HQ in the EU**
- **B2B + B2C biz model**
- **> 25,000 employees**
- **> $25 billion revenue**

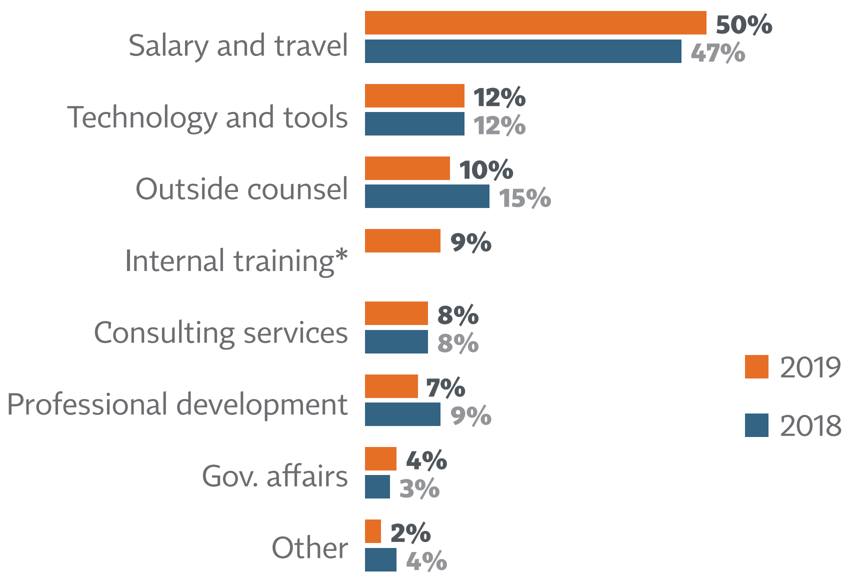
Getting the Work Done: Staffing and Budgets

The ramp-up to the GDPR's May 25, 2018, compliance deadline involved significant investments in privacy staff and outside counsel/consultants. This year, although staffing and budgets have not plummeted, we do see them leveling off.

Privacy staffing appears to have stabilized. Respondents in this year's survey are more likely to say that their staff levels are going to stay the same next year than they were in 2018. They are also less likely to expect staff increases.

Budgets are lower than in 2018, the year of landing for the GDPR. The median total privacy spend was $400,000 in 2018; this year, the median was half that amount. That

Distribution of Privacy Budget Components



said, most respondents did not expect a decrease in their budgets for next year. In fact, 55% expect their budgets to increase.

As usual, privacy professionals feel their budgets are inadequate — 62% reported inadequate resources, which is in line with other recent IAPP studies in which lack of budget has hindered compliance efforts. With corporate boards ever more likely to tackle privacy as a key business risk, perhaps privacy teams will benefit from additional financial support in the coming months and years.

Compensation for privacy professionals has historically been the largest cost center. This year is no exception. When we compare the smaller firms by employee size (under 75,000) to the very largest (more than 75,000), however, we see a great disparity in how privacy budgets are allocated. Firms with more than 75,000 employees allocate far more to compliance technology (for both the privacy team and outside the team) as a percentage of their overall privacy spend.

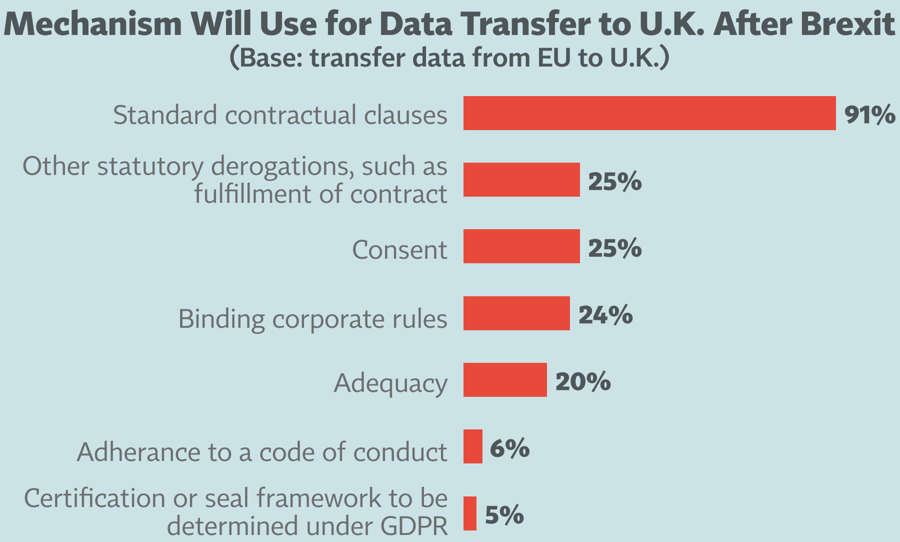
Regionally, privacy budgets in the U.S. remain larger than those in the EU. Respondents in the U.S. report total privacy

Brexit's looming impact

More than half (56%) of all respondents indicated they will feel the impact of Brexit. Among EU respondents alone, the number of affected respondents climbs to 68%.

Despite the massive uncertainty around the deal — or lack thereof — that Britain will strike with the EU, nearly one in four (23%) respondents believes they are "very prepared" for the event, while 43% are at least "moderately prepared." This could be because, as a practical matter, 44% of those respondents who think Brexit will impact their organization do not think it will affect their privacy team;; another 26% are taking a "wait-and-see" approach — not making any plans at this time.

Among companies with a "main establishment" in the EU, 24% locate it in the U.K. More than half (55%) of these organizations do not plan to move their main establishment post-Brexit. Nevertheless, a noticeable number (12%) will be moving their headquarters to Ireland, with another 18% planning to move to another EU location; 16% simply do not yet know. Their options for moving are largely dependent on corporate location (55%), although the supervisory authority's comfort with the English language is a factor for 31% of those planning to move.



spend on average of $952,000 compared to just $387,000 for EU respondents. This also holds true when we look at the numbers based not on where the respondent is located but rather where their employer is headquartered. Those with U.S. headquarters outspend those with EU headquarters almost four to one.

When we compare regions on a per-employee-spend basis, however, it comes out about the same, suggesting that the larger tech companies based in the U.S. are pulling the U.S. average considerably higher.

iapp

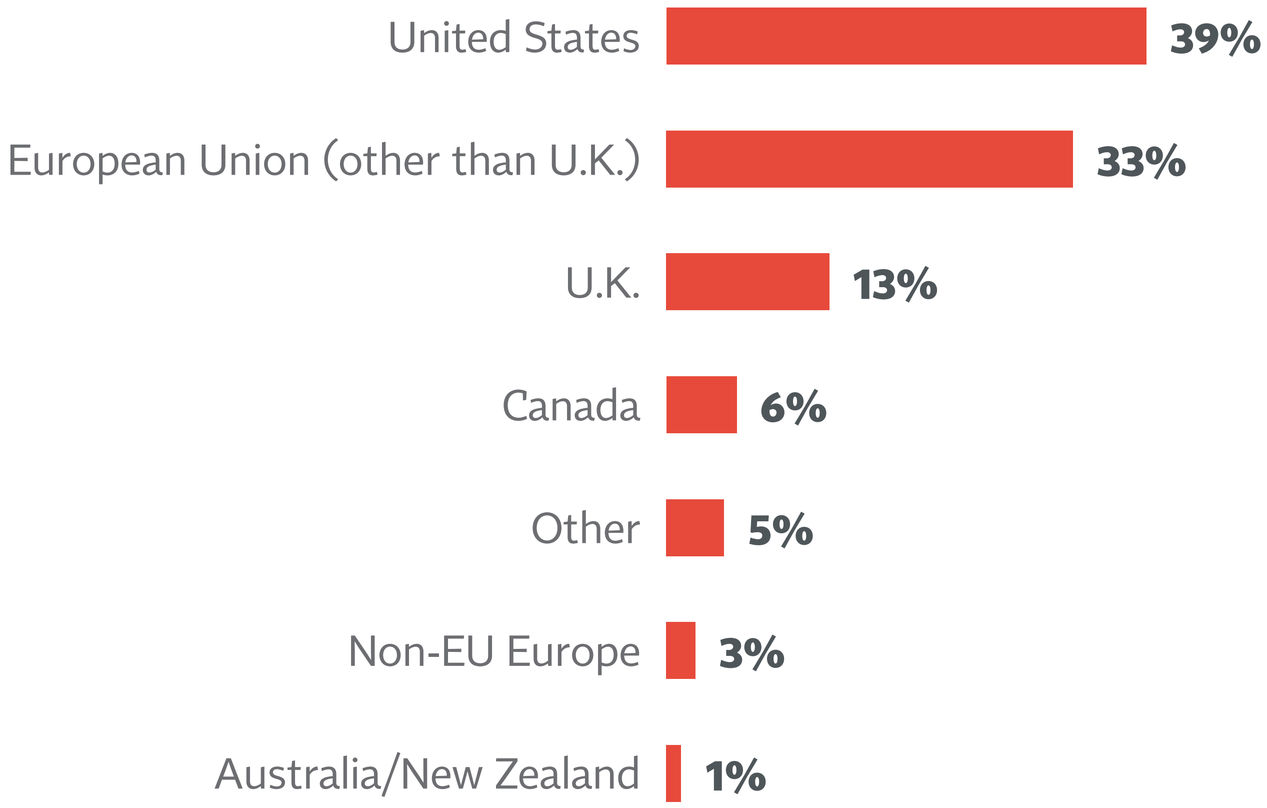
EY

Building a better working world

Contents

This year’s survey struck a good balance between organizations based in North America and Europe

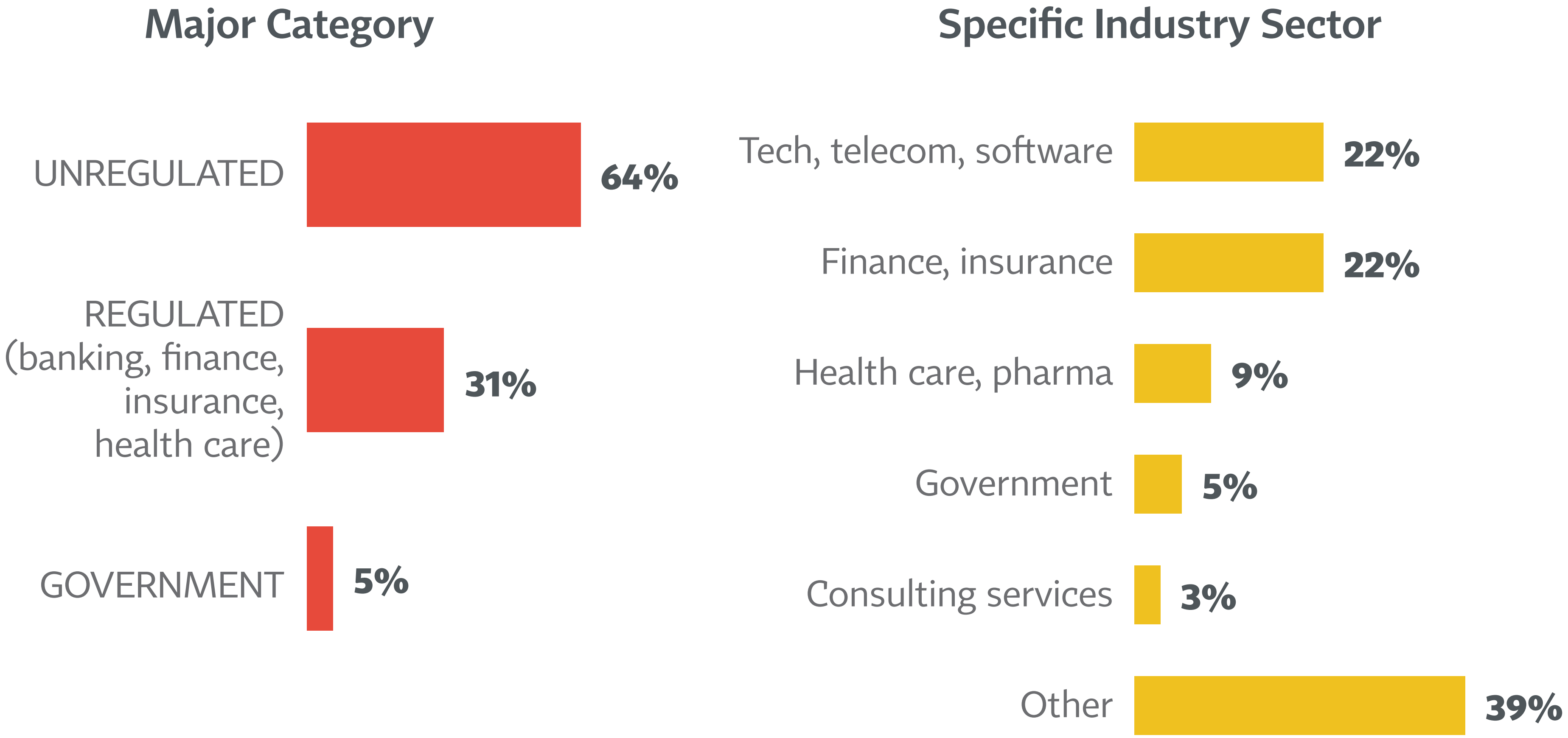
Company Profile: HQ Location



A4. What is the primary location of your company’s headquarters?

Firms in this year's survey primarily came from unregulated industries, such as tech and telecom

Company Profile: Industry

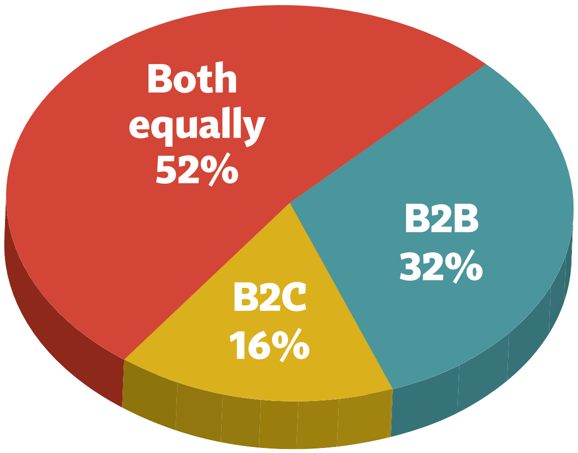


A1. Which sector listed below best describes how your company would be classified?

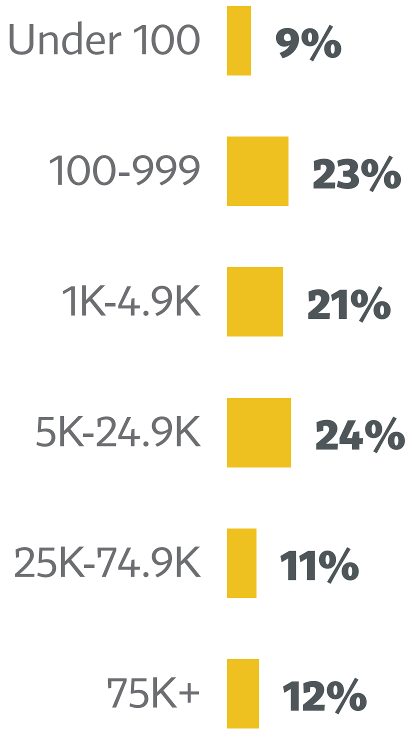
Respondents distributed across a range of small, medium, and large organizations

Company Profiles

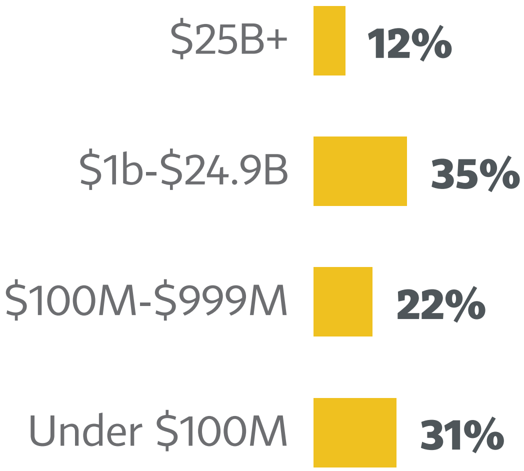
Business Type



Employees

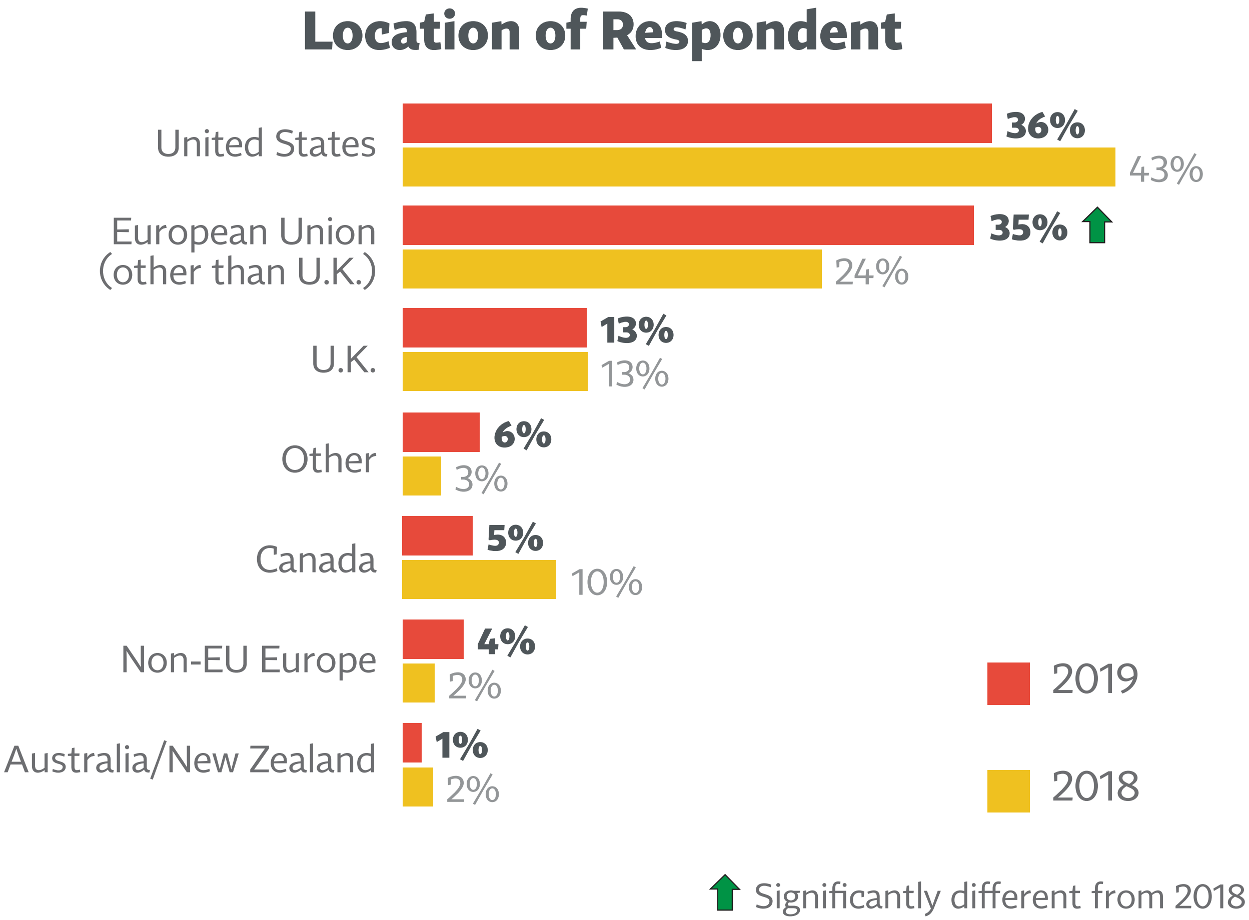


Revenue



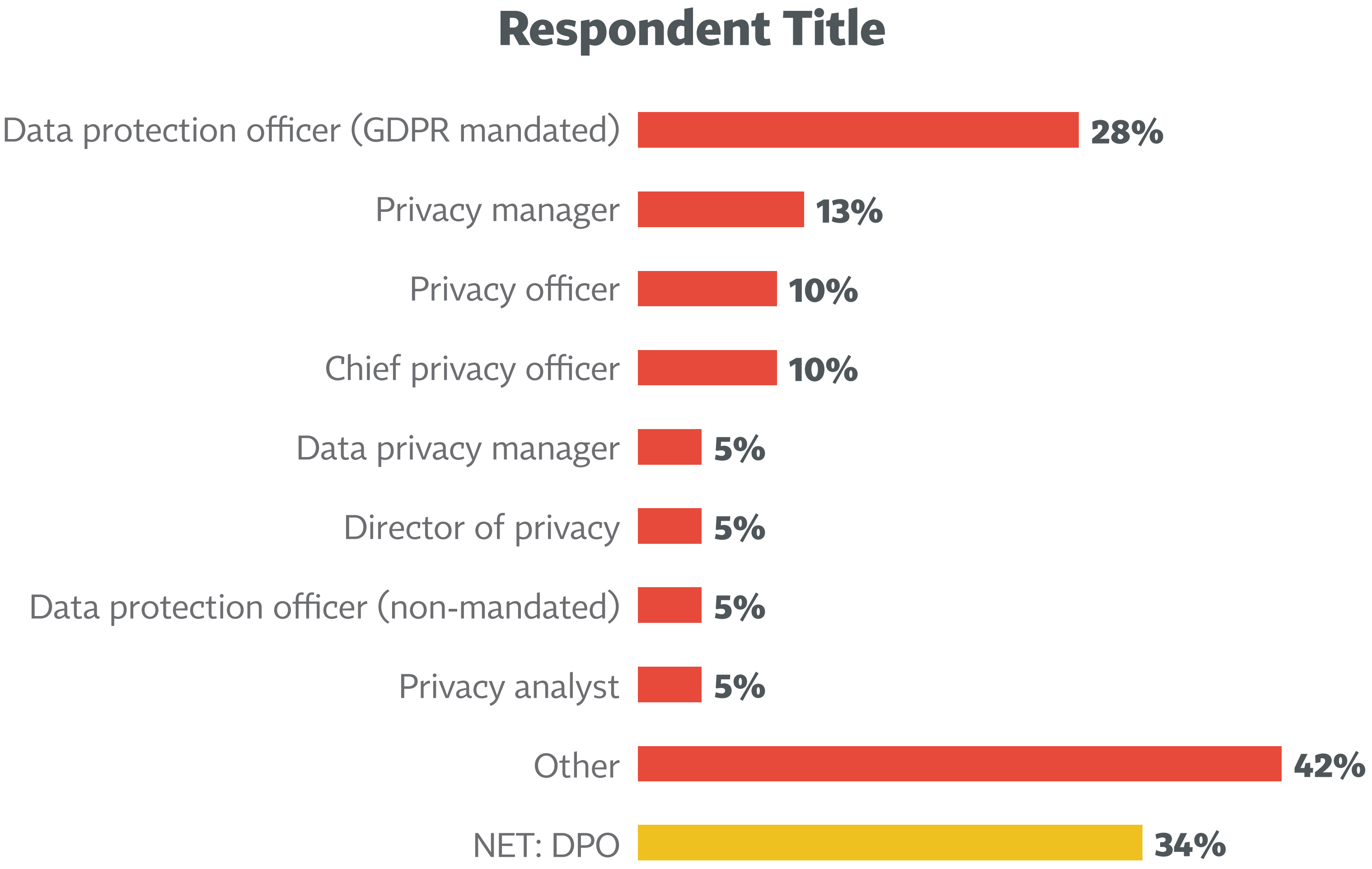
A1a. Does your company primarily serve:
A3. What is the total number of employees in your company (full time and part time)?
A2. Please tell us (as accurately as you can) your company's annual revenue.

Looking at respondents themselves, we see an even split between those located in the U.S. and the EU



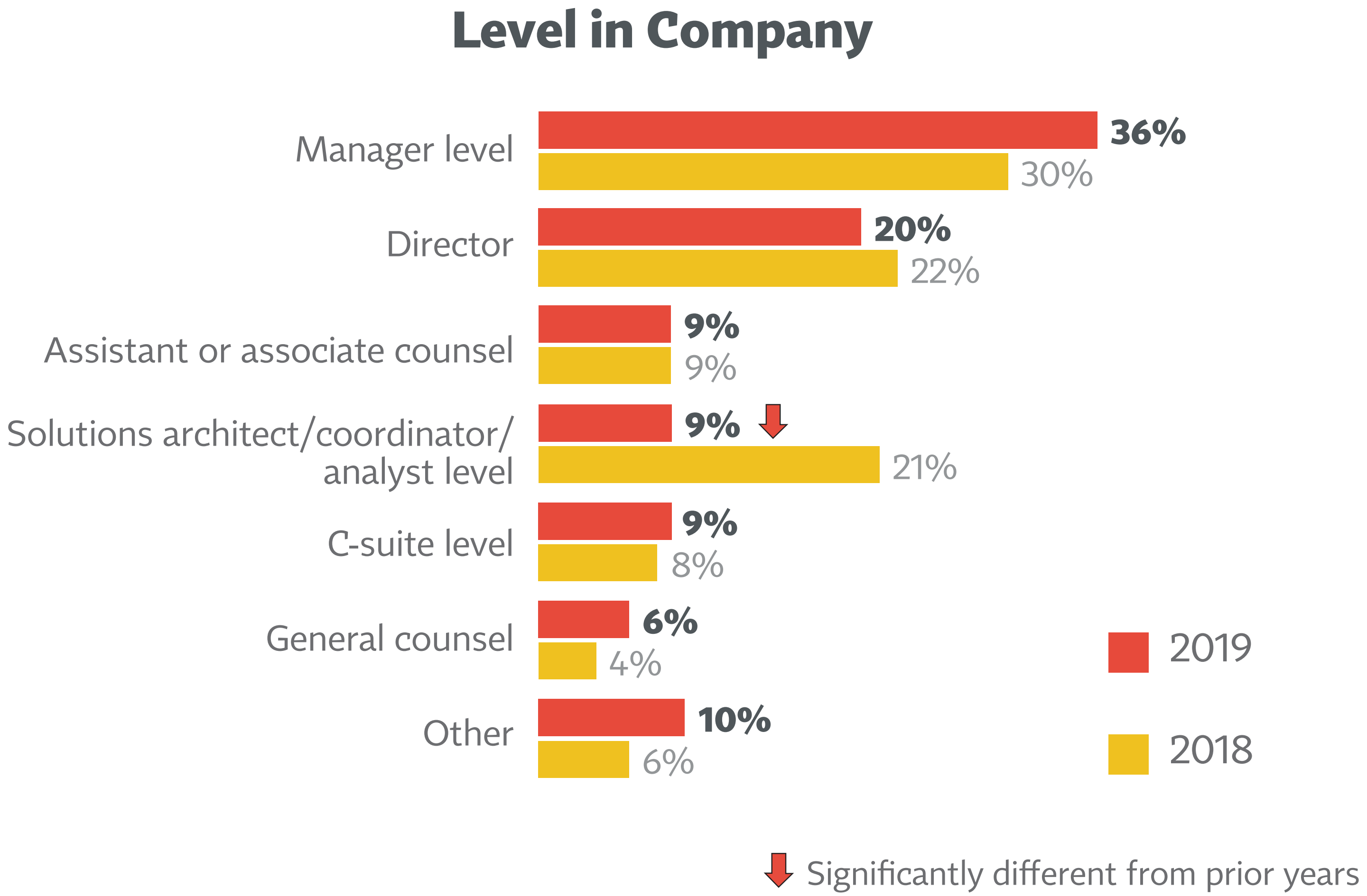
A5. In what region and country are you currently based?

The most commonly held position for respondents was data protection officer, most of whom are mandated



D2A: What is your job title?

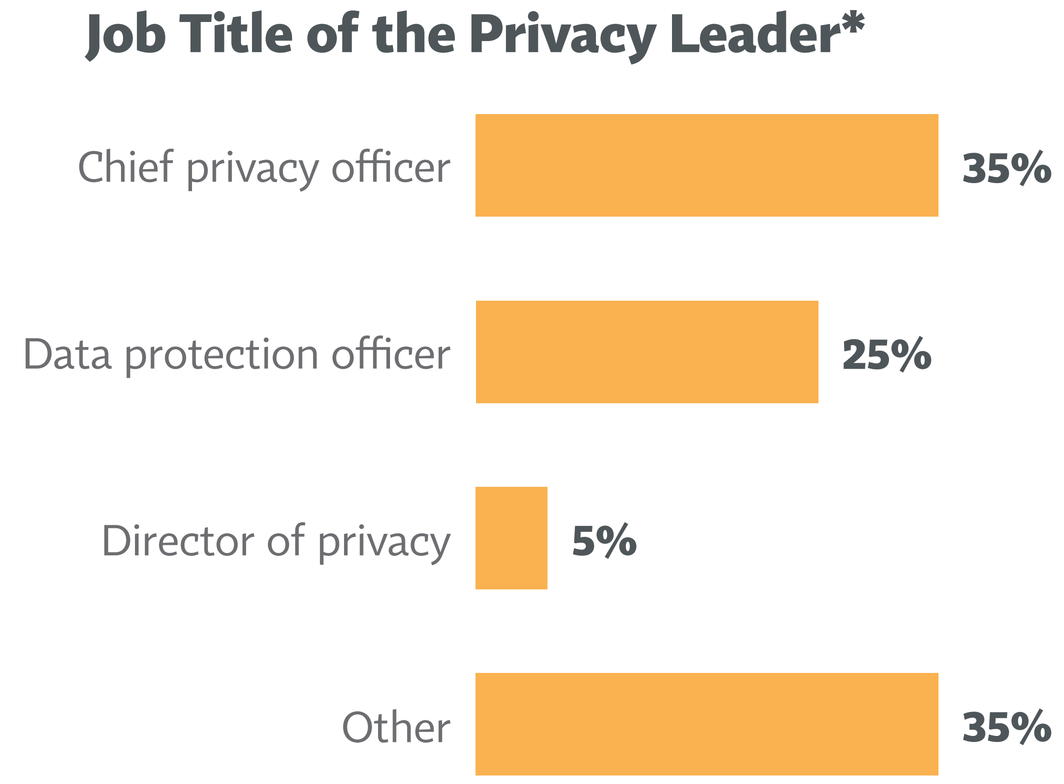
This year's survey drew more respondents who are managers and fewer from coordinator/analyst jobs



D2: Which of the following levels best describes your position in your company?

Contents

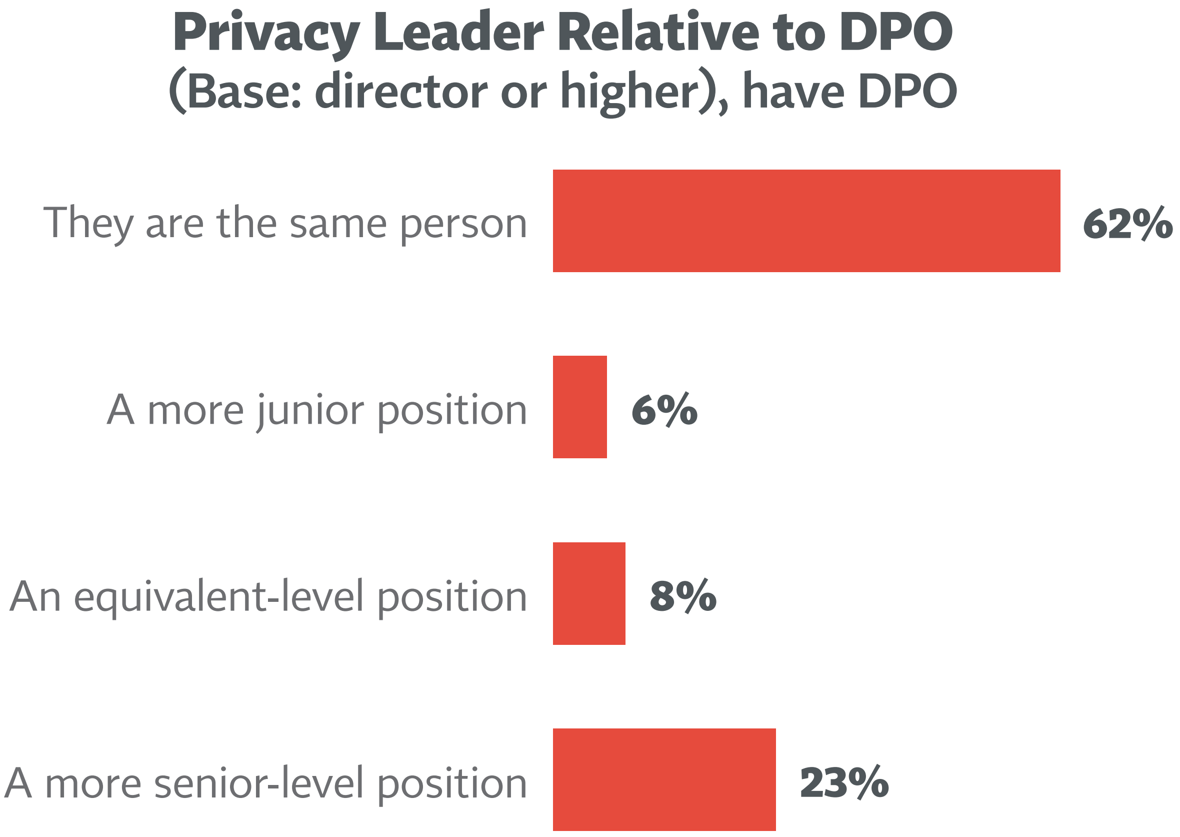
The privacy leader is usually the chief privacy officer or the data protection officer



**Privacy leader: We ask respondents to self-report whether they are the "privacy leader," that is the most senior officer responsible for privacy in an organization, having responsibility for oversight of the privacy program. As we demonstrate in the report, this could be anyone from the CEO to a data protection officer.*

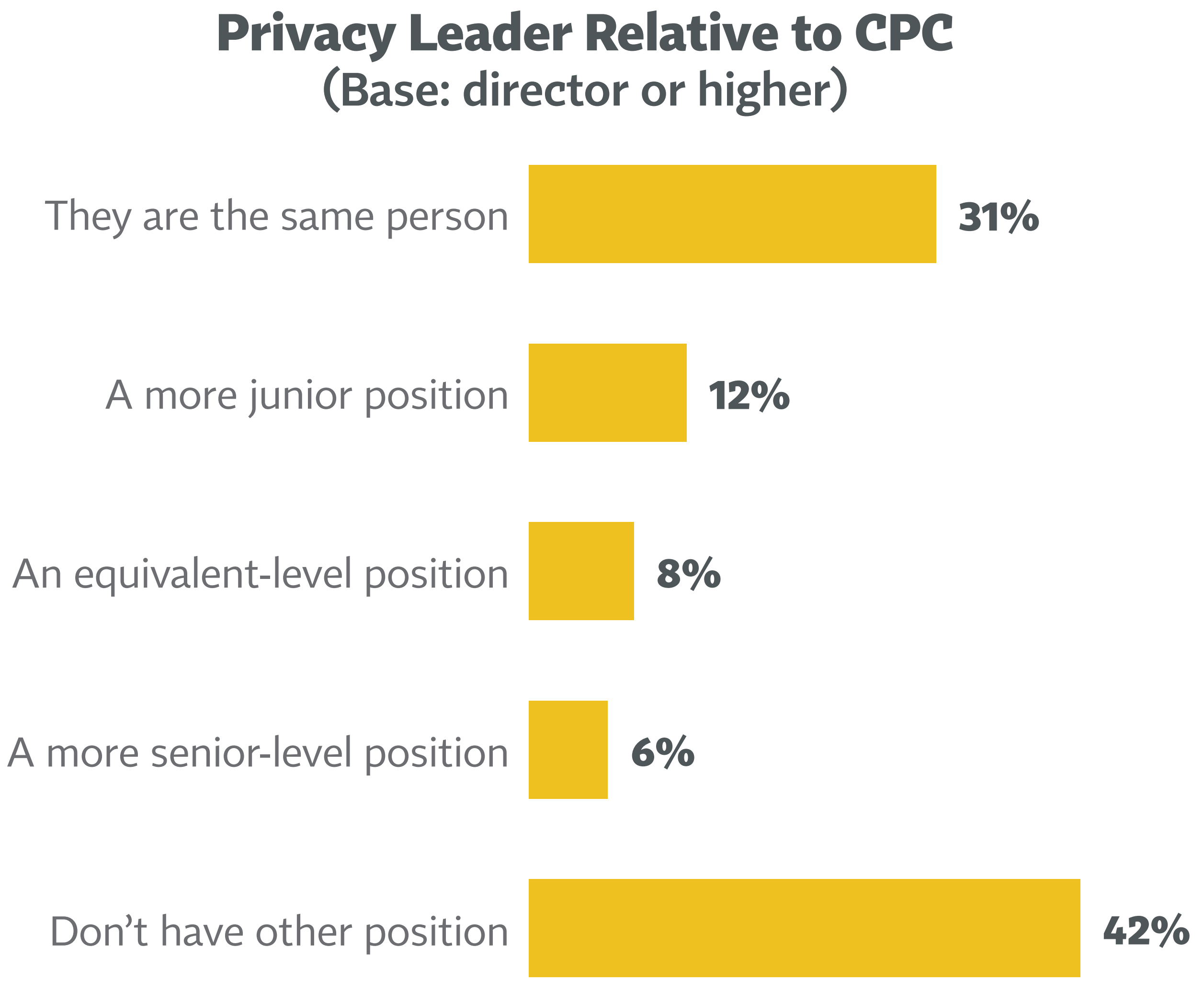
F21: What is the job title of the privacy leader in your company?

DPOs are the privacy leaders at about 6 out of 10 organizations that have a DPO



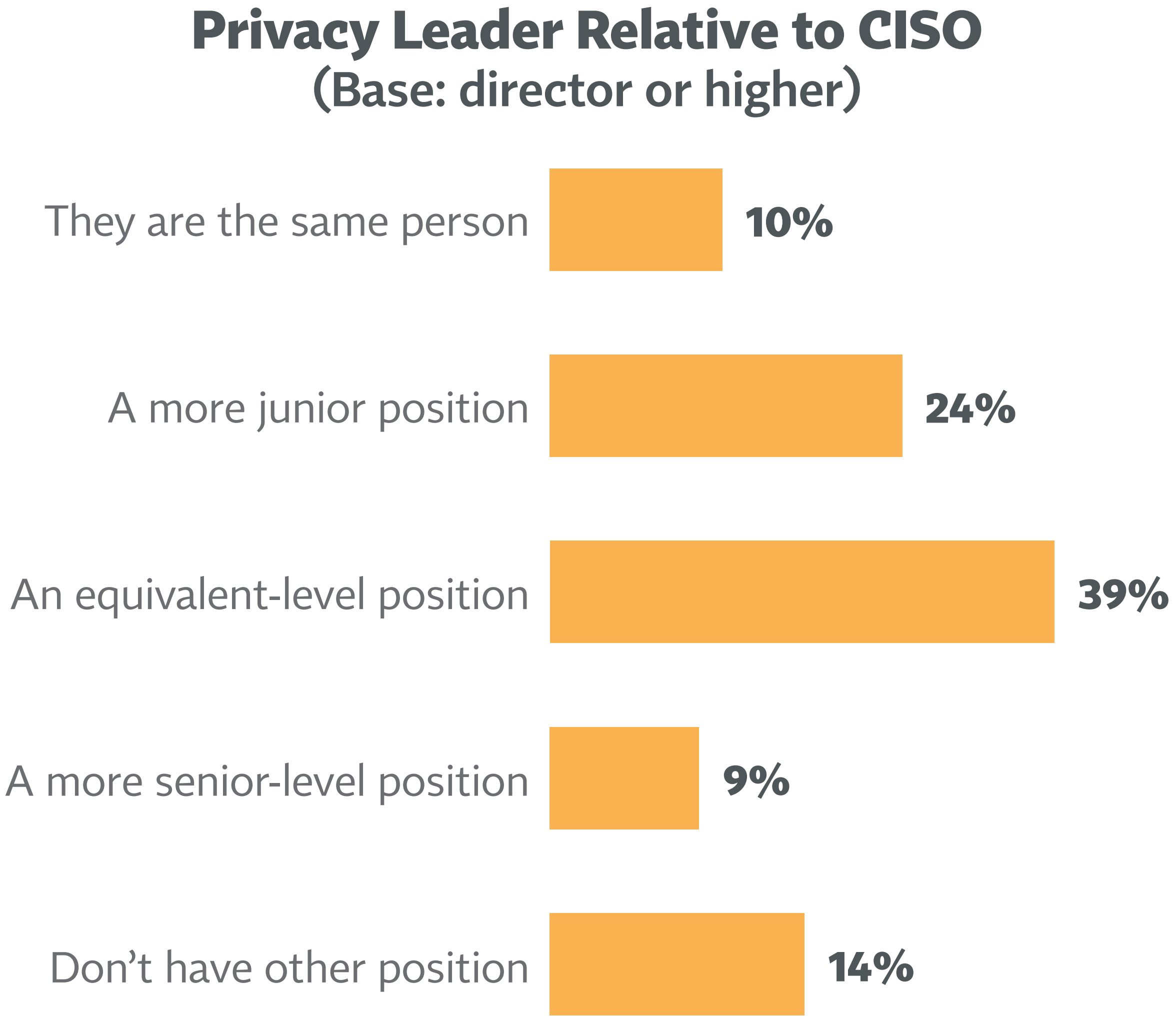
F31: How does the privacy leader compare with your company's DPO, if any?

The chief privacy counsel is the privacy leader in 3 out of 10 firms



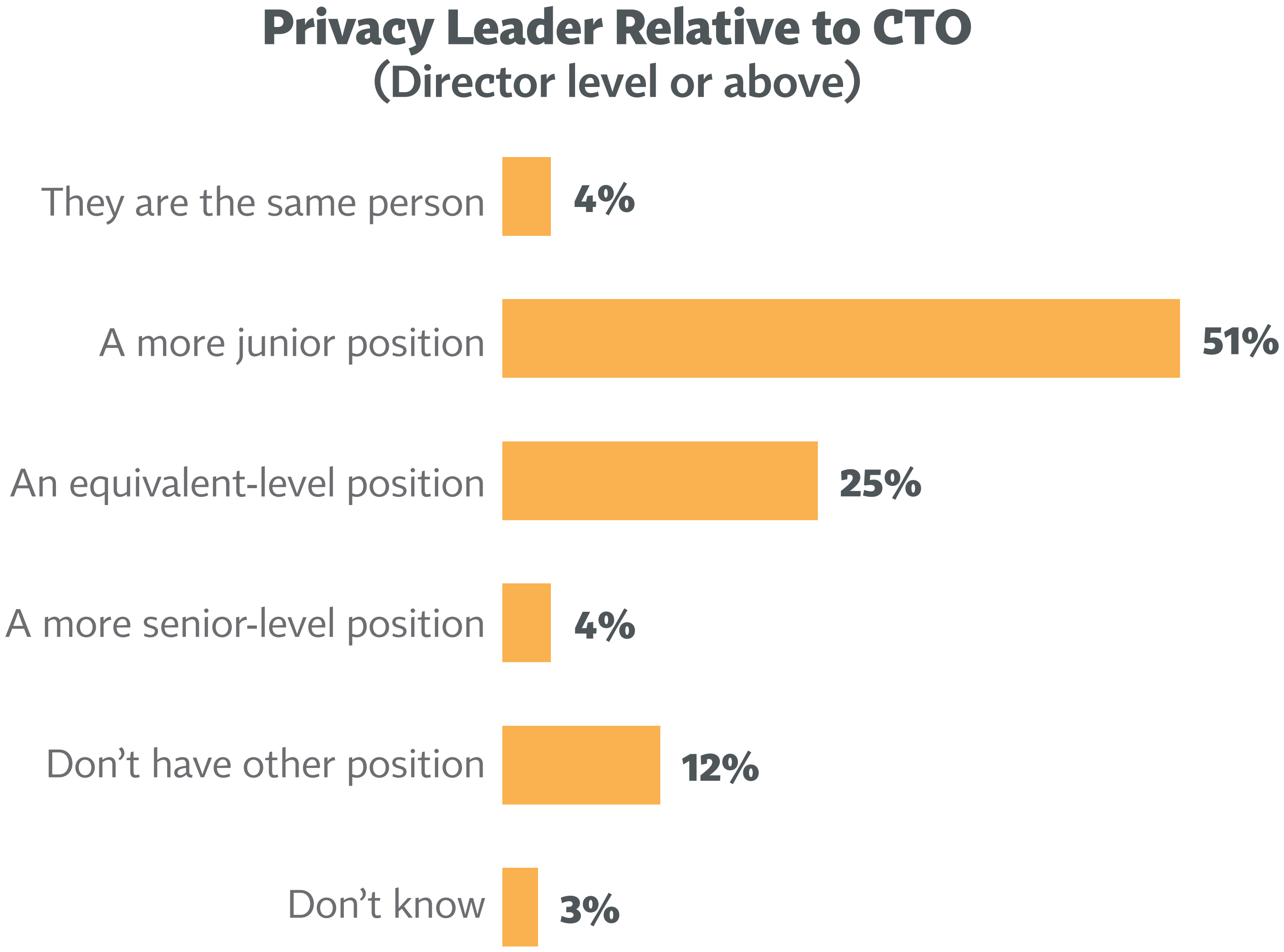
F23: How does the privacy leader compare with your company's chief privacy counsel? The privacy leader is …

In only 1 out of 10 firms, the CISO is the privacy leader; these two positions are often on the same level



F22: How does the position of the privacy leader compare with your company’s CISO or the highest-level information security person in the company?

CTOs are rarely privacy leaders, tending to hold a more senior position than them



F22A: How does the position of the privacy leader compare with that of your company’s CTO or the highest-level information technology person?

EU-based Privacy Leaders more often report to Board of Directors, U.S.-based ones to General Counsel

BY RESPONDENT LOCATION

	U.S.	EU
Privacy Leader Reports To		
General counsel	**35%**	18%
CEO	16%	25%
Board of directors	10%	**35%**

BY COMPANY REVENUE

	<$100M	$100M-$999M	$1B-$24.9B	$25B+*
Privacy Leader Reports To				
General counsel	**13%**	22%	**42%**	21%
CEO	30%	34%	**9%**	22%
Board of directors	**39%**	19%	**9%**	32%

■ Significantly different than other segments   * Small sample size

Privacy Leaders at small firms more often report to the CEO, and less often to the CCO, than those at big firms

BY EMPLOYEE SIZE

	<5K	5K–24.9K	25K–74.9K*	75K+*
Privacy Leader Reports To				
General counsel	20%	27%	41%	27%
CEO	**31%**	15%	13%	12%
Board of directors	29%	**11%**	13%	28%
Chief compliance officer	**15%**	24%	31%	**43%**
Executive vice president or VP	**9%**	19%	22%	19%
CFO	10%	2%	0%	10%

BY INDUSTRY SEGMENT

	Regulated	Unregulated
Privacy Leader Reports To		
General counsel	20%	29%
CEO	22%	22%
Board of directors	24%	21%
Chief compliance officer	**35%**	17%
Executive vice president or VP	12%	13%
CFO	3%	10%

🟧 Significantly different than other segments * Small sample size

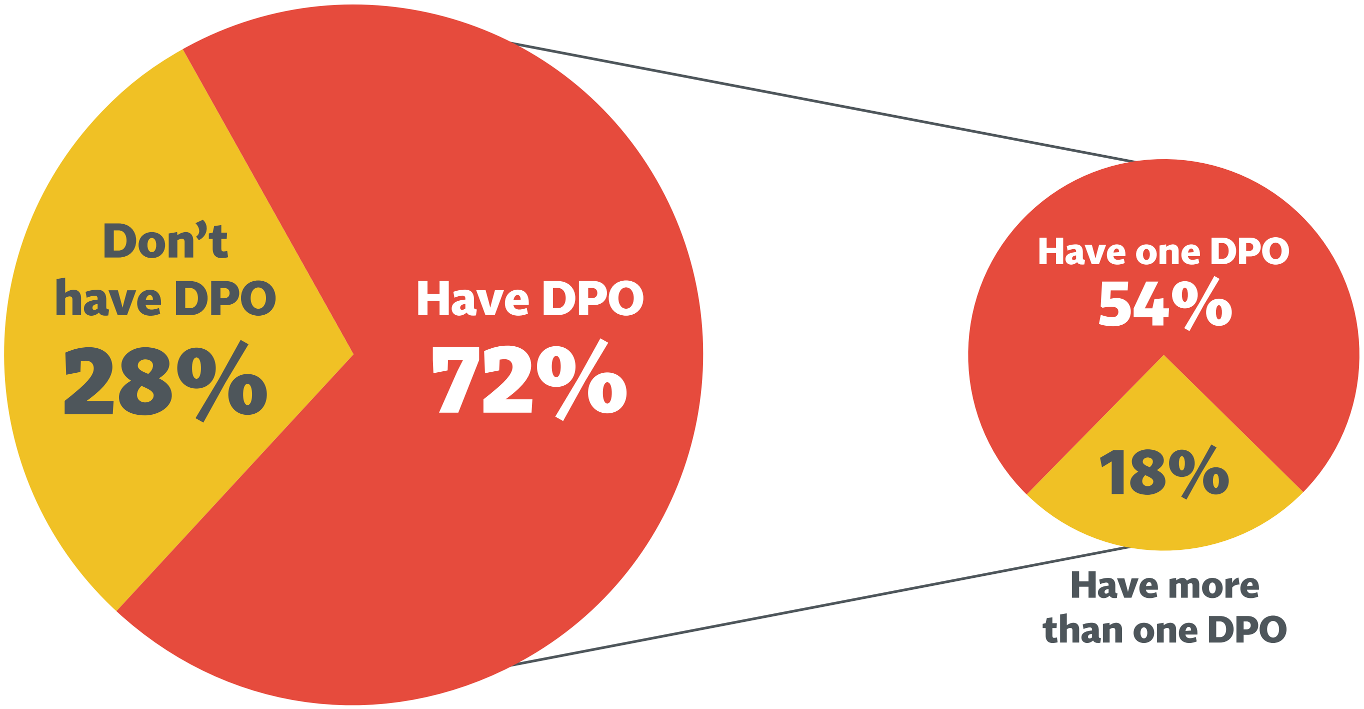
Roughly 3 out of 4 firms have a data protection officer, essentially unchanged since last year

Whether Firm Has DPO and Number of DPOs
(Base: director or higher)

TOTAL WHO HAVE DPO

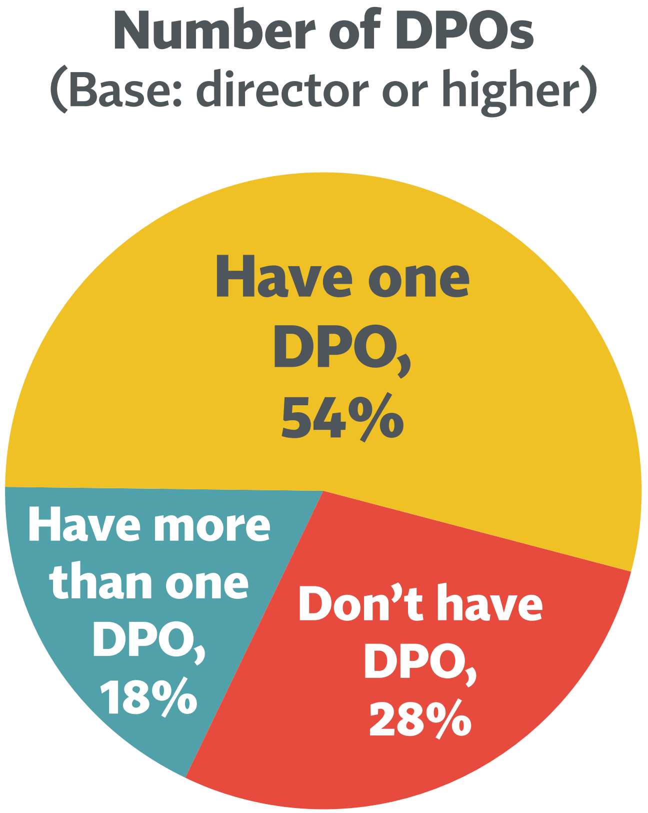
2019: 72%

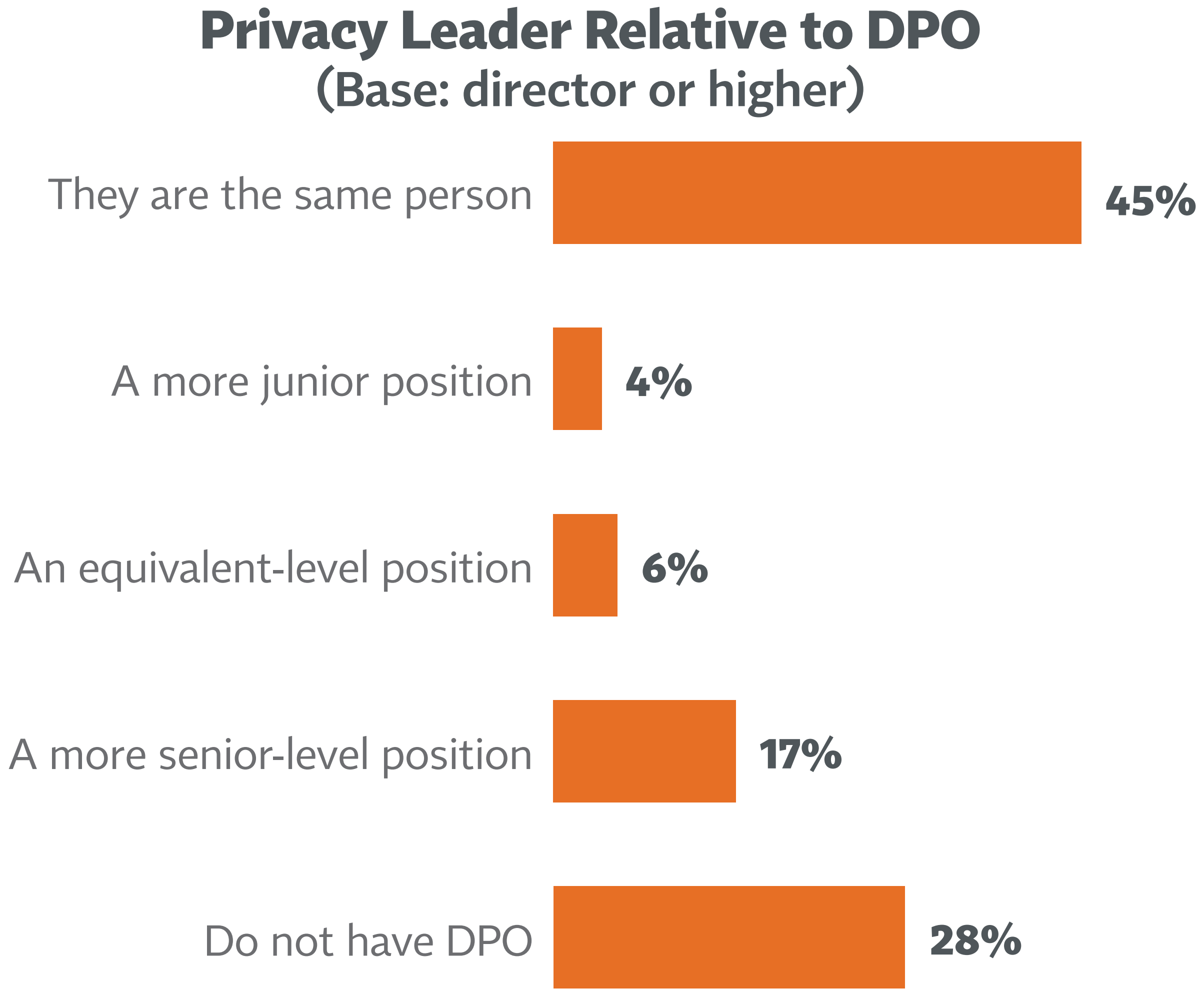
2018: 75%



F30: Does your company have only one DPO responsible for overseeing data protection strategy across the company? Or does it have more than one?

Among those with a DPO, most have only one, and that person is usually the privacy leader





F30: Does your company have only one DPO responsible for overseeing data protection strategy across the company? Or does it have more than one?
F31: How does the privacy leader compare with your company's DPO, if any?

Respondents who are DPOs more likely to be based in the EU and work for B2B or hybrid (B2B&C) firms

BY RESPONDENT LOCATION

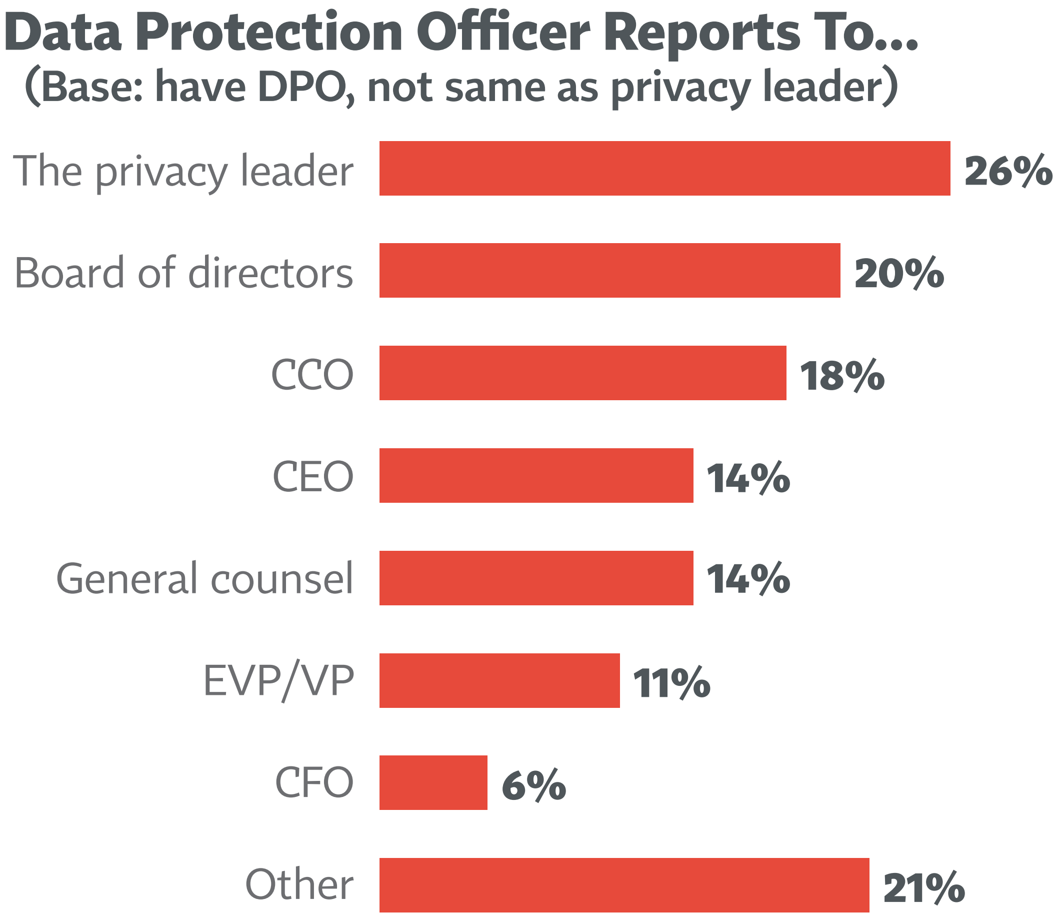
	U.S.	EU
Respondent is DPO	39%	**67%**

BY TARGET

	B2B	B2C	B2B&C
Respondent is DPO	**47%**	21%	**51%**

▨ Significantly different than other segments

Most DPOs who are not the privacy leader report directly to the privacy leader, board or Chief Compliance Officer



F32: To whom in your company does the data protection officer report?

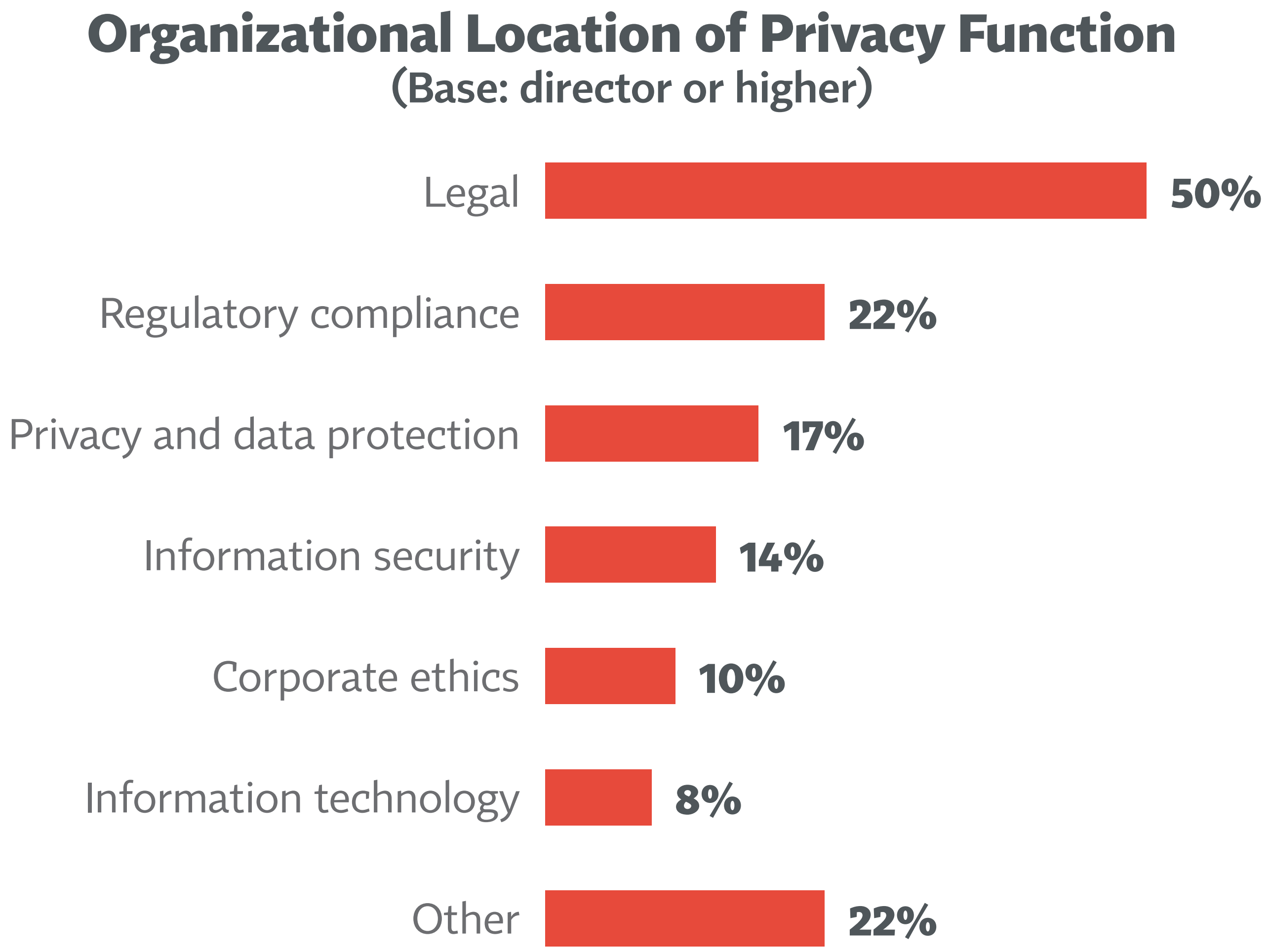
Firms where the DPO and privacy leader are the same person are smaller and more likely to be non-U.S.

BY DPO STATUS

	DPO IS PRIVACY LEADER	DPO IS NOT PRIVACY LEADER
Mean company revenue	$2.7B	$8.2B
Mean company employees	7.6K	13.7K
Mean total privacy employees	13.3	18.1
Headquarters is in U.S.	16%	59%
Respondent is in U.S.	13%	59%
Privacy team responsible for GDPR compliance	93%	73%
Privacy team responsible for CCPA prep	23%	56%
Privacy team in place for two years or fewer	58%	42%
Brexit will affect organization	66%	41%

Contents

Half of privacy teams are located in the legal department



F12: In which department within your company is the privacy team located?

Staff who devote part of their time to privacy outnumber full-time staff by a ratio of about 2:1

Privacy Staff: Mean

	2019
	Mean
Full-time privacy staff	7.1
Part-time privacy staff	15.7

NOTE: Outliers over 999 removed.

F1: How many employees are dedicated full time to your company's privacy program?

Not surprisingly, privacy staff size increases with total employee size and company revenue

Mean Privacy Staff by Total Employee Size and Company Revenue

	<5K	5K-24.9K	25K-74.9K*	75K+*
Full-time privacy staff	2.2	11.4	11.0	18.9
Part-time privacy staff	5.5	17.8	23.3	56

	Under $100M	$100M-$999M	$1B-$24.9B	$25B+*
Full-time privacy staff	2.5	4.7	10.0	15.6
Part-time privacy staff	4.6	14.6	19.3	50.7

NOTE: Outliers over 999 removed.

* Small sample size

F1: How many employees are dedicated full time to your company's privacy program?

Hybrid B2B/B2C firms tend to have more privacy staff than their B2B and B2C counterparts

Mean Privacy Staff by Industry Category and Consumer Target

	Regulated	Unregulated	Gov't.*
Full-time privacy staff	7.1	7.3	1.8
Part-time privacy staff	14.1	16.3	12.9

	B2B	B2C*	Both
Full-time privacy staff	3.9	5.3	9.4
Part-time privacy staff	7.9	8.3	22.0

NOTE: Outliers over 999 removed.

* Small sample size

F1: How many employees are dedicated full time to your company's privacy program?

Unlike last year, EU organizations now have larger privacy staffs than U.S. firms, both full and part time

Mean Privacy Staff Size by HQ Location

	U.S.	EU
Full-time privacy staff	5.2	10.4
Part-time privacy staff	8.0	28.0

NOTE: Outliers over 999 removed.

F1: How many employees are dedicated full time to your company's privacy program?

3 out of 10 privacy pros expect to see an increase in full-time privacy staff; only 1 in 20 expect a decrease

Expected Employee Change in Coming Year

	% Saying Increase		% Saying Decrease		% Saying Stay the Same		Net % Change	
	2019	2018	2019	2018	2019	2018	2019	2018
Full-time privacy staff	30%	41%	4%	1%	66%	58%	+12%	+17%
Part-time privacy staff	19%	24%	2%	2%	79%	74%	+6%	+11%

NOTE: Outliers over 999 removed.

F2: In the coming year, do you expect the number of employees in each of these categories to increase, decrease or stay the same? If increase or decrease, please enter your estimate of the percentage change you expect.

Privacy spending has dropped since 2018, a peak year for GDPR-related spending

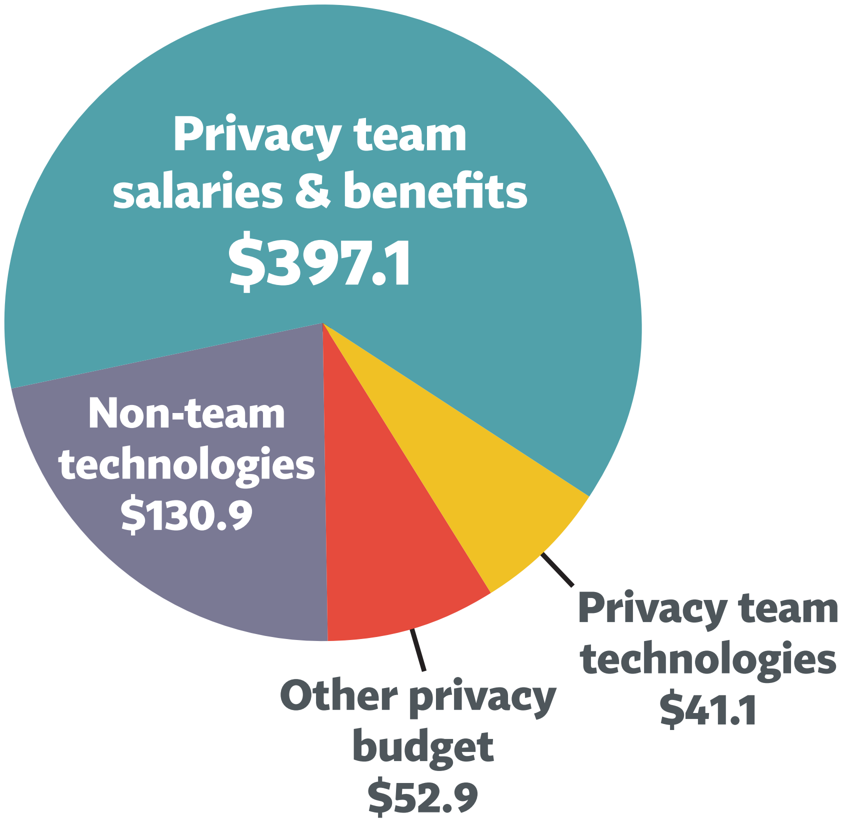
Privacy Spend

TOTAL PRIVACY SPEND

2018 MEAN: $1.0M
2019 MEAN: $622K

2018 MEDIAN: $400K
2019 MEDIAN: $200K

Mean spending per employee:
2018: $140
2019: $128



F4: And what is the total privacy spend for your company in each of the following categories?

Not surprisingly, privacy team salaries are higher at larger firms, as is total privacy spend

Median Estimated Privacy Spend (000)

(Base: director or higher)

	BY EMPLOYEE SIZE			
	<5K	5K-24.9K	25K-74.9K*	75K+*
Privacy team salaries	$120.0	$228.6	$307.5	$400.0
Privacy team technologies	$3.4	$11.2	$10.6	$6.0
Total privacy spend	$150.0	$400.0	$402.5	$506.0

* Small sample size

As we saw in 2018, privacy spending per company employee is highest at smaller firms

Mean Estimated Privacy Spend (000)

(Base: director or higher)

	BY EMPLOYEE SIZE			
	<5K	**5K-24.9K**	**25K-74.9K***	**75K+***
Privacy team salaries	$170.7	$581.8	$744.2	$847.1
Privacy team technologies	$23.5	$47.1	$39.7	$115.6
Outside privacy team technologies	$38.7	$30.5	$57.5	$814.2
Other privacy budget	$24.7	$84.5	$82.0	$106.2
Total privacy spend	$257.7	$743.8	$923.4	$1,883.2
Privacy spend per employee	$207	**$73**	**$24**	**$11**

🟧 Significantly different than other segments   * Small sample size

Regulated firms are the biggest spenders on privacy, while government agencies spend the least

Median Estimated Privacy Spend (000)

(Base: director or higher)

BY INDUSTRY CATEGORY

	Regulated	Unregulated	Gov't.*
Privacy team salaries	$162.4	$127.0	$112.0
Privacy team technologies	$1.5	$6.4	$11.2
Total privacy spend	$250.0	$190.0	$168.0

* Small sample size

As with staff size, spend per employee is higher in regulated firms than other firms or government entities

Mean Estimated Privacy Spend (000)

(Base: director or higher)

BY INDUSTRY CATEGORY

	Regulated	Unregulated	Gov't.*
Privacy team salaries	$468.5	$383.4	**$110.1**
Privacy team technologies	$24.4	$48.8	$14.0
Outside privacy team technologies	$54.1	$165.7	$24.3
Other privacy budget	$79.3	$45.2	**$1.9**
Total privacy spend	$626.3	$643.1	**$150.3**
Privacy spend per employee	$160	$118	$71

🟥 Significantly lower than other segments

Firms based in the U.S. have much higher median spending figures than EU firms

Median Estimated Privacy Spend (000)

(Base: director or higher)

	BY HQ LOCATION	
	U.S.	EU
Privacy team salaries	$300.0	$74.9
Privacy team technologies	$15.0	$0.1
Total privacy spend	$400.0	$123.8

F4: And what is the total privacy spend for your company in each of the following categories?

U.S. firms spend more overall on privacy than EU firms, but spend per employee is on par

Mean Estimated Privacy Spend (000)

(Base: director or higher)

	BY HQ LOCATION	
	U.S.	EU
Privacy team salaries	$583.1	$291.0
Privacy team technologies	$61.0	$22.9
Outside privacy team technologies	$238.9	$39.0
Other privacy budget	$69.2	$34.5
Total privacy spend	$952.2	**$387.4**
Privacy spend per employee	$138	$131

🟥 Significantly lower than other segments

F4: And what is the total privacy spend for your company in each of the following categories?

Privacy spending drops are seen at every level of company by employee size

Mean Estimated Privacy Spend (000)

(Base: director or higher)

	BY EMPLOYEE SIZE							
	<5K		5K–24.9K		25K–74.9K*		75K+*	
	2019	2018	2019	2018	2019	2018	2019	2018
Total privacy spend (000)	$257.7	$465.7	$743.8	$1,292.0	$923.4	$1,178.7	$1,883.2	$2,153.4
Privacy spend per employee	$207	$305	$73	$122	$24	$25	$11	$15

* Small sample size

F4: And what is the total privacy spend for your company in each of the following categories?

However, the one segment spending more this year than last are those with revenues of more than $25B

Mean Estimated Privacy Spend (000)

(Base: director or higher)

BY COMPANY REVENUE

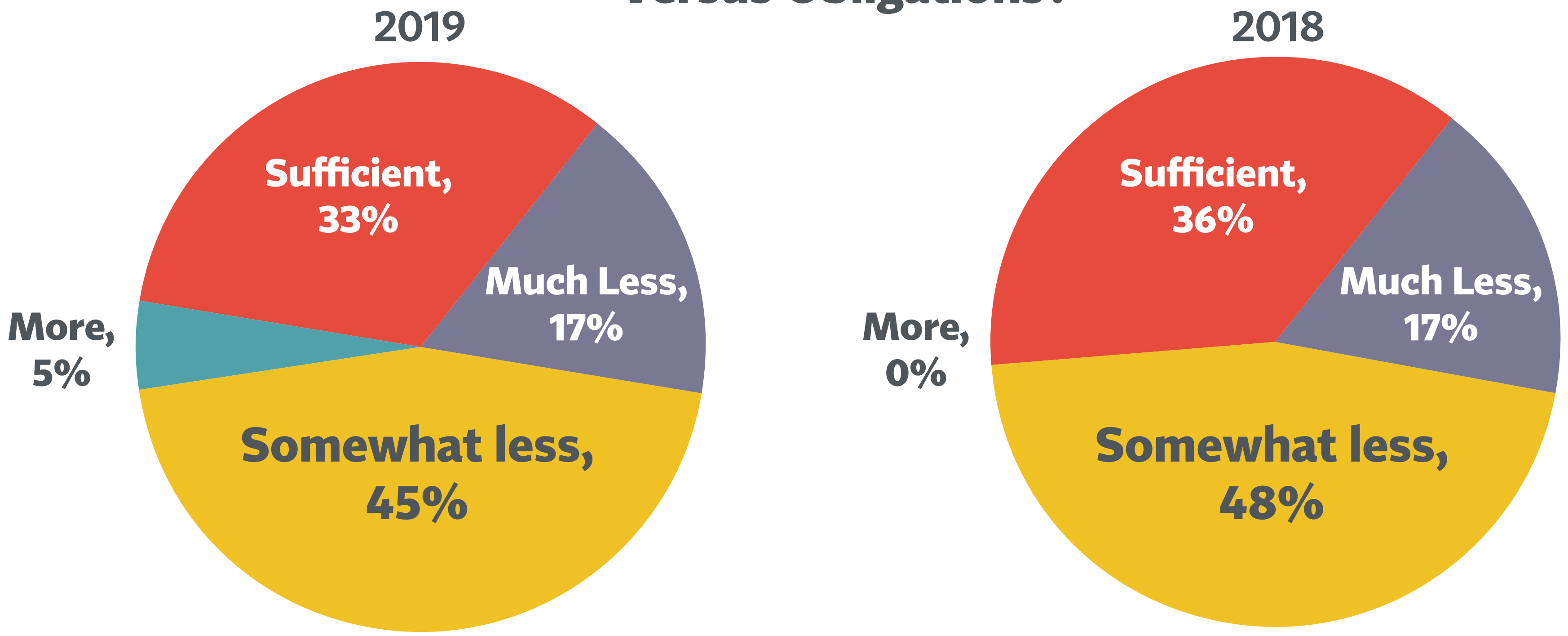
	Under $100M*		$100M-$999M*		$1B-$24.9B		$25B+*	
	2019	2018	2019	2018	2019	2018	2019	2018
Total privacy spend (000)	$356.7	$419.4	$253.9	$707.0	$1,037.5	$1,636.8	$1,556.2	$1,112.5
Privacy spend per employee	$207	$254	$179	$264	$85	$120	$8	$7

* Small sample size

F4: And what is the total privacy spend for your company in each of the following categories?

Feeling the budget squeeze: 62% feel their privacy budget is insufficient to meet their obligations

How Sufficient Is Privacy Budget Versus Obligations?



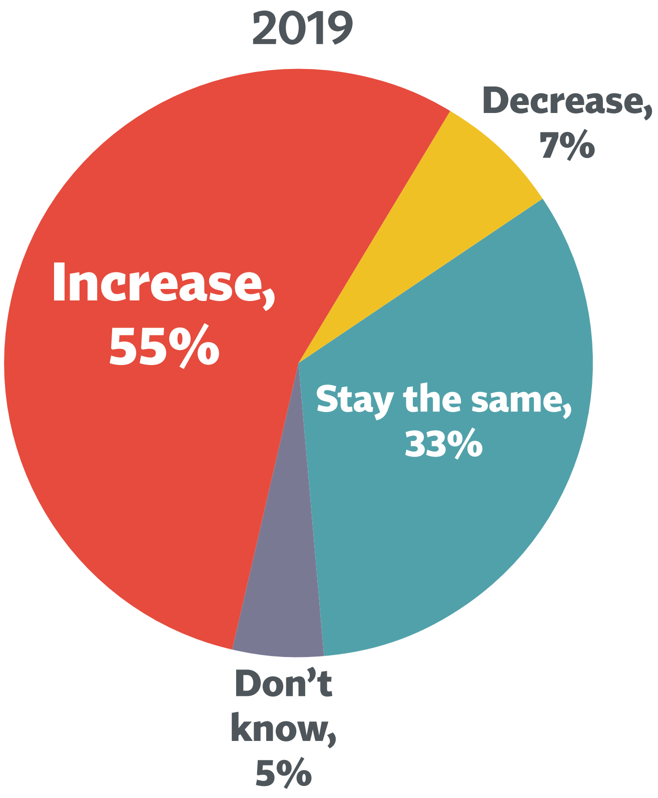
TOTAL WHO SAY LESS THAN SUFFICIENT

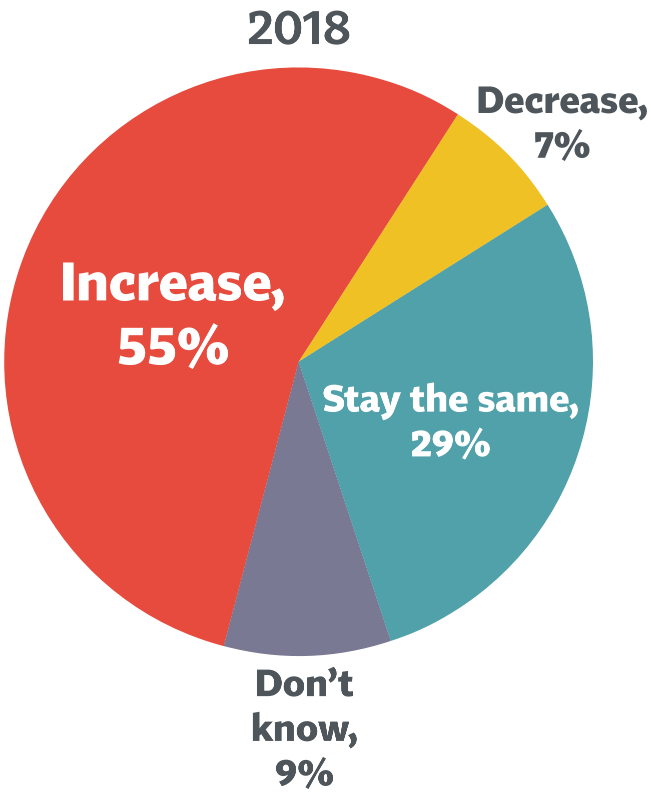
2019: 62%
2018: 65%

F6: In your opinion, your company's privacy budget is ...to meet your privacy obligations.

Wishful thinking? Despite lower privacy spending this year, half of privacy pros still expect budgets to rise

In Next 12 Months, Privacy Budget Will…

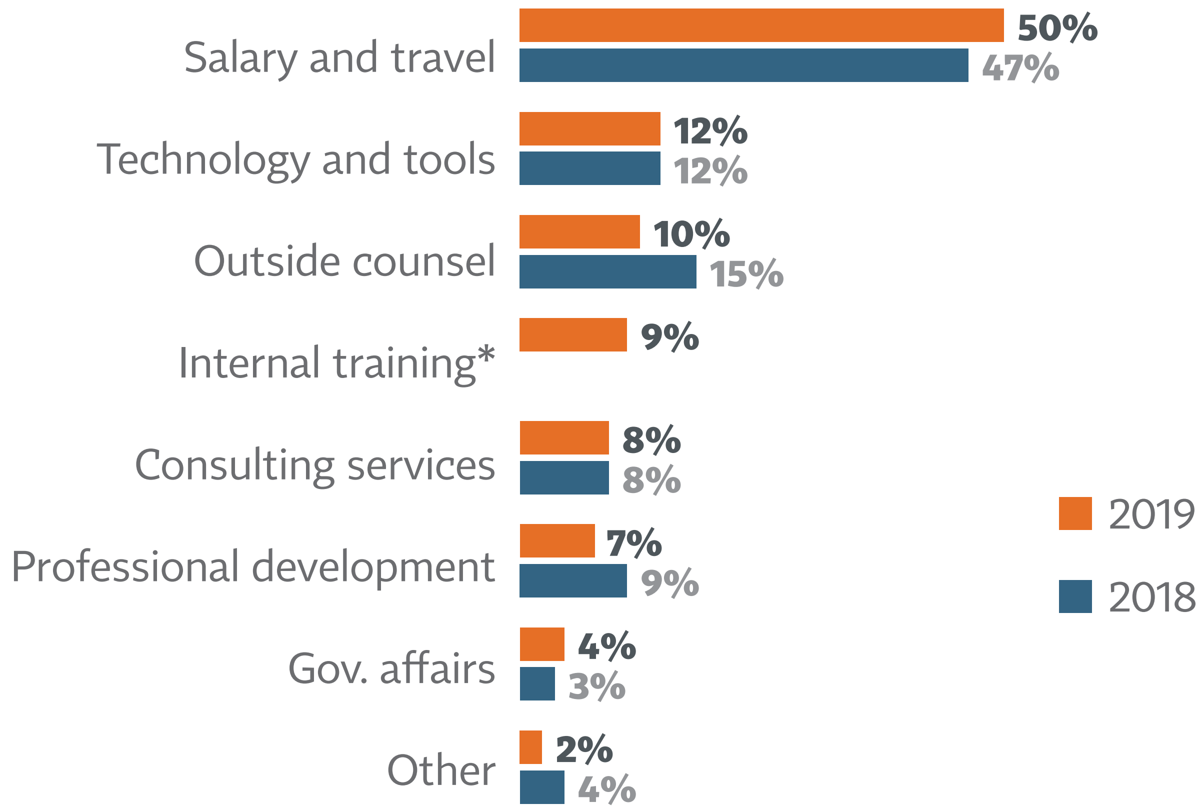




F5: In the next 12 months, you expect your company's privacy budget will …

Outside counsel received a smaller share of the privacy budget this year compared to last

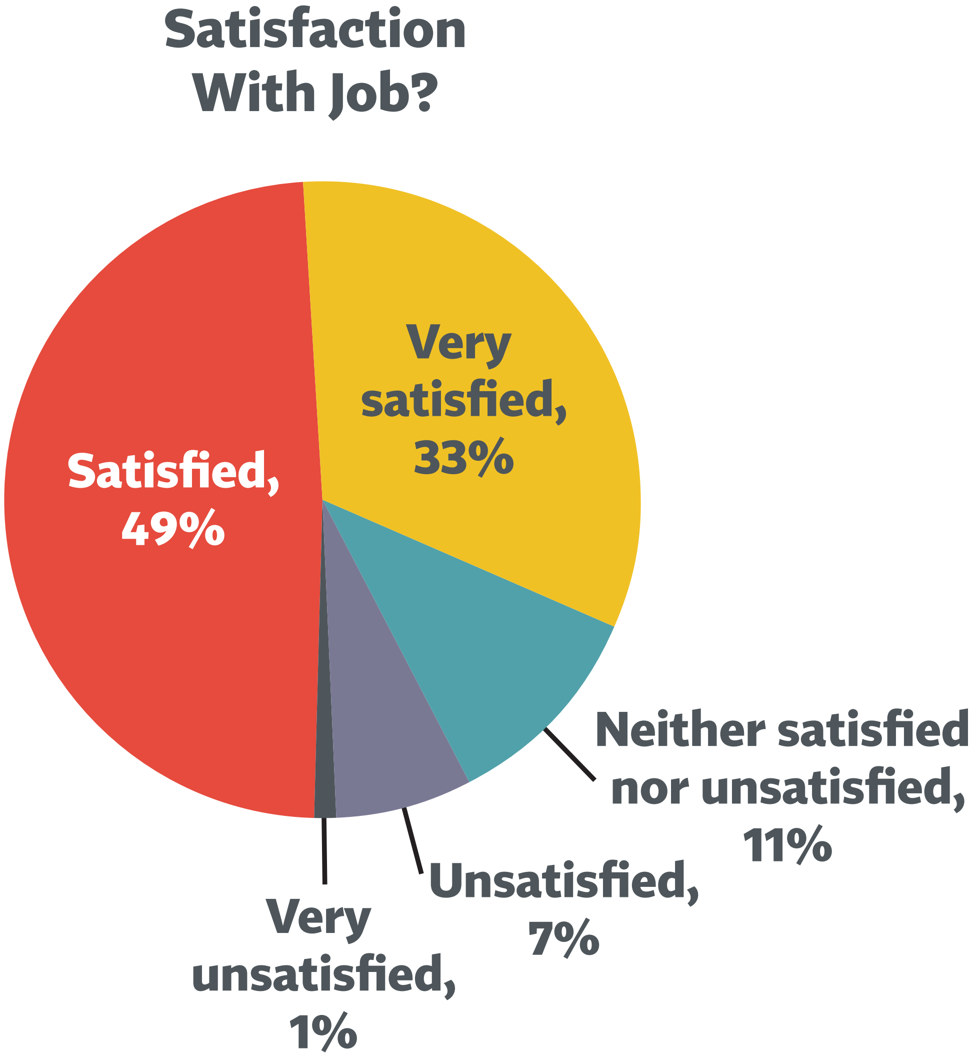
Distribution of Privacy Budget Components

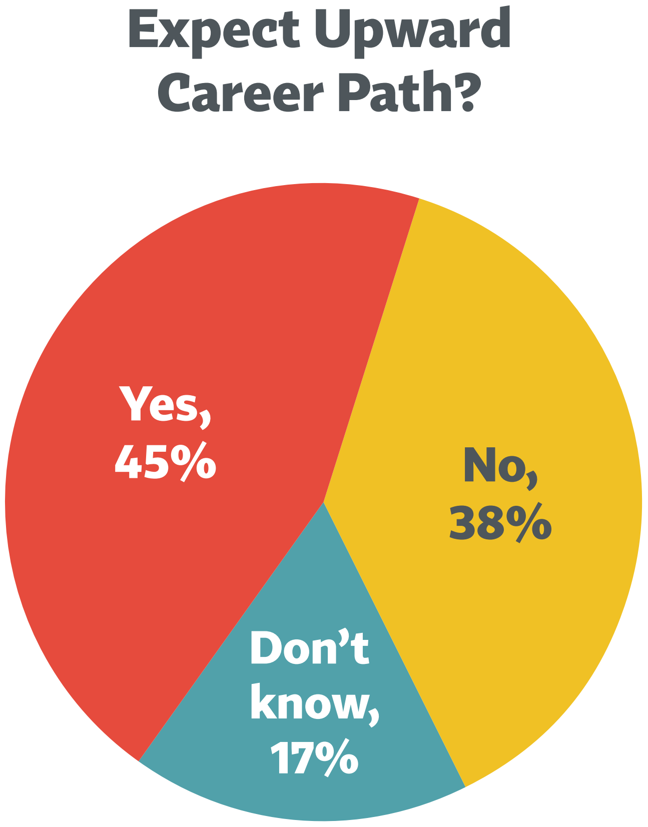


*Not included in 2018

F3: What percent of your company's total privacy budget is allocated to each of the following components?

The overwhelming majority of privacy pros are happy with their jobs; many expect a promotion

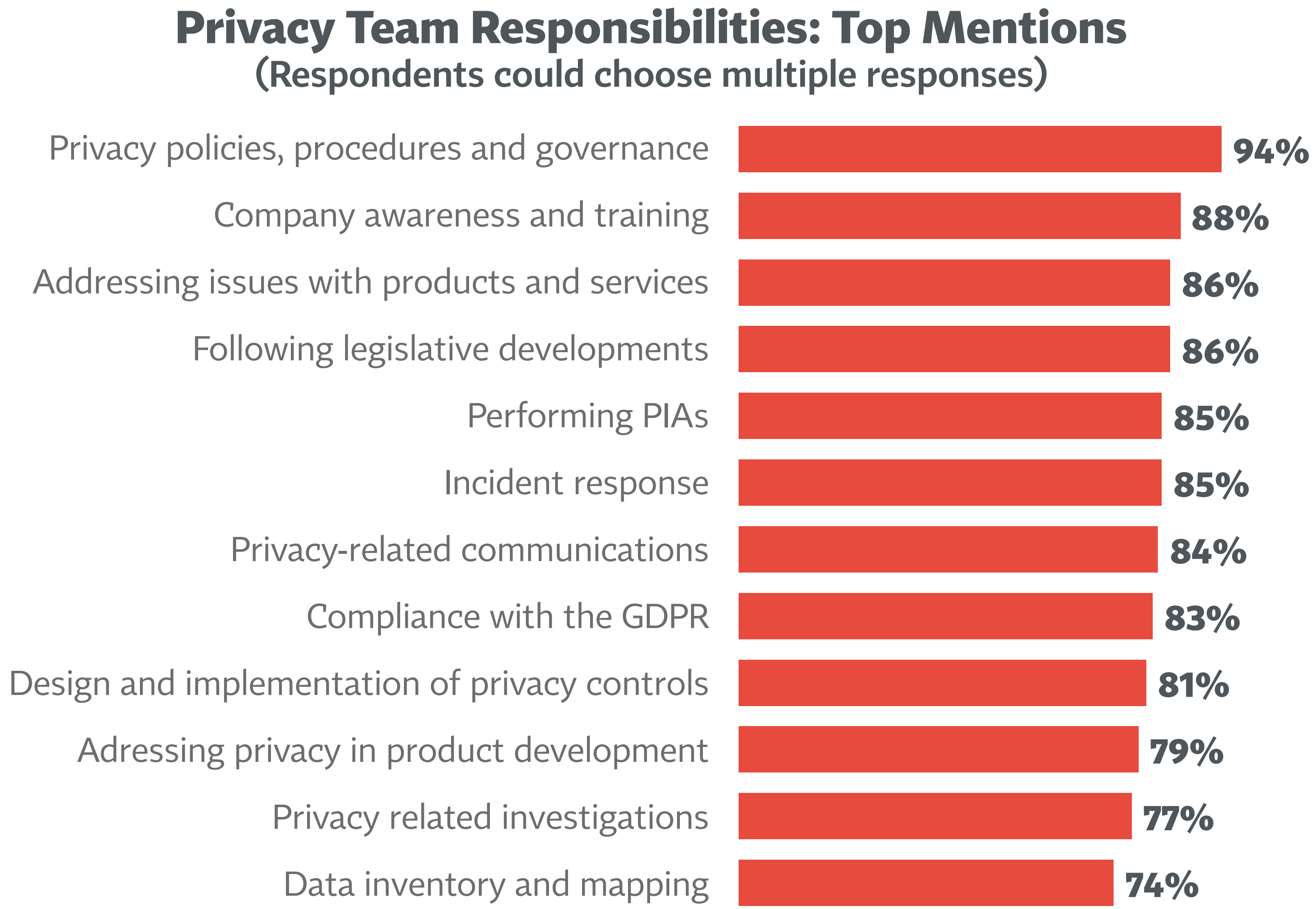




I13: How satisfied are you with your job?
I14: Are you expecting an upwards career trajectory?

Contents

The privacy team's main duties include dealing with privacy policies and companywide training

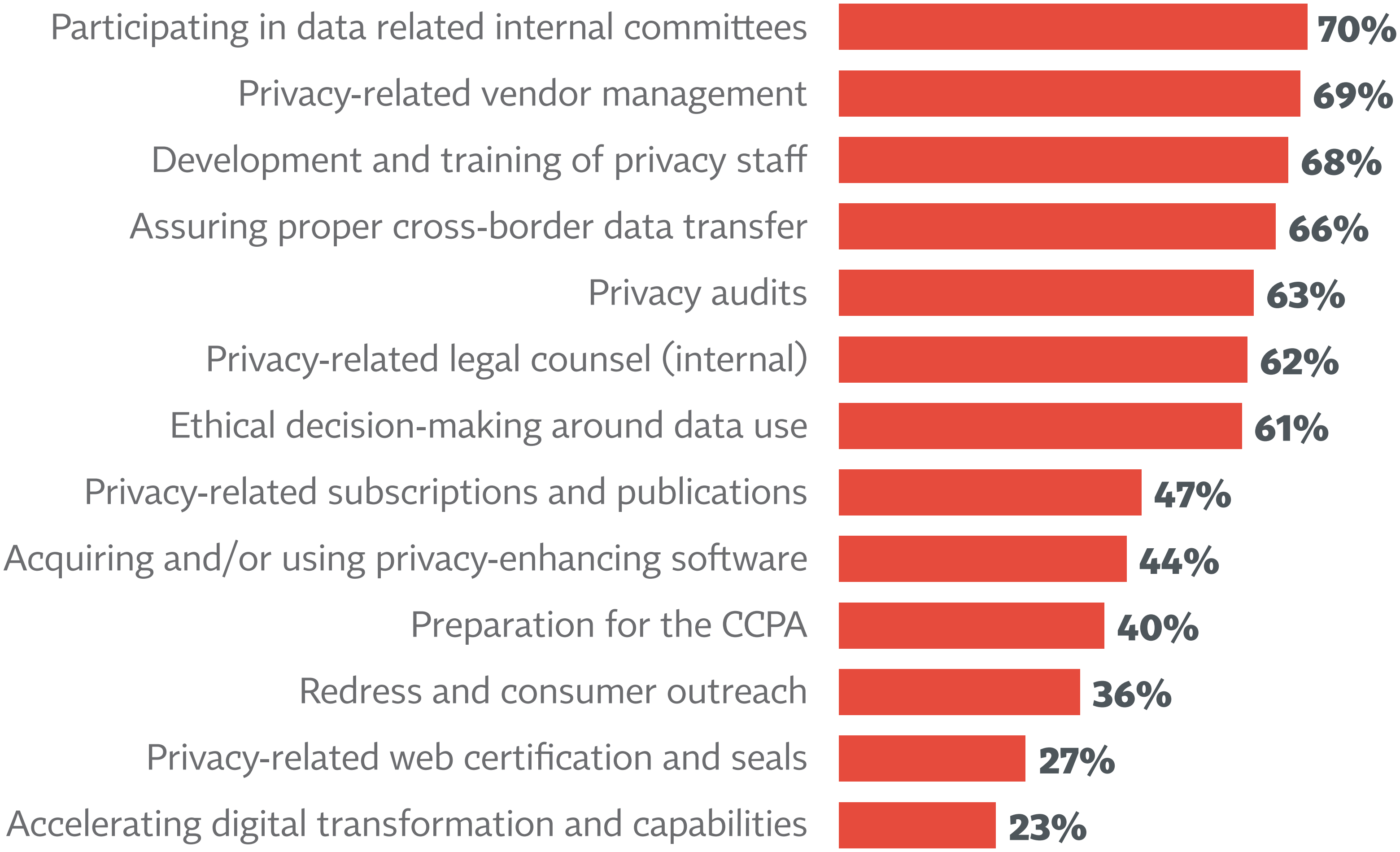


D4: Which of the following is your team responsible for accomplishing on an annual basis?

Redress, certification and seals, and accelerating digital transformation were the least common duties

Privacy Team Responsibilities: Other Mentions

(Respondents could choose as many as they liked)



D4: Which of the following is your team responsible for accomplishing on an annual basis?

EU teams more focused on GDPR, while U.S. teams give more time to managing vendors and CCPA prep

BY RESPONDENT LOCATION

	U.S.	EU
Privacy Responsibilities		
GDPR compliance	72%	97%
Following privacy legislative developments	92%	80%
Vendor management	83%	64%
Ethical decision-making around data use	72%	56%
Privacy-related subscriptions and publications	60%	43%
Preparation for the CCPA	80%	17%
Redress and consumer outreach	47%	33%
Privacy-related web certification and seals	38%	21%

B2C firms are less likely than others to be involved in GDPR compliance and privacy-related communication

BY TARGET

	B2B	B2C	Both
Privacy Responsibilities			
Privacy policies, procedures and governance	93%	89%	96%
Companywide privacy-related awareness and training	87%	78%	92%
Addressing privacy issues with existing products and services	84%	81%	90%
Following legislative developments around privacy and data protection	85%	82%	88%
Performing PIAs or DPIAs	86%	73%	88%
Incident response	86%	80%	86%
Privacy-related communications	85%	**67%**	89%
Compliance with the GDPR	87%	**65%**	85%
Guiding the design and implementation of privacy controls	83%	73%	83%
Addressing privacy by design in product development	77%	65%	84%
Privacy-related investigations	78%	73%	78%
Data inventory and mapping	78%	67%	75%

🟥 Significantly different than other segments

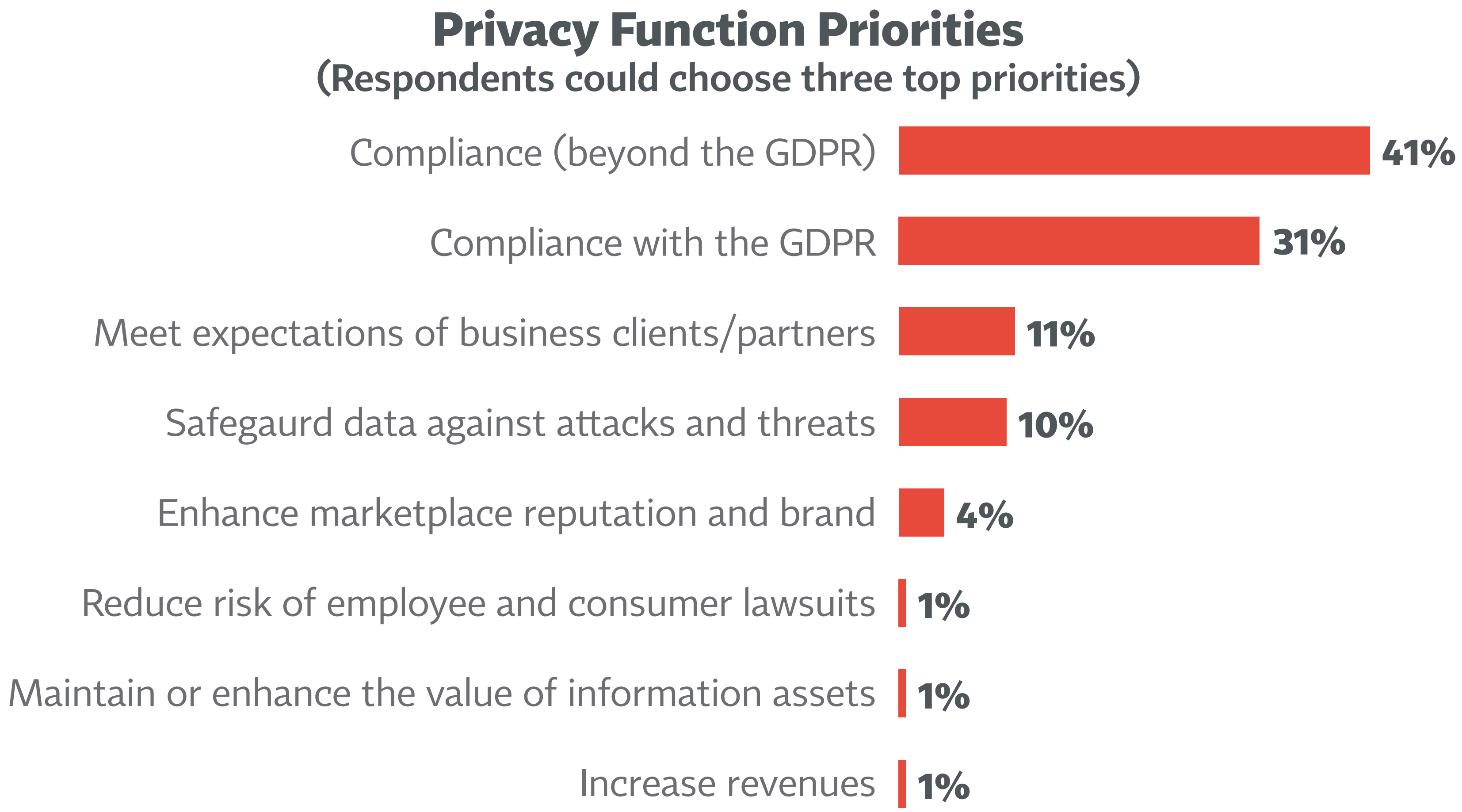
B2C firms are also less likely to engage in cross-border data transfers and internal legal counsel matters

BY TARGET

	B2B	B2C	Both
Privacy Responsibilities			
Participating in data related internal committees	67%	56%	75%
Privacy-related vendor management	73%	61%	70%
Development and training specifically of privacy staff	63%	60%	73%
Assuring proper cross-border data transfer	71%	**48%**	68%
Privacy audits	61%	56%	66%
Privacy-related legal counsel (internal)	65%	**43%**	67%
Ethical decision-making around data use	59%	51%	66%
Privacy-related subscriptions and publications	45%	33%	53%
Acquiring and/or using privacy-enhancing software	42%	39%	48%
Preparation for the CCPA	45%	27%	40%
Redress and consumer outreach	26%	32%	43%
Privacy-related web certification and seals	34%	20%	24%
Accelerating digital transformation and digital capabilities	22%	21%	25%

🟥 Significantly different than other segments

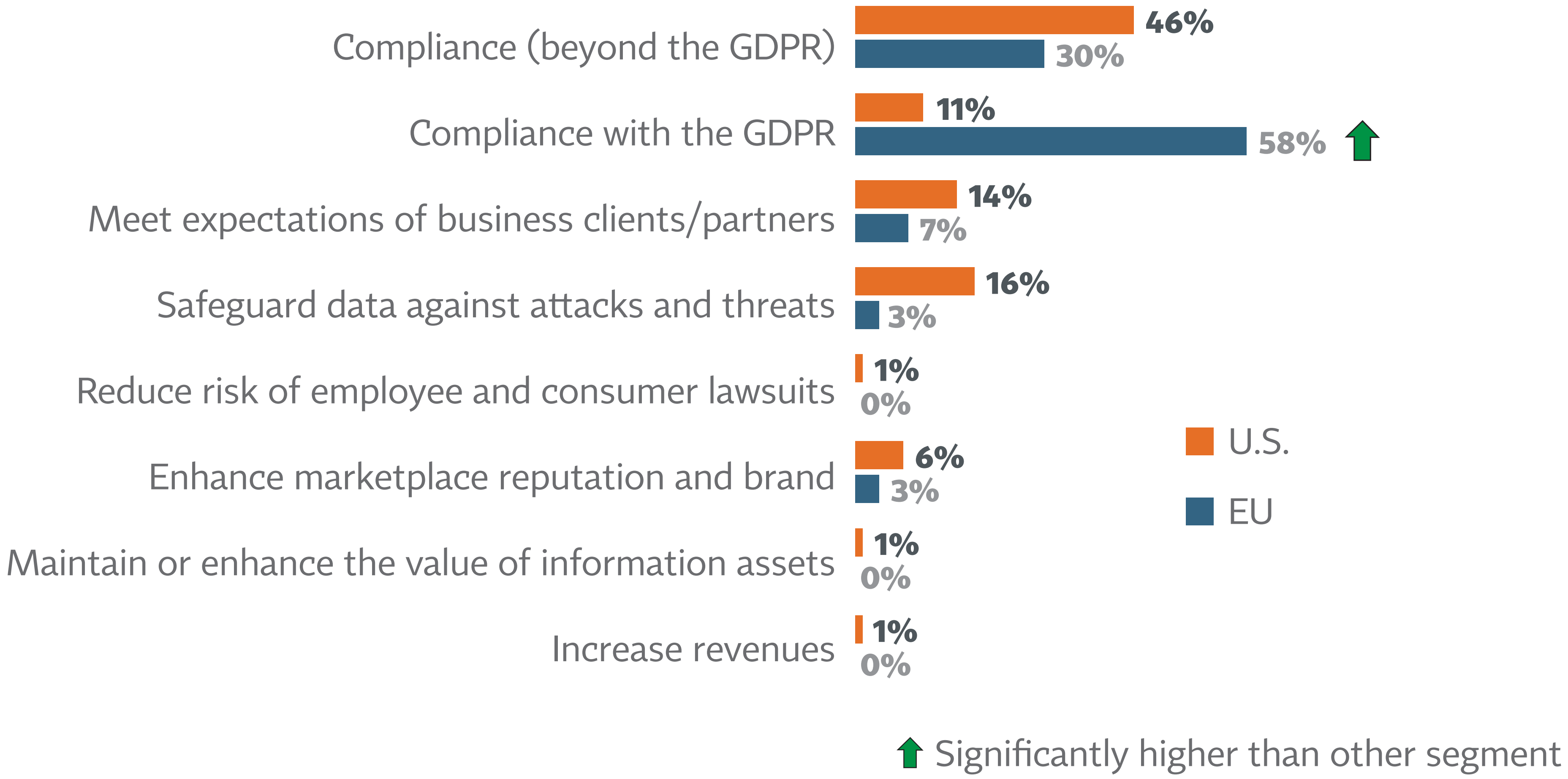
When asked to choose the team's most critical responsibilities, most pros say it is compliance



E3: Which of the following is the highest priority within your privacy program. NOTE: Question asked differently in 2018 versus prior years.

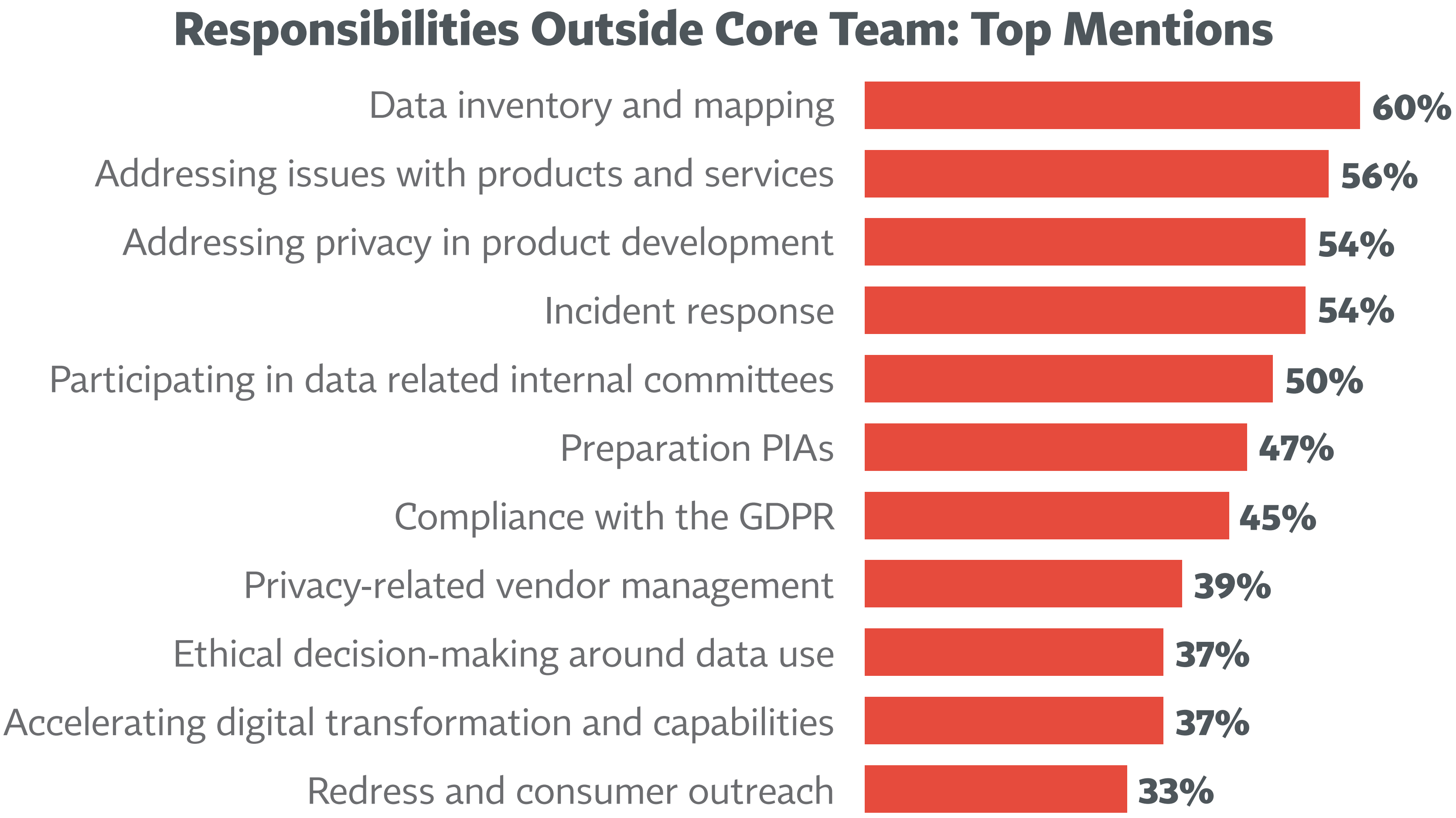
EU pros focus on GDPR compliance, while U.S. pros prioritize client expectations and threat mitigation

Privacy Function Priorities
(Respondents could choose three top priorities)



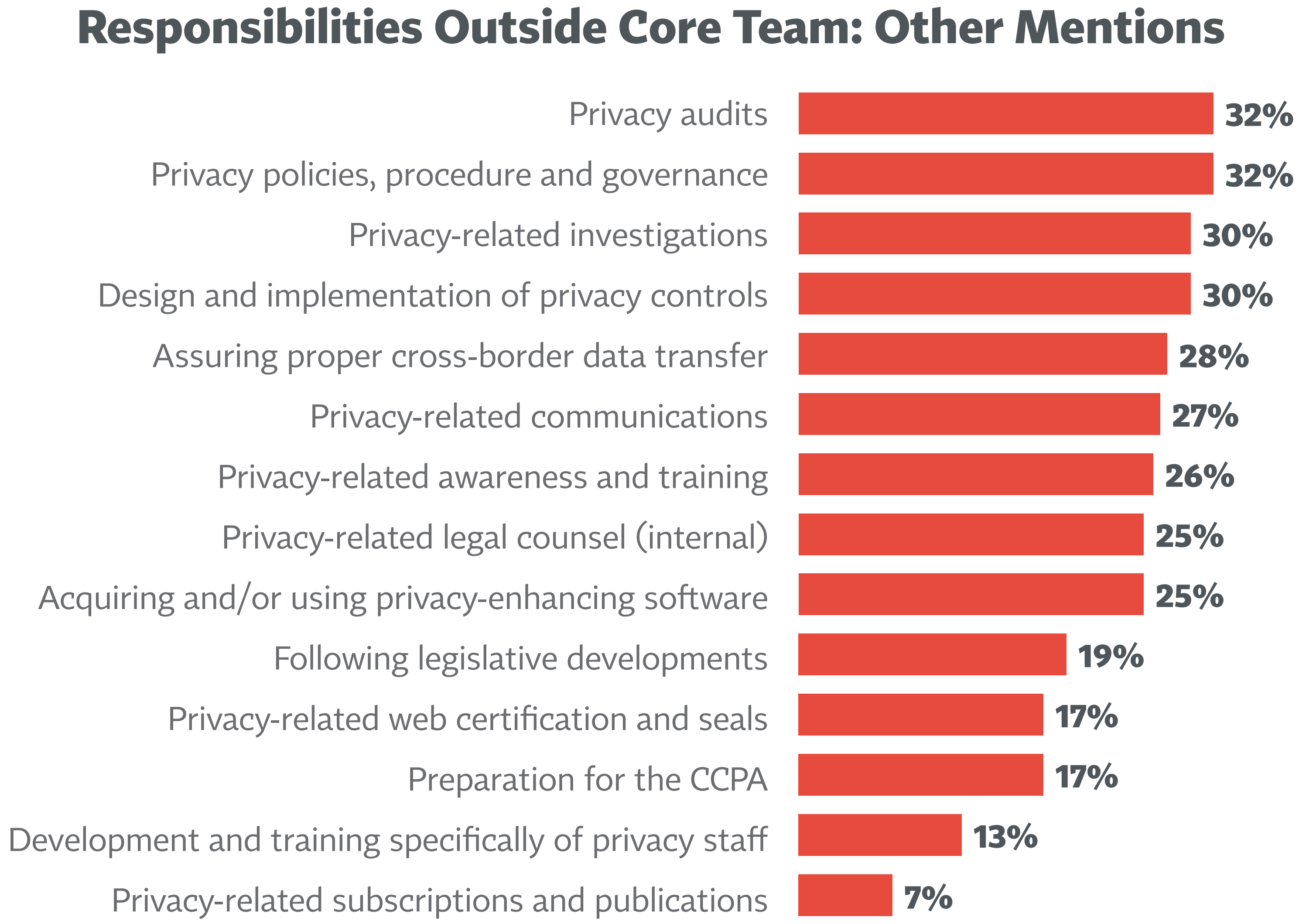
E3: Which of the following is the highest priority within your privacy program?

Data inventory/mapping and product/service issues are top privacy duties for those outside the core team



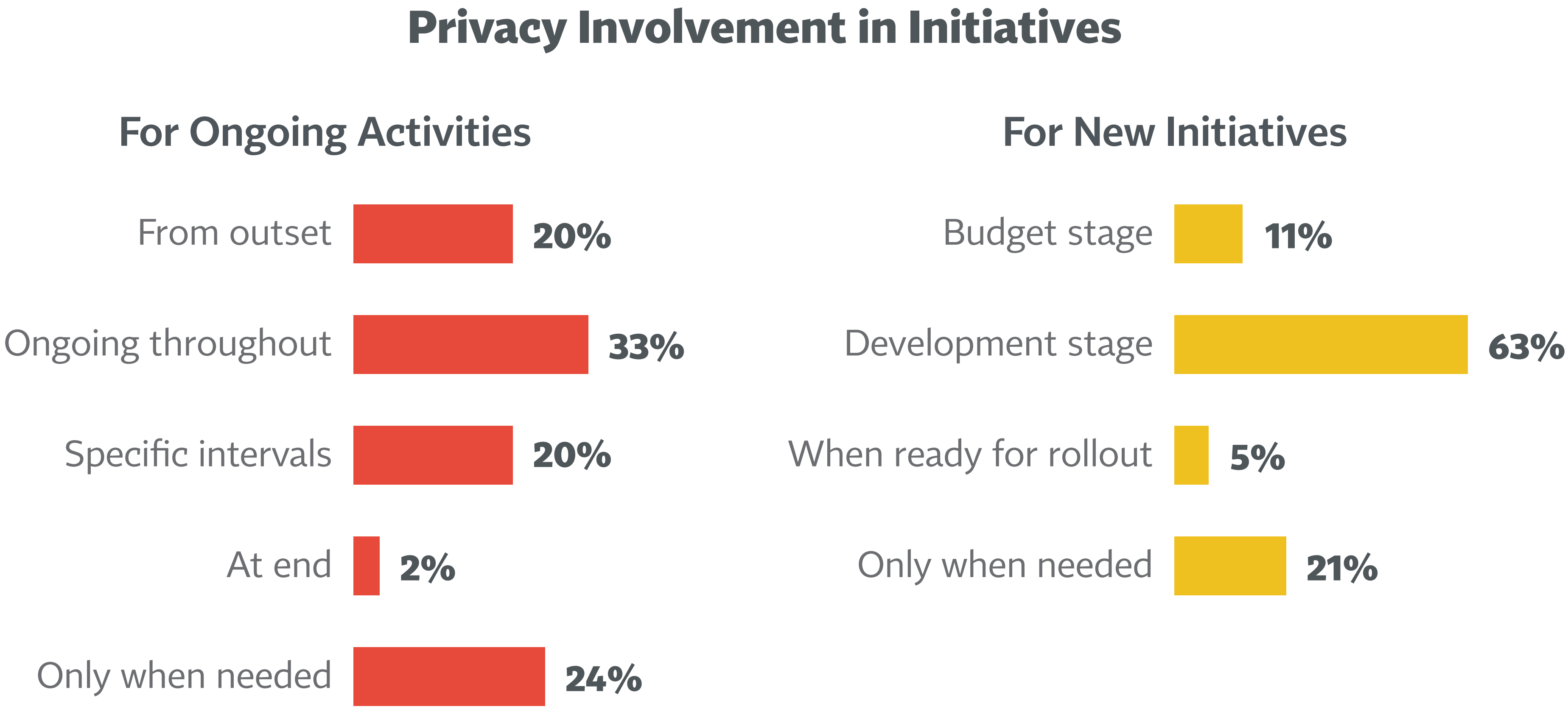
D5: Next, for employees who are OUTSIDE the privacy team generally but have privacy responsibilities, which of the following are they responsible for accomplishing on an annual basis, whether or not you personally are involved?

CCPA preparation, privacy staff training and subscriptions/ publications rank lowest for outside team



D5: Next, for employees who are OUTSIDE the privacy team generally but have privacy responsibilities, which of the following are they responsible for accomplishing on an annual basis, whether or not you personally are involved?

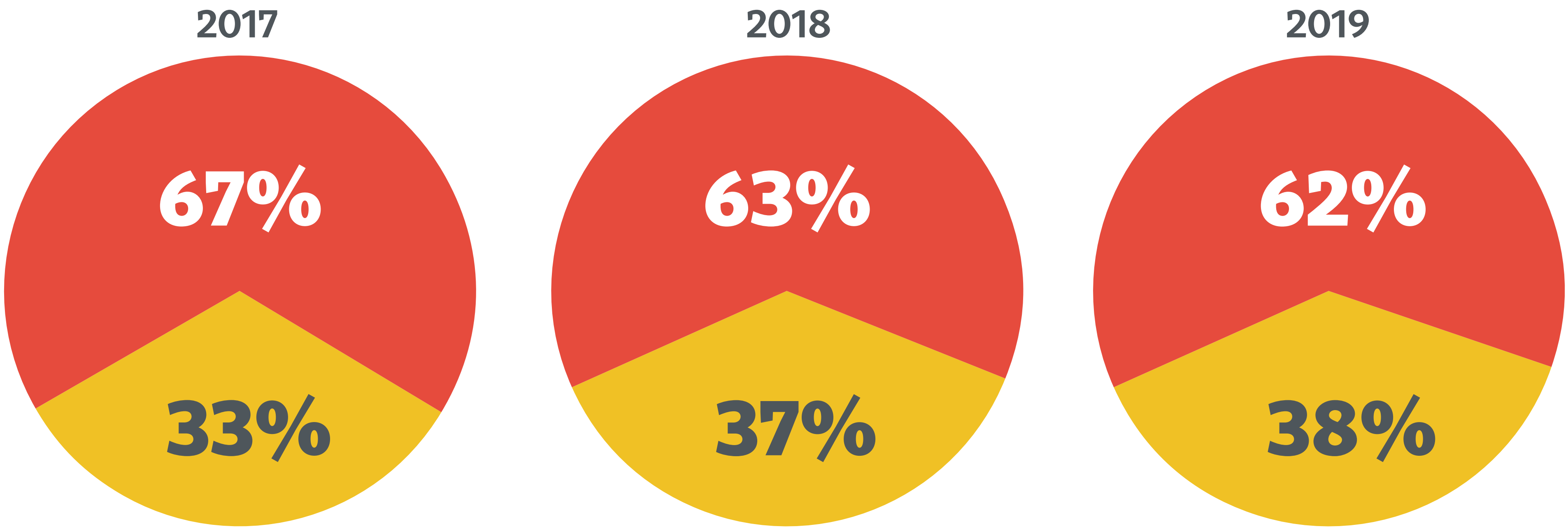
For new and ongoing initiatives, privacy is involved early, as well as throughout the process



G5: In a general sense, for ongoing activities within your company that may involve privacy-related information, representatives of the privacy function are involved …
G6: Now thinking strictly about new projects or initiatives established by your company that may involve privacy, representatives of the privacy program are involved …

For nearly 4 out of 10 privacy pros, 100% of their job is doing privacy-related work

Privacy as Percent of Job



🟥 % saying privacy is less than 100% of job
🟨 % saying privacy is 100% of job

PRIVACY AS % OF TOTAL JOB (MEDIAN)
2019: 85%
2018: 85%
2017: 80%

RESPONDENT IS PRIVACY LEADER
2019: 70%
2018: 67%
2017: 68%

D1: About what proportion of your work at your company is made up of privacy responsibilities?

Predictably, pros at smaller and lower-revenue firms tend to spend less of their time on privacy

BY EMPLOYEE SIZE

	<5K	5K-24.9K	25K-74.9K*	75K+*
Median % of time spent on privacy	71%	90%	100%	100%

BY COMPANY REVENUE

	Under $100M	$100M-$999M	$1B-$24.9B	$25B+*
Median % of time spent on privacy	70%	80%	100%	100%

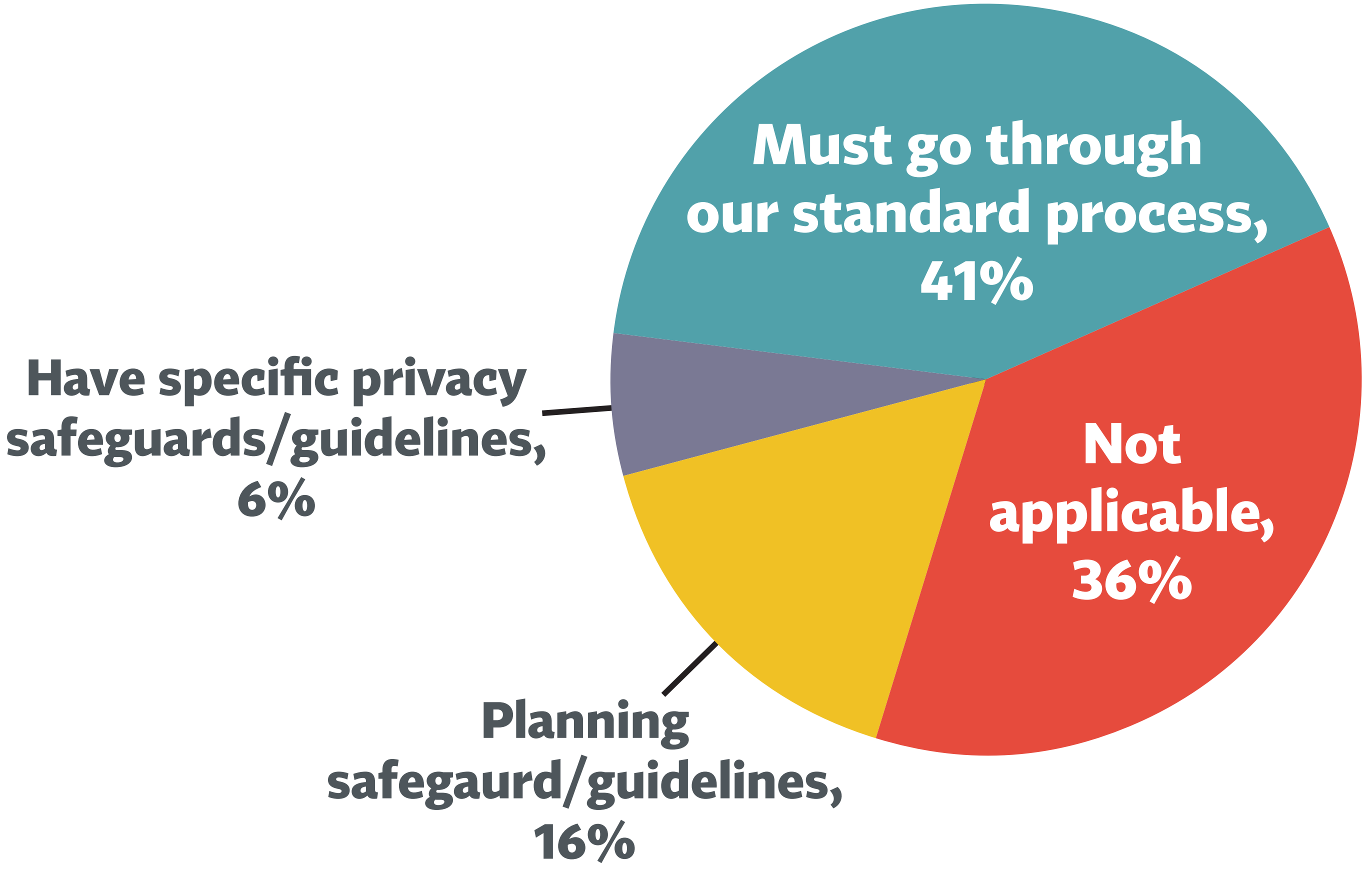
BY HQ LOCATION

	U.S.	EU
Median % of time spent on privacy	90%	85%

* Small sample size

4 in 10 privacy pros say that AI/ML must abide by standard processes, while equal amount say they are not applicable

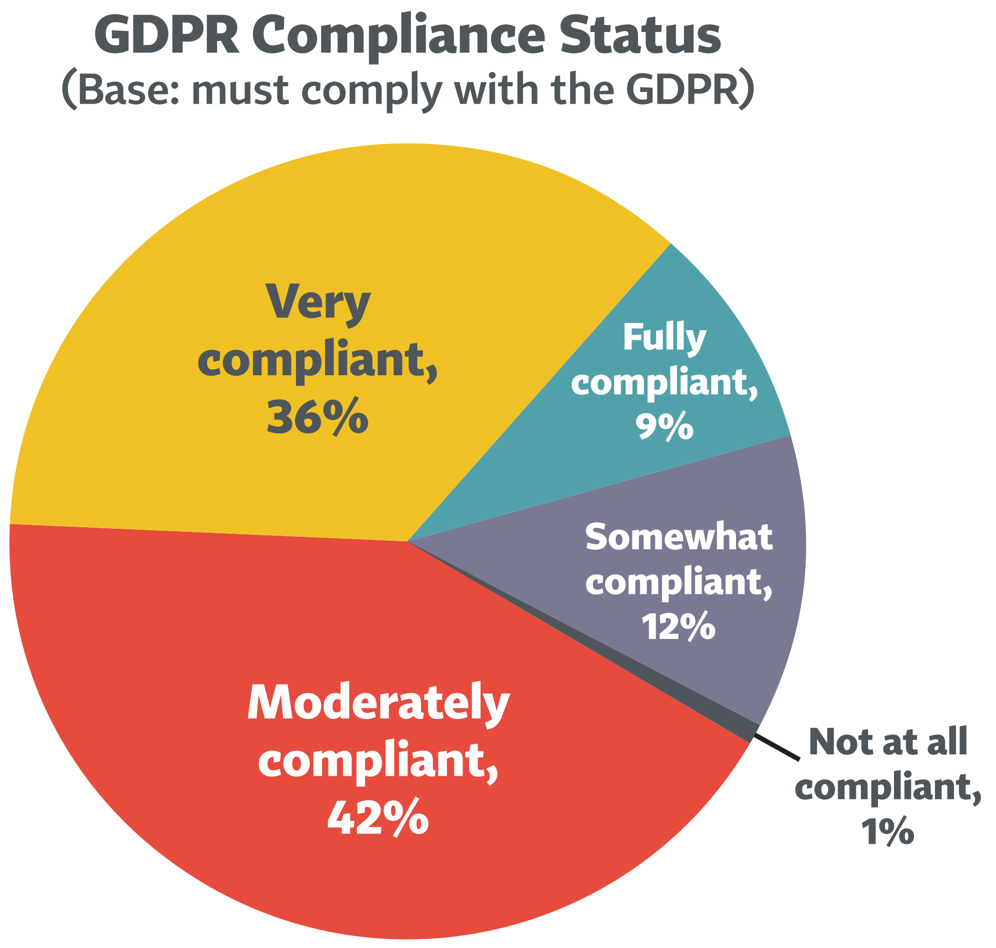
Impact of Privacy Risks on AI or ML



F40: To what extent do privacy risks factor into your artificial intelligence or machine learning strategy or processes?

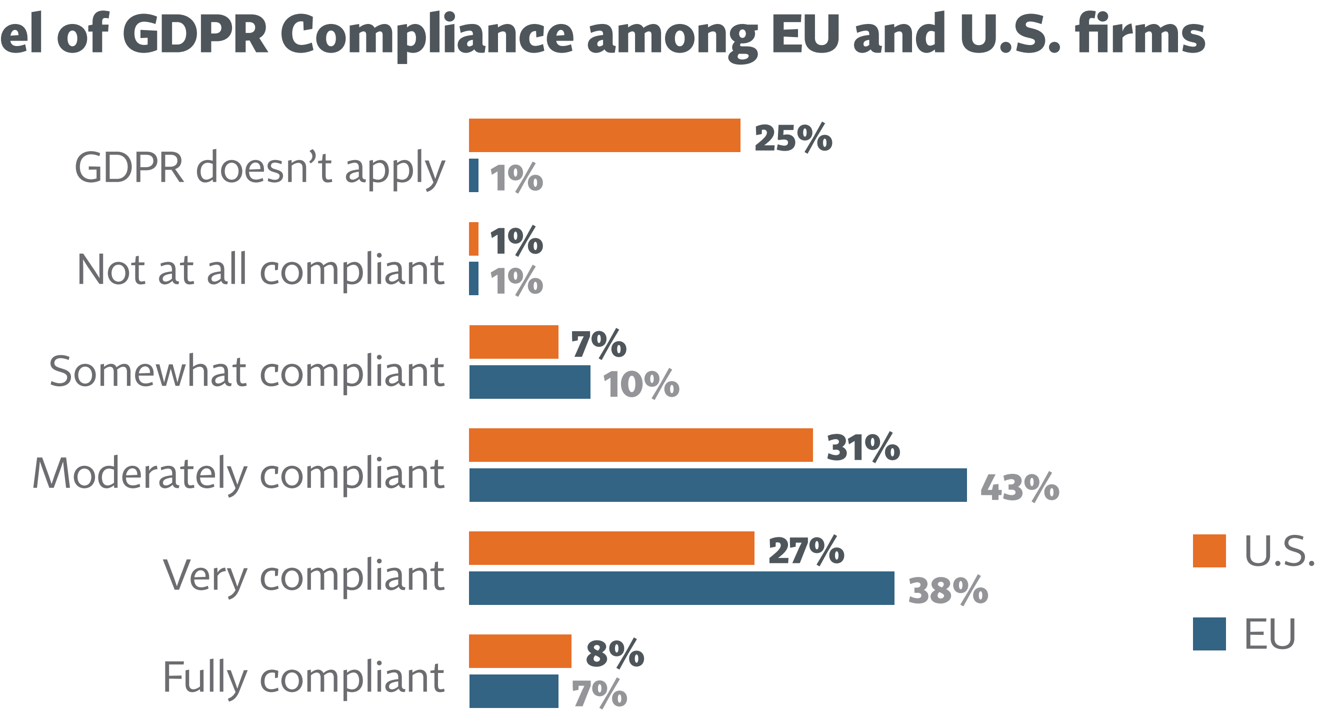
Contents

More than a year after implementation, fewer than half say they are "fully" or "very" GDPR compliant



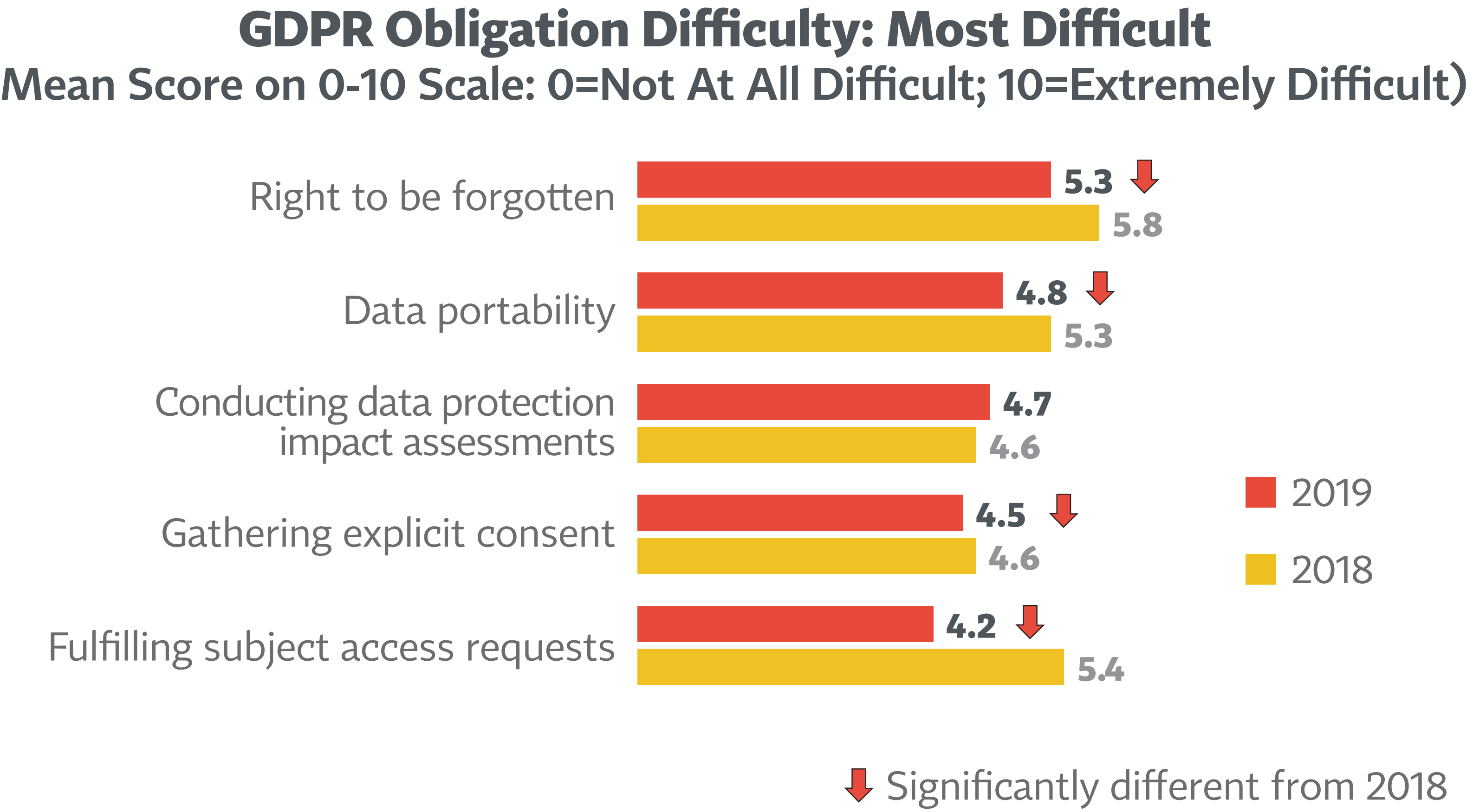
J18: All things considered, how would you rate your current level of GDPR compliance?

EU-based companies are more likely to feel compliant with GDPR; 1 in 4 U.S. firms say it doesn't apply



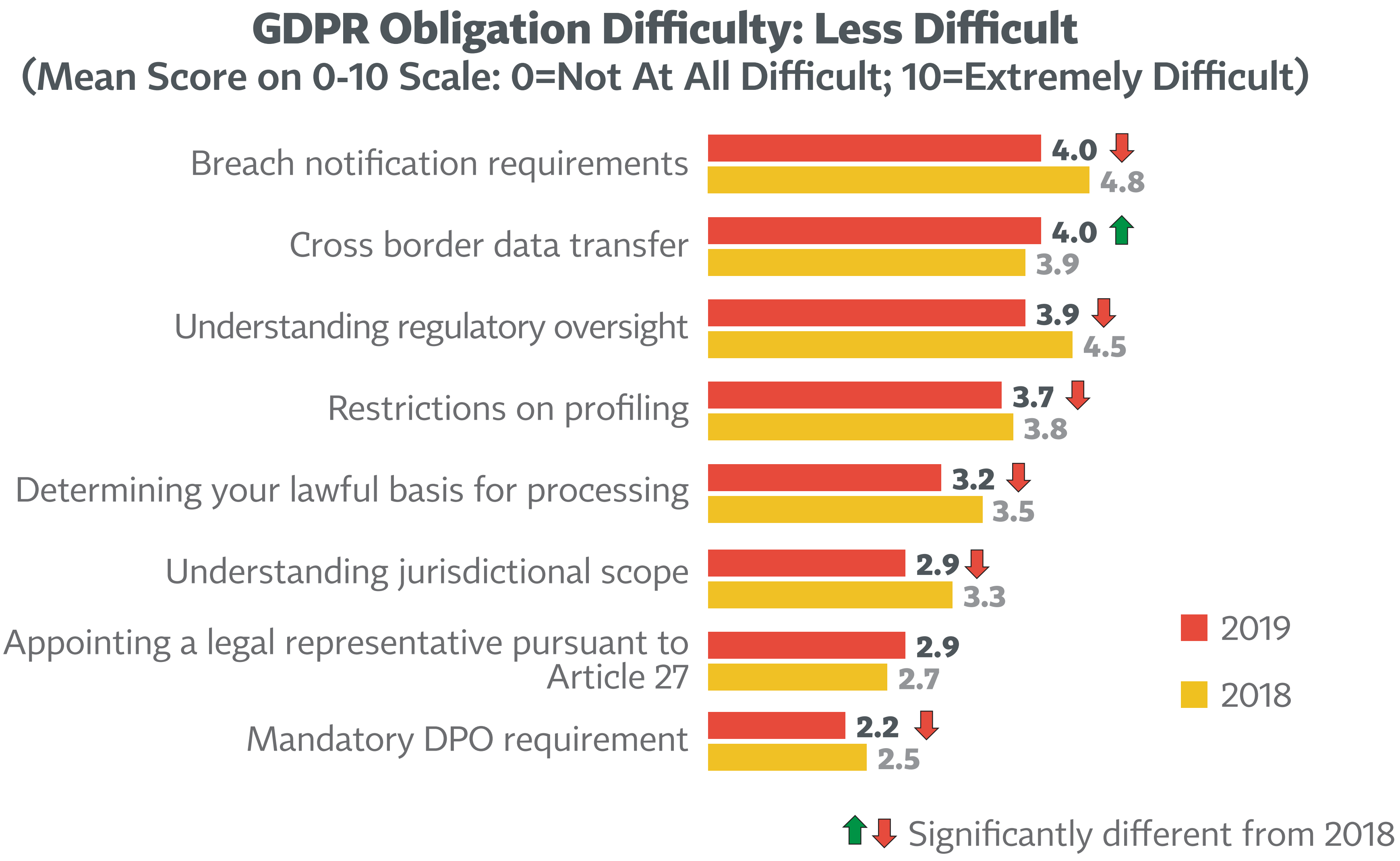
J18: All things considered, how would you rate your current level of GDPR compliance?

Fulfilling core GDPR obligations is perceived as easier for companies over the past year



J8: Rate the following legal obligations of the GDPR in terms of how difficult they are for your company to comply.

Cross-border data transfers is the only obligation that is perceived as more difficult since last year

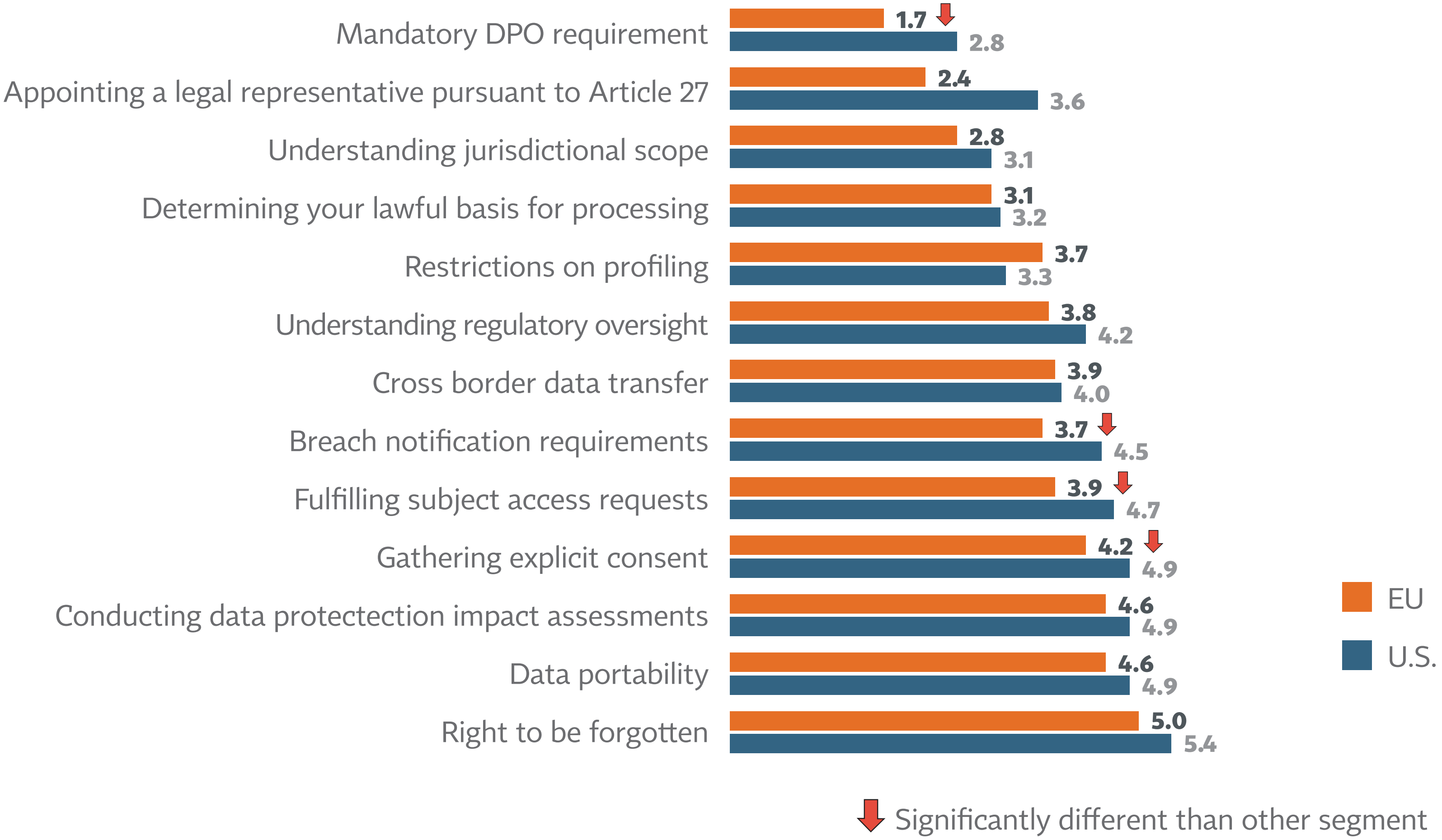


J8: Rate the following legal obligations of the GDPR in terms of how difficult they are for your company to comply.

U.S. firms generally consider GDPR obligations more difficult than EU firms

GDPR Obligation Difficulty: Higher Than Average Concerns by U.S. HQ Firms

(Mean Score on 0-10 Scale: 0=Not At All Difficult; 10=Extremely Difficult)



J8: Rate the following legal obligations of the GDPR in terms of how difficult they are for your company to comply.

Consent, access requests, breach notifications and DPO requirement are particularly difficult for U.S. firms

GDPR Obligation Difficulty

(Mean Score on 0-10 Scale: 0=Not At All Difficult; 10=Extremely Difficult)

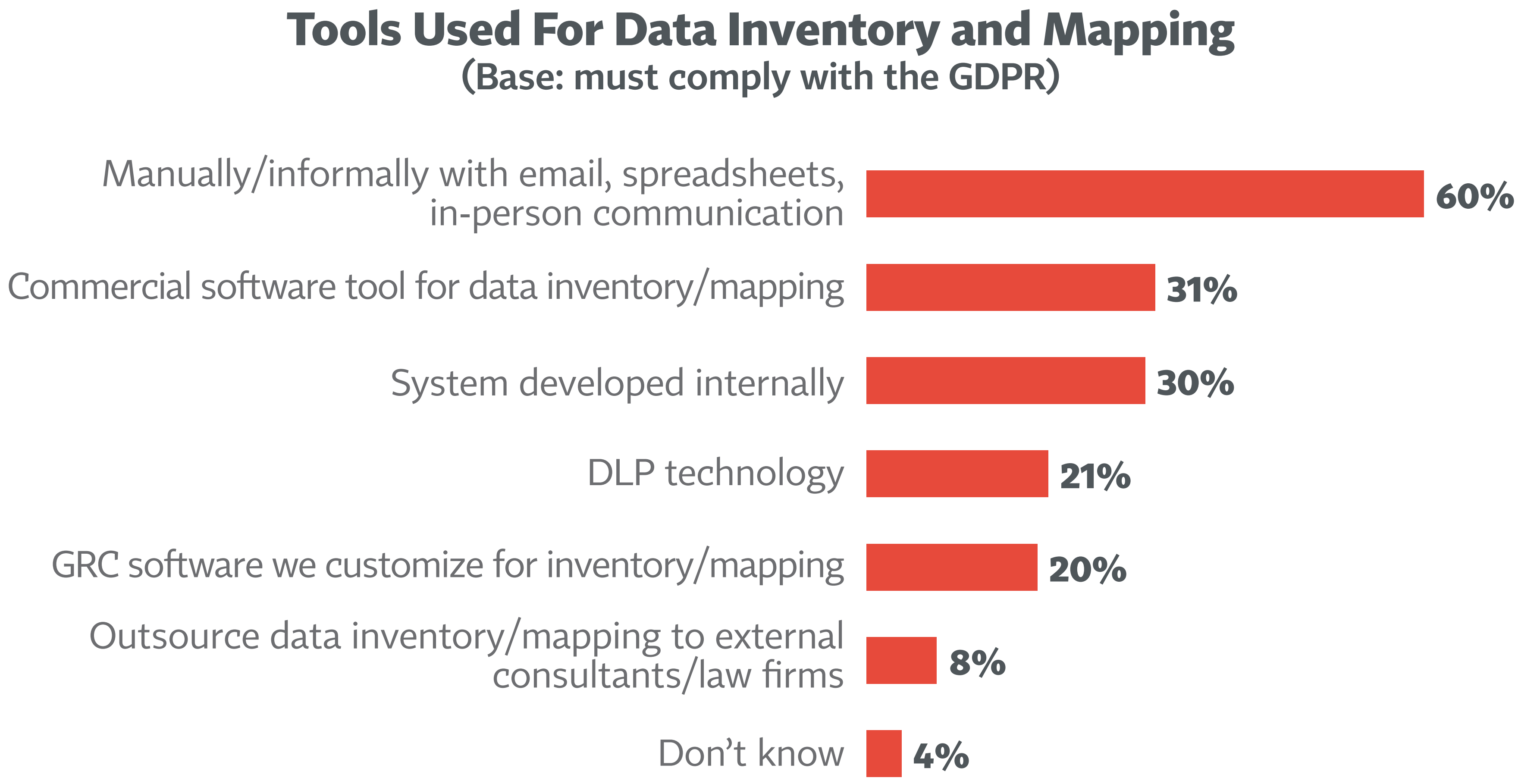
BY HQ LOCATION

	U.S.	EU
Right to be forgotten	5.4	5.0
Data portability	4.9	4.6
Conducting data protection impact assessments	4.9	4.6
Gathering explicit consent	**4.9**	4.2
Fulfilling subject access requests	**4.7**	3.9
Breach notification requirements	**4.5**	3.7
Cross border data transfer	4.0	3.9
Understanding regulatory oversight	4.2	3.8
Restrictions on profiling	3.3	3.7
Determining your lawful basis for processing	3.2	3.1
Understanding jurisdictional scope	3.1	2.8
Appointing a legal representative pursuant to Article 27	3.6	2.4
Mandatory DPO requirement	**2.8**	1.7

🟥 Significantly different than other segment

J8: Rate the following legal obligations of the GDPR in terms of how difficult they are for your company to comply.

Manual methods remain the most common way to do data inventory and mapping

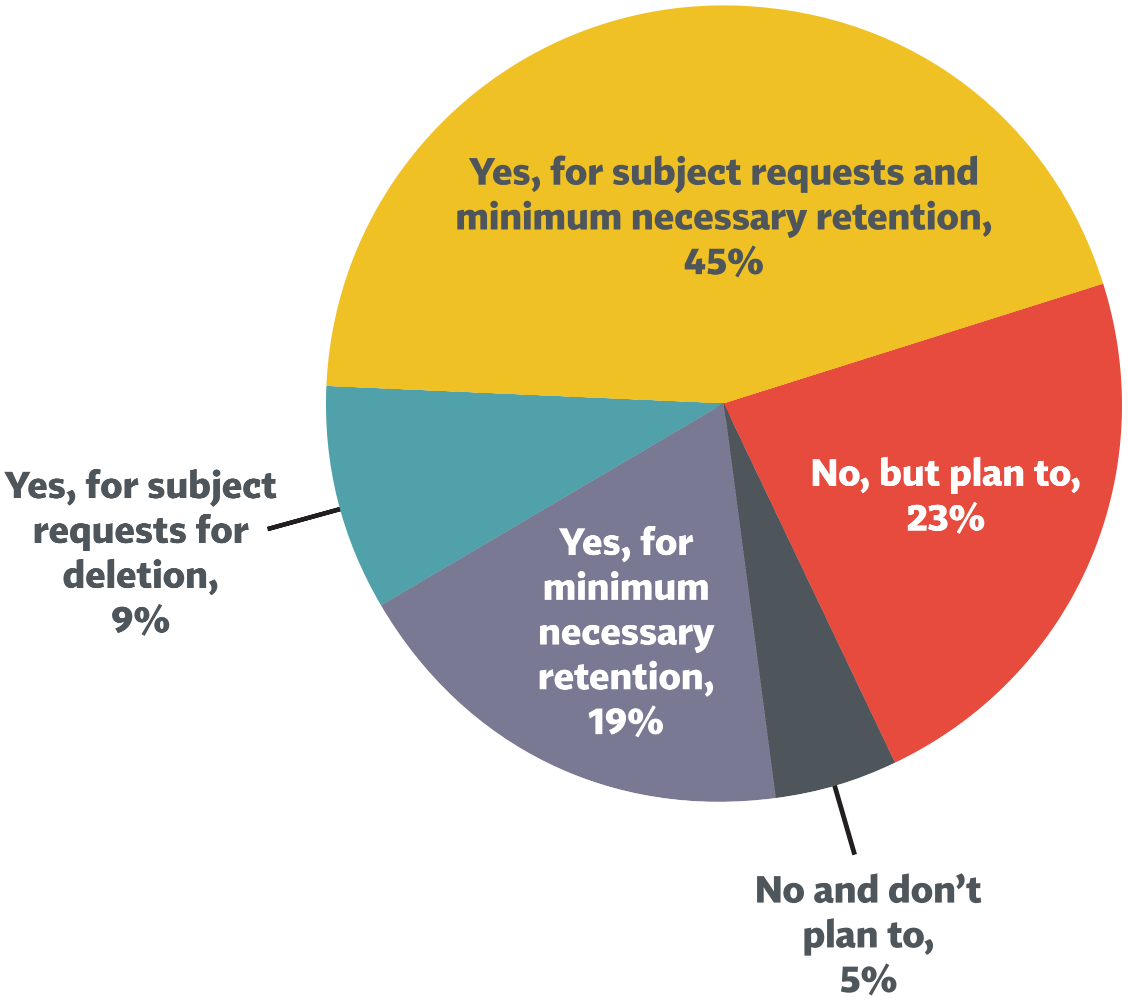


J20: Which of the following tools do you use to conduct data inventory and mapping to meet the record of processing activities requirements of the GDPR?

3 in 4 firms have undertaken data deletion efforts, typically to minimize retention

Data Deletion Efforts Undertaken?

(Base: must comply with the GDPR)

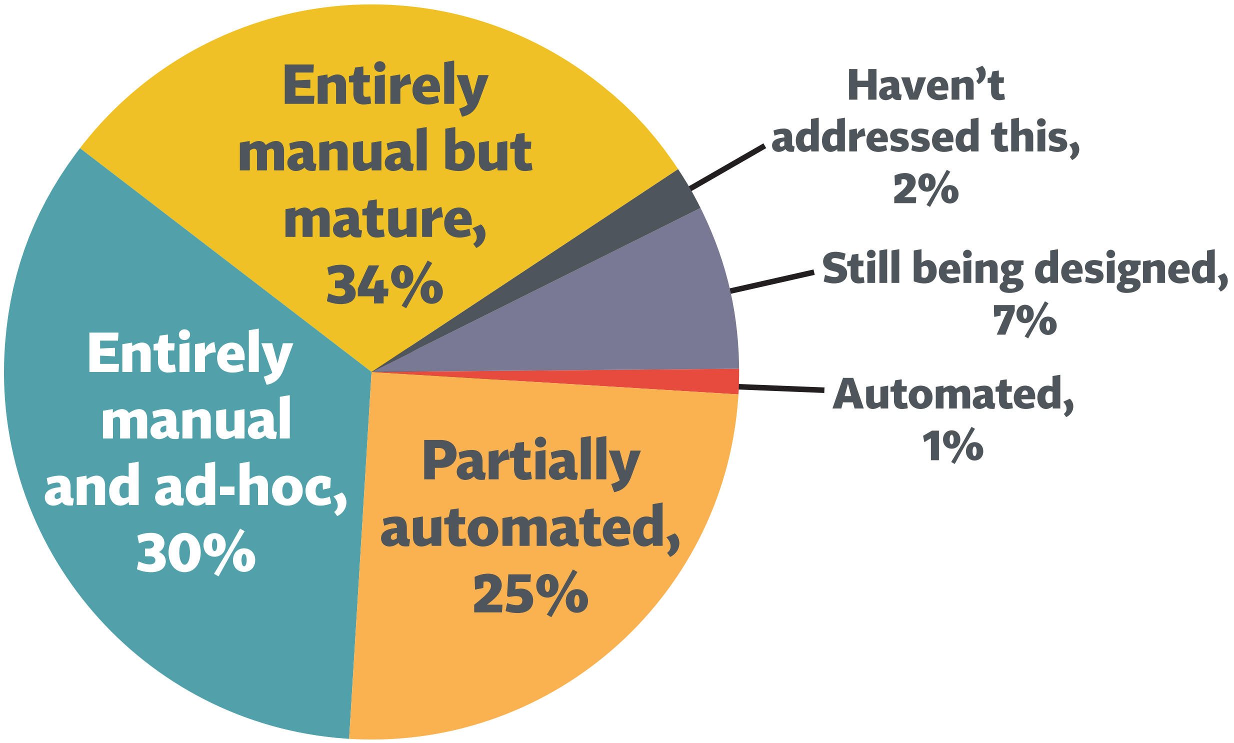


J22: Has your company undertaken efforts specifically aimed at data deletion?

When it comes to DSRs, 2 in 3 handle them entirely manually; 1 in 3 handle them manually and ad hoc

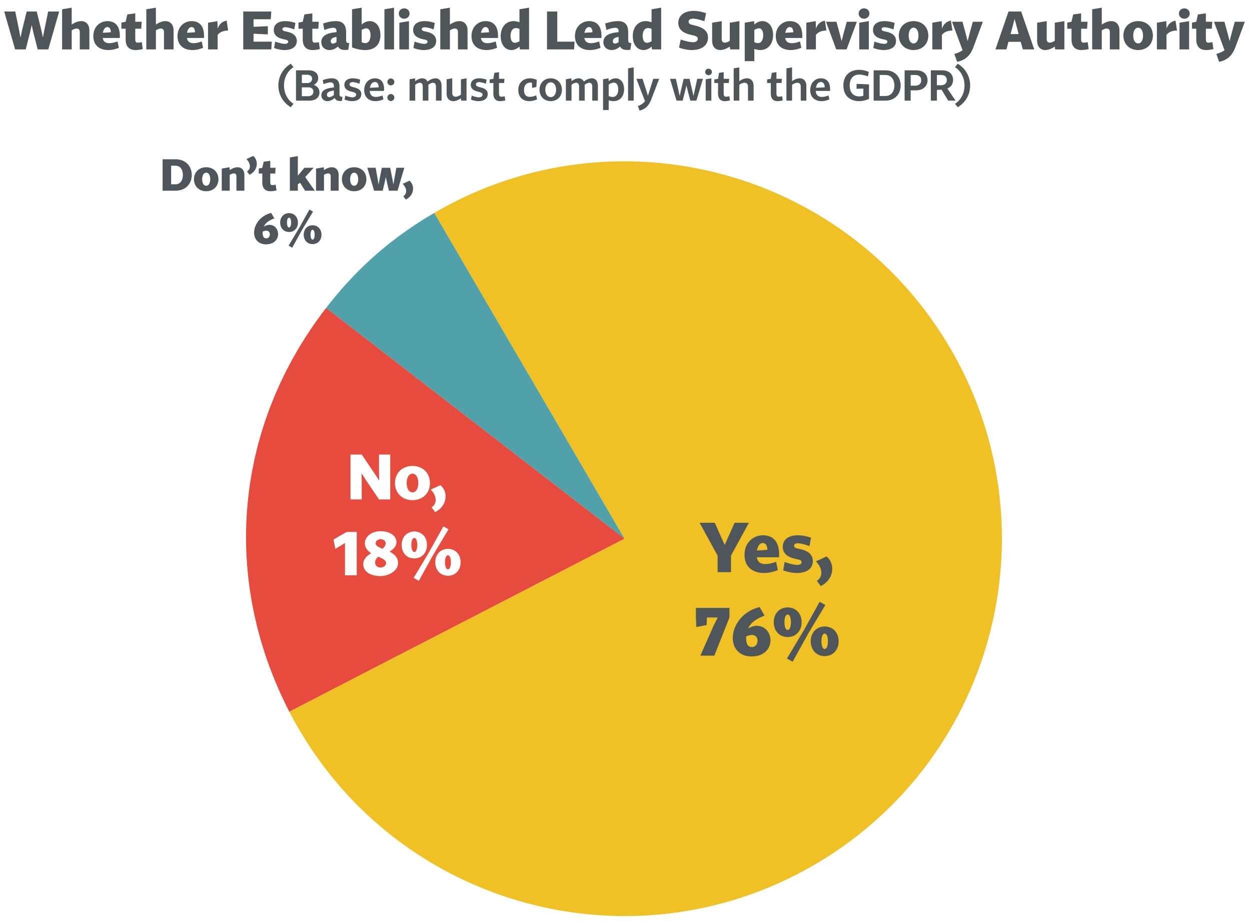
How Handling Data Subject Requests

(Base: must comply with the GDPR)



J23: How is your company addressing data subject requests, such as access, portability, right-to-be-forgotten requests, or objections to processing?

Most firms subject to GDPR have established a lead supervisory authority



J24: Per GDPR regulations, has your company identified a supervisory authority you consider to your “lead supervisory authority”?

As elsewhere, EU firms are more likely than U.S. firms to have established a lead supervisory authority

BY RESPONDENT LOCATION

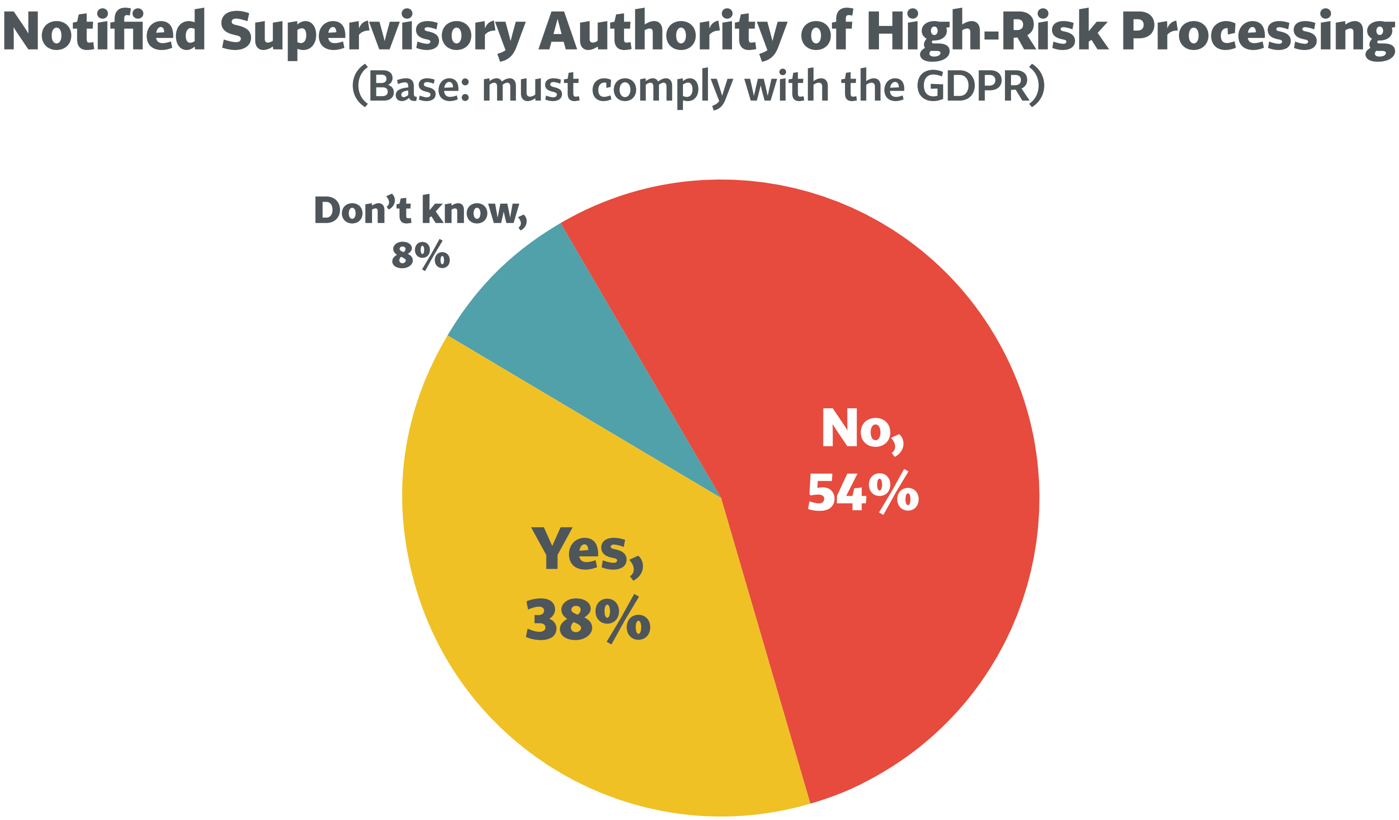
	U.S.	EU
Have identified lead supervisory authority	65%	**89%**

BY HQ LOCATION

	U.S.	EU
Have identified lead supervisory authority	61%	**91%**

🟥 Significantly different than other segment

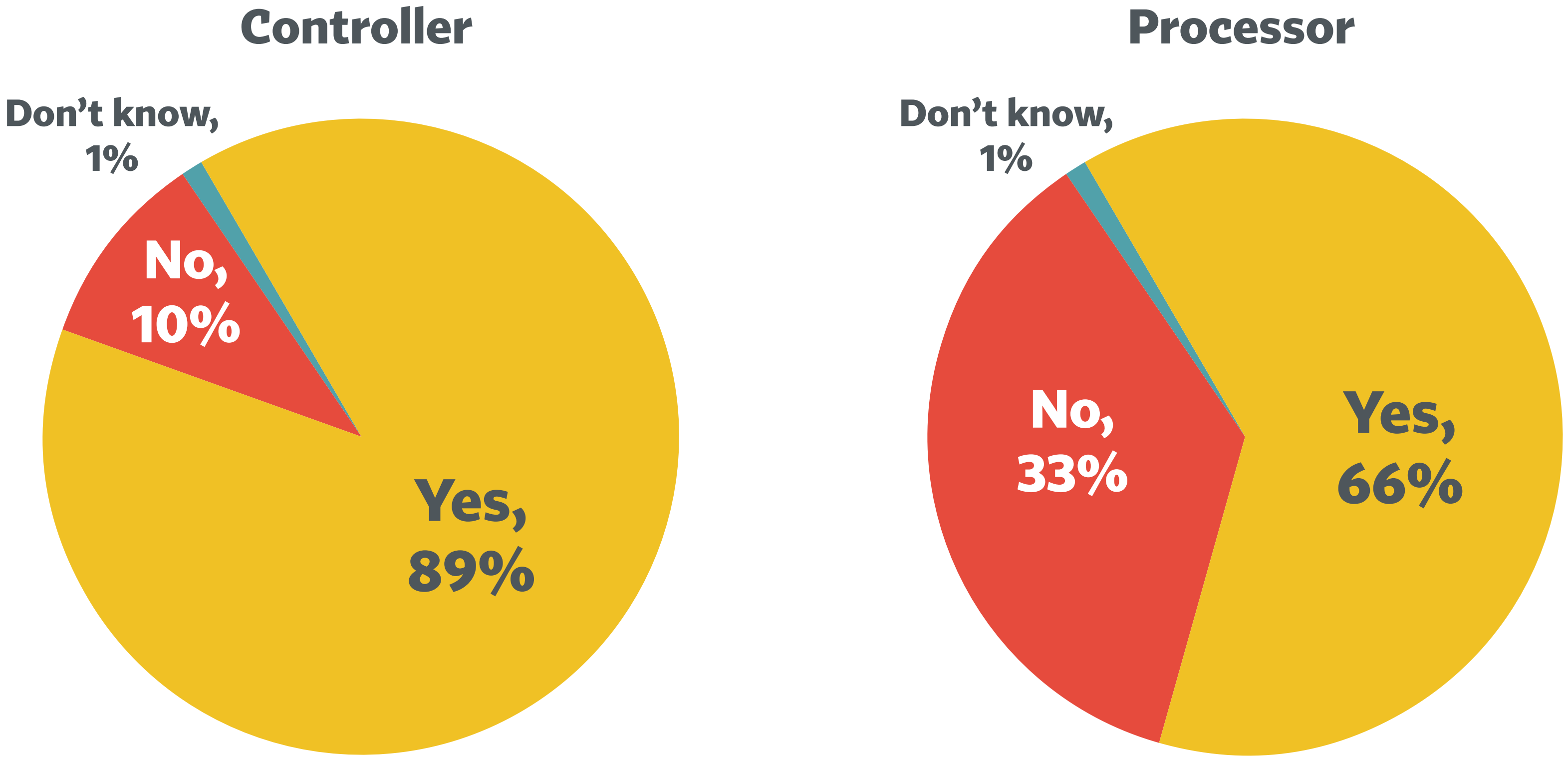
More than one-third of companies subject to GDPR have notified an SA of high-risk processing



J28: Pursuant to GDPR, has your company notified a supervisory authority of a high-risk processing activity?

Almost all companies subject to GDPR wear the “controller” hat, with two-thirds also having “processor” duties

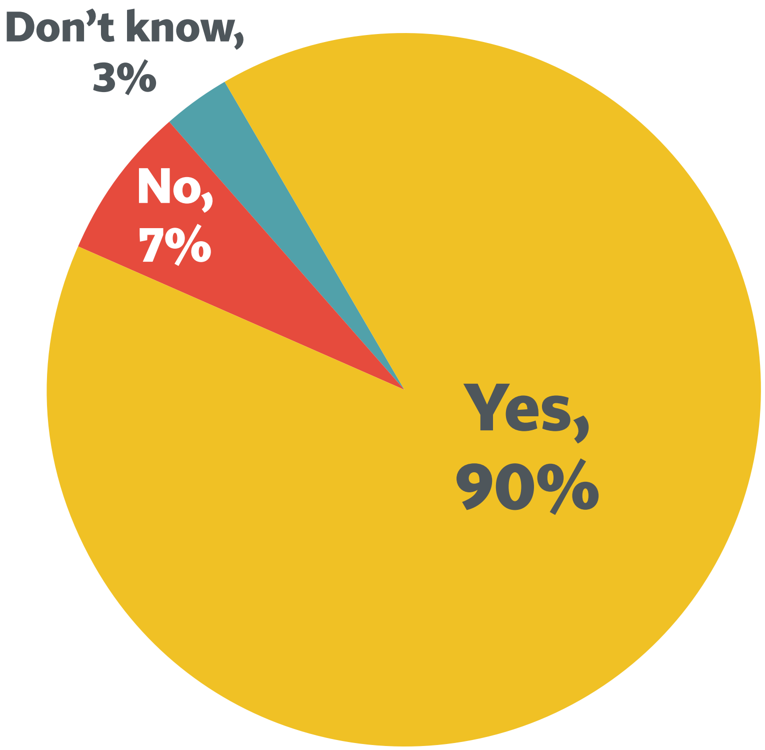
Whether Company is “Controller” or “Processor”
(Among companies saying they must comply with the GDPR)



Z1: Does your company determine the purposes and means of processing personal data (i.e., you are a controller)?
Z2: Does your company process personal data on behalf of other companies (i.e., you are a processor)?

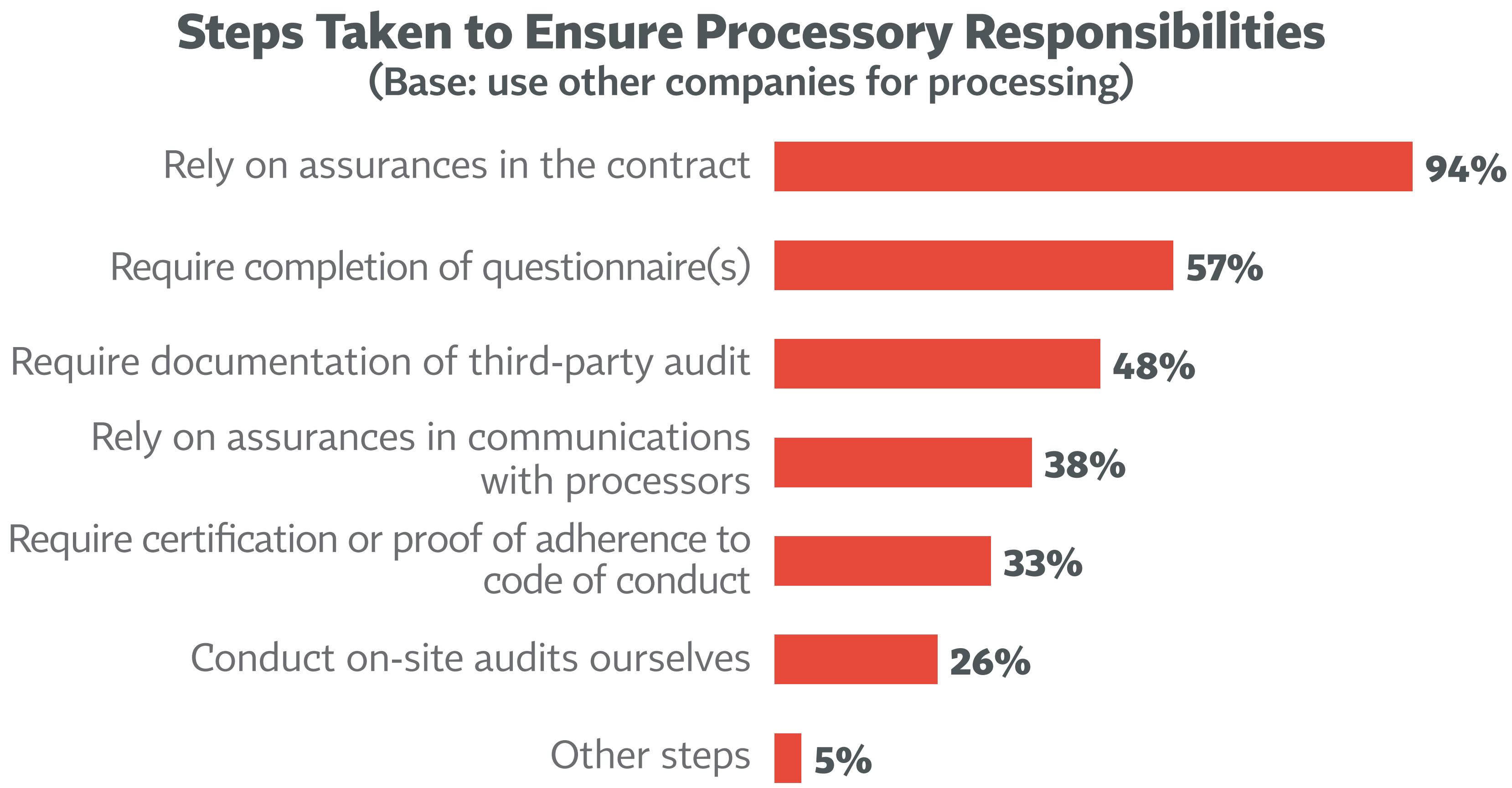
9 out of 10 firms subject to GDPR say they use other companies to process data

Use of Other Companies to Process Data
(Among companies saying they must comply with the GDPR)



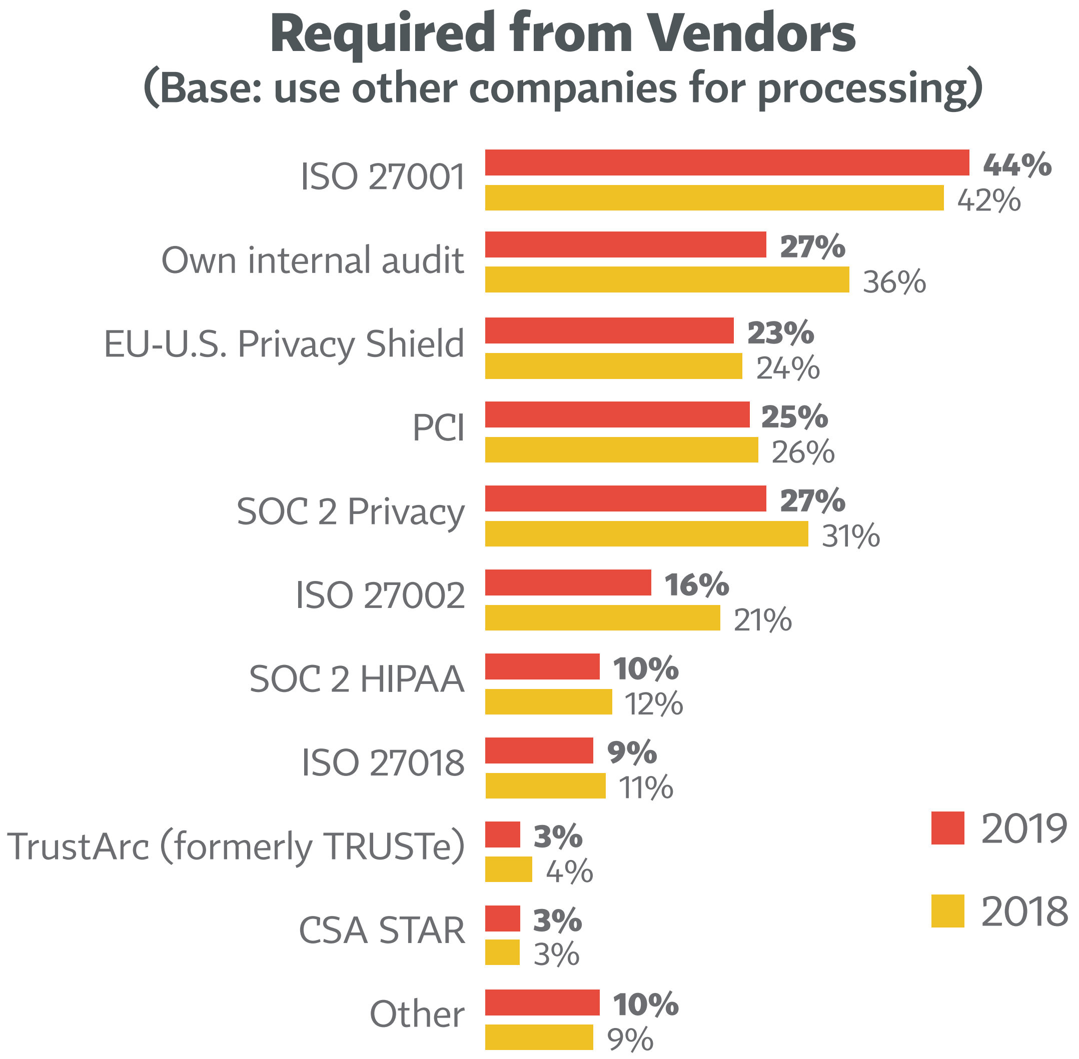
H3: Does your company have other companies process personal data on your behalf (i.e., you use “processors”)?

Contracts are by far most commonly used to ensure processor compliance; questionnaires and audits follow



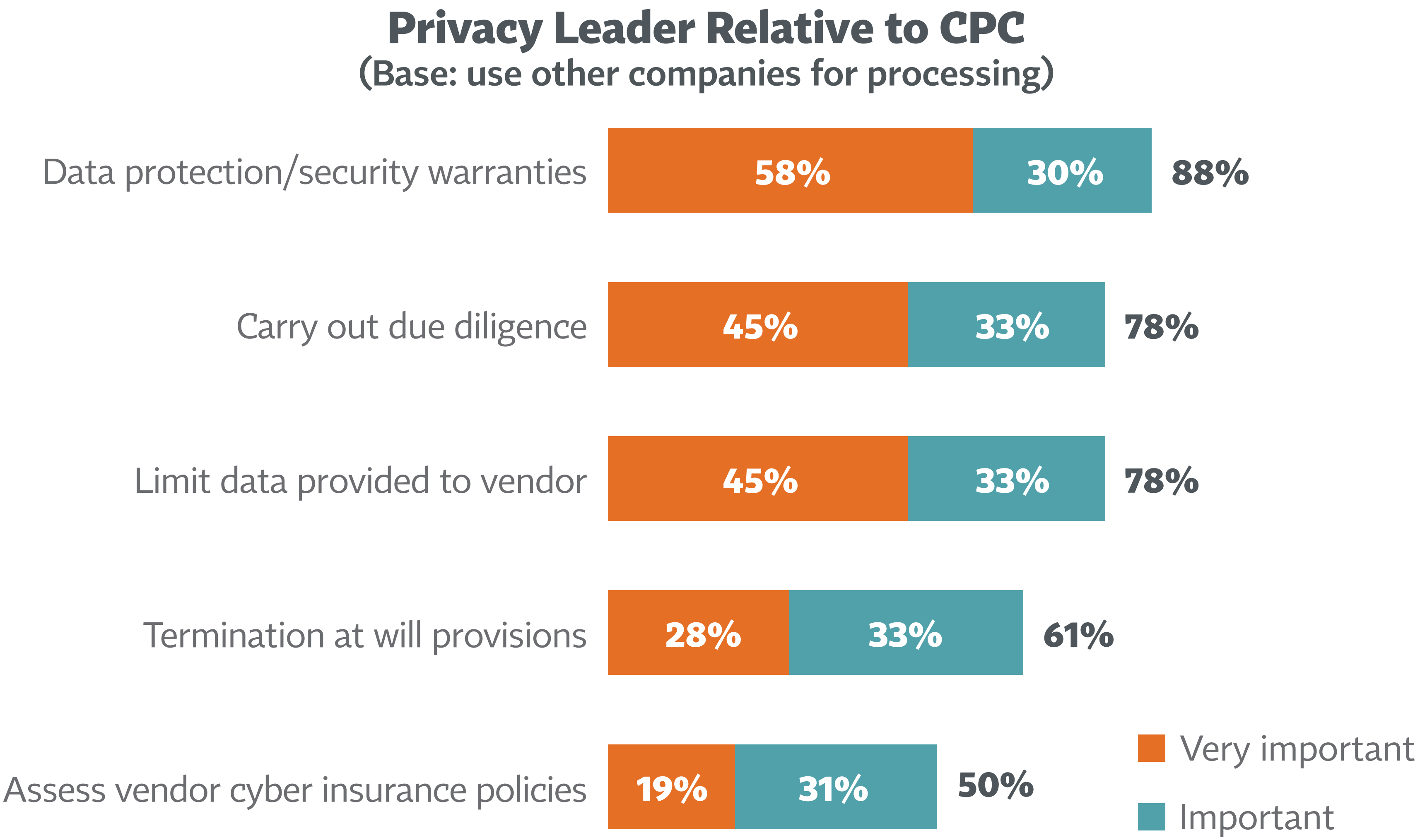
H8: What steps do you take to ensure your processors are doing what they've committed to doing?

ISO 27001 remains the the most common certification required of vendors; internal audits are less popular



K3: Which, if any, third-party audits or certifications does your organization require from vendors?

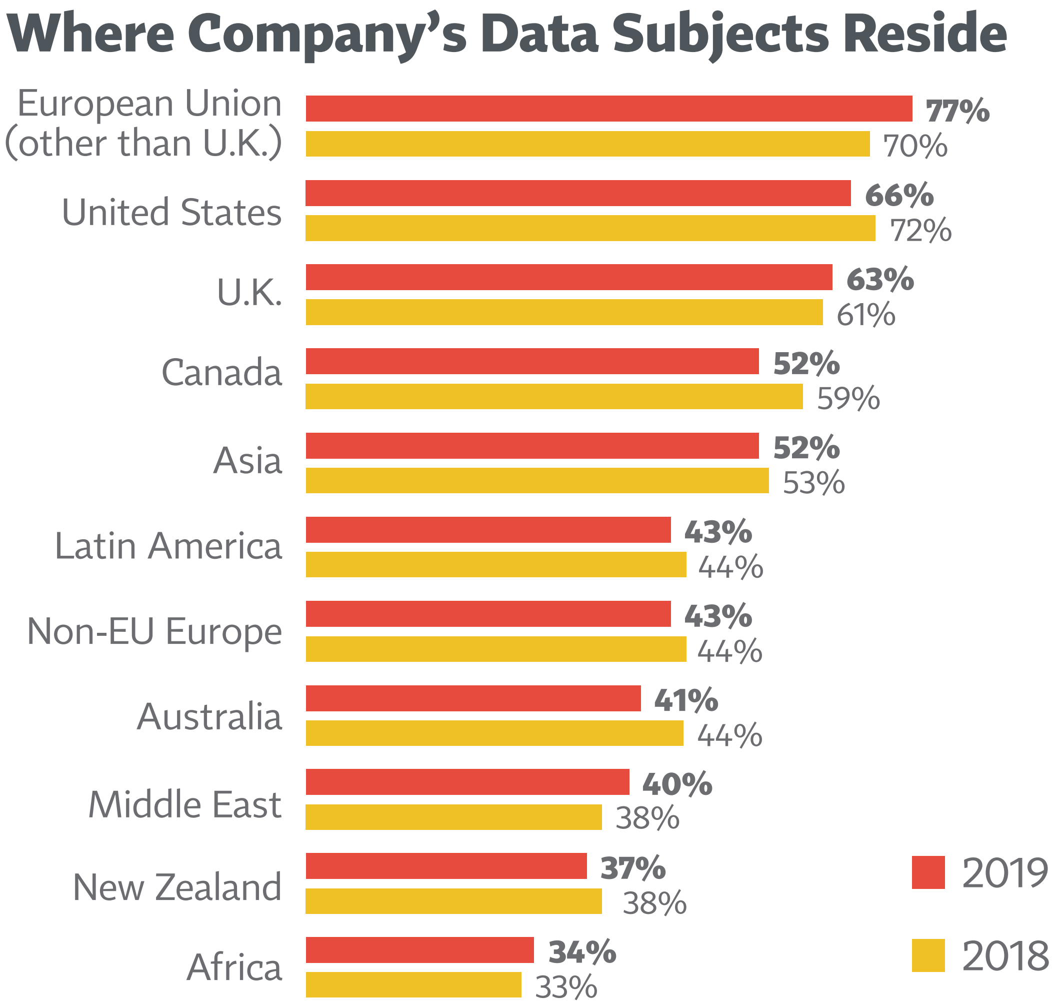
When privacy pros are choosing a processor, contractual warranties are their top consideration



K4-K8: In selecting data processors, how important is it to your company to …

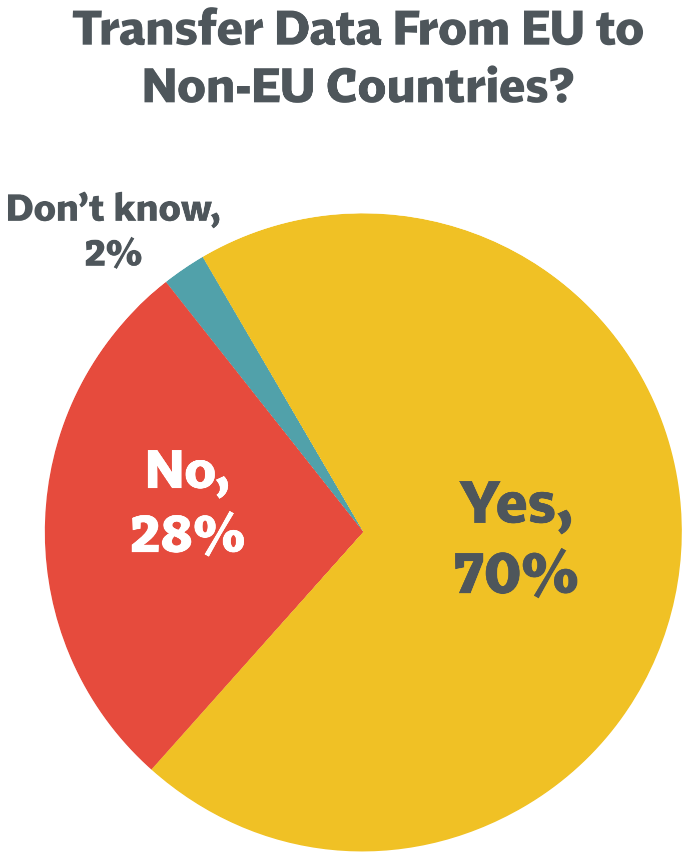
Contents

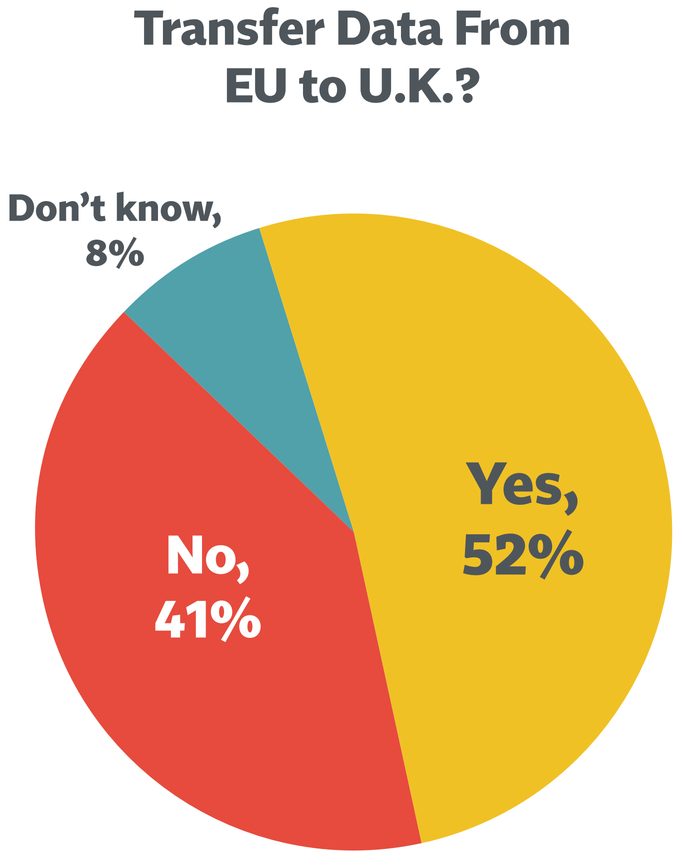
More firms this year reported they are collecting data from subjects in the EU



A6. Do you collect personal data from data subjects in any of the following regions and countries?

7 in 10 firms transfer data outside the EU; half transfer data from the EU to the U.K.





Z3: Does your company transfer personal information from the European Union and/or those countries in the European Economic Area (together: *EU*) to another country outside of the EU?
Z13: Does your company transfer personal information from an EU/EEA country to the U.K.?

Small businesses, B2C firms, and government agencies are the least likely to transfer data from EU

BY COMPANY REVENUE

	Under $100M	$100M-$999M	$1B-$24.9B	$25B+*
Transfer data from EU outside	**61%**	66%	80%	84%

BY INDUSTRY SEGMENT

	Regulated	Unregulated	Government*
Transfer data from EU outside	62%	**78%**	**27%**

BY TARGET

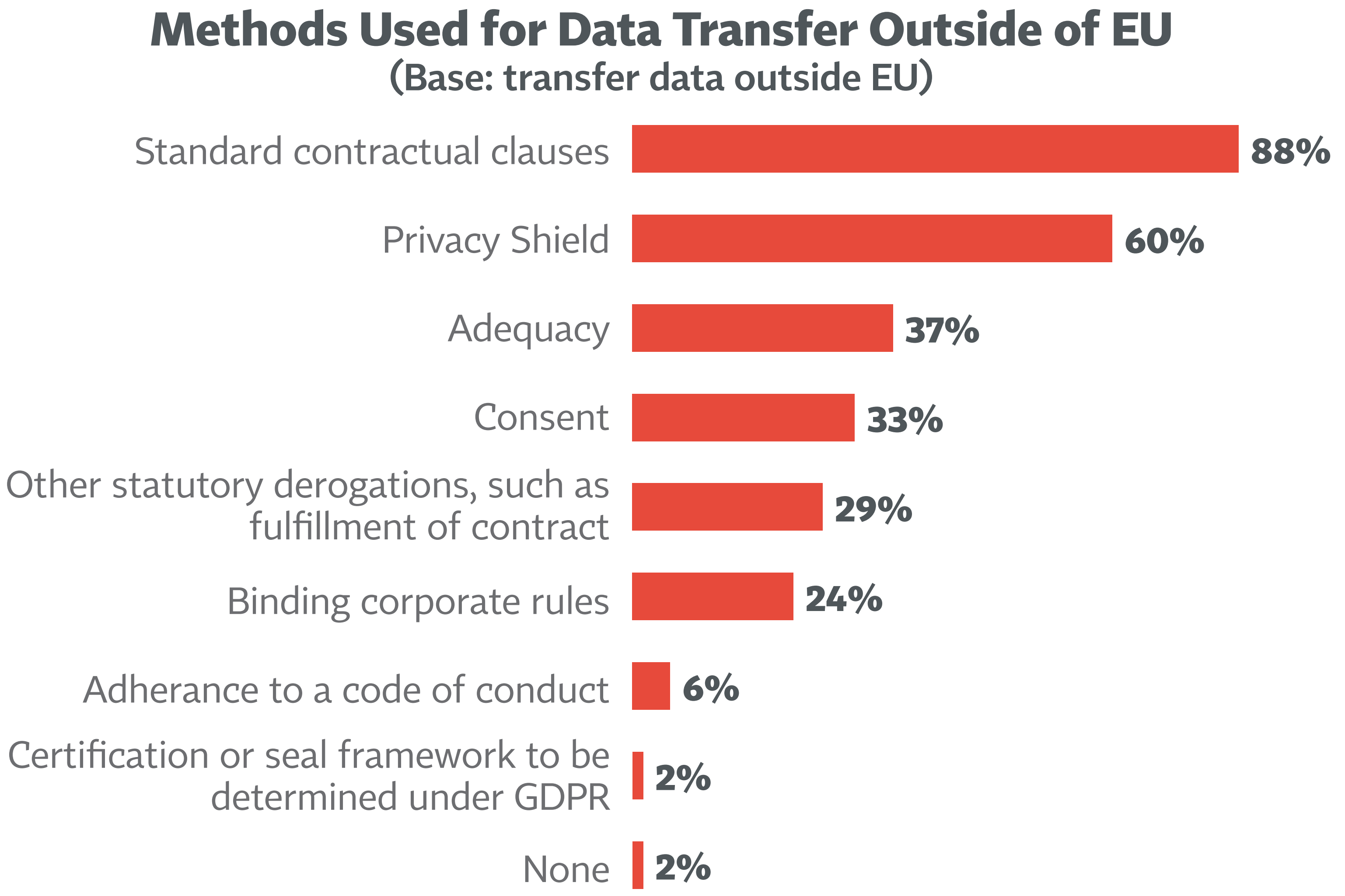
	B2B	B2C	Both
Transfer data from EU outside	78%	**50%**	72%

BY EMPLOYEE SIZE

	<5K	5K-24.9K	25K-74.9K*	75K+*
Transfer data from EU outside	**64%**	68%	88%	86%

🟥 Significantly different than other segments   * Small sample size

SCCs are by far the most common method to transfer data outside the EU; 6 in 10 use Privacy Shield



Z4: What mechanisms does your company currently use to transmit data outside the EU?

EU firms more likely to rely on adequacy for data transfers, U.S. firms more likely to rely on consent

BY RESPONDENT LOCATION

	U.S.	EU
Transfer data from EU outside	66%	79%
Data transfer mechanisms		
SCCs	88%	88%
Privacy Shield	48%	**72%**
Adequacy	**21%**	45%
Consent	**50%**	**21%**
Other statutory derogations, such as fulfillment of contract	41%	22%

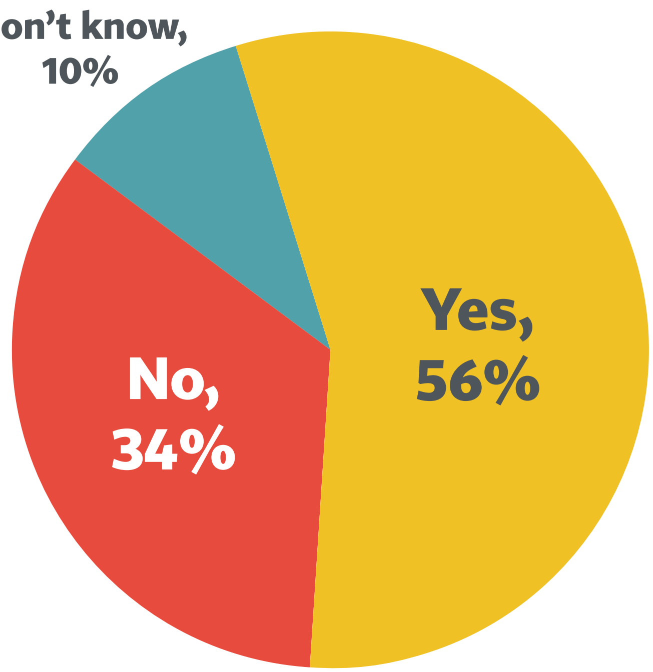
BY HQ LOCATION

	U.S.	EU
Data transfer mechanisms		
SCCs	91%	85%
Privacy Shield	53%	68%
Adequacy	**22%**	45%
Consent	43%	**23%**
Other statutory derogations, such as fulfillment of contract	32%	26%

■ Significantly different than other segments

More than half of all privacy pros say Brexit will have some impact on their organization, especially in EU

Will Brexit Affect Organization?



BY RESPONDENT LOCATION

	U.S.	EU
Brexit will affect organization	47%	68%

BY HQ LOCATION

	U.S.	EU
Brexit will affect organization	51%	64%

BY TARGET

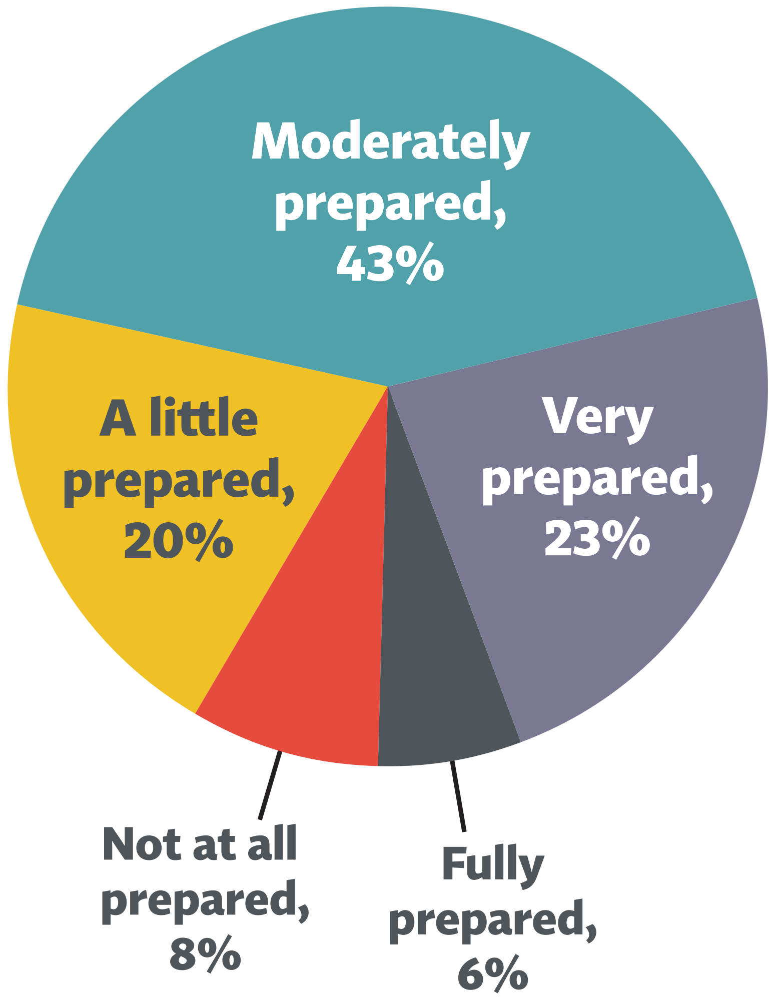
	B2B	B2C	Both
Brexit will affect organization	67%	27%	58%

Z8: Do you think Brexit will affect your organization?

However, among those who say Brexit will have an impact, just 1 in 4 feel "very prepared" for it

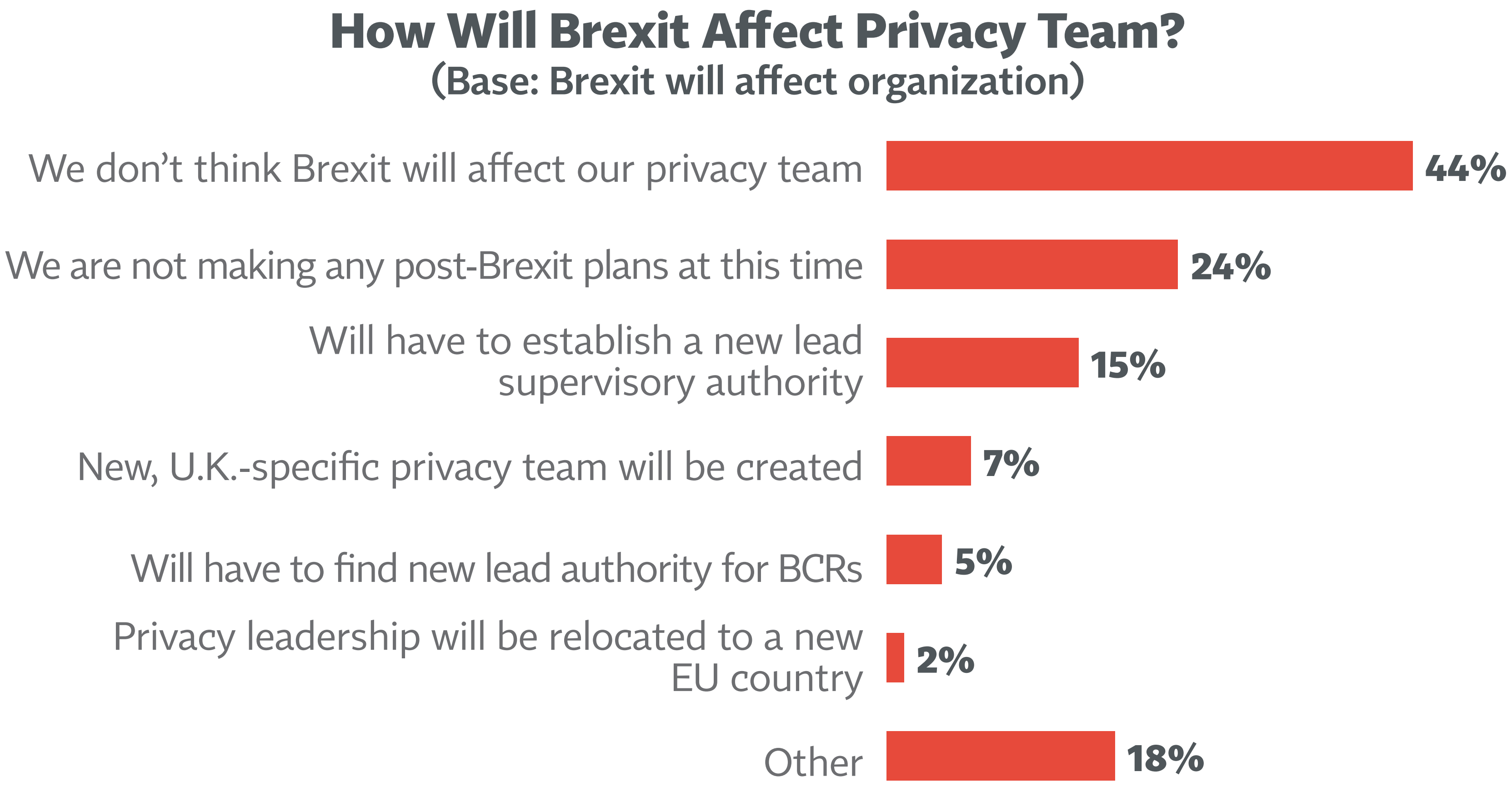
How Prepared Are You for Brexit?

(Base: Brexit will affect organization)



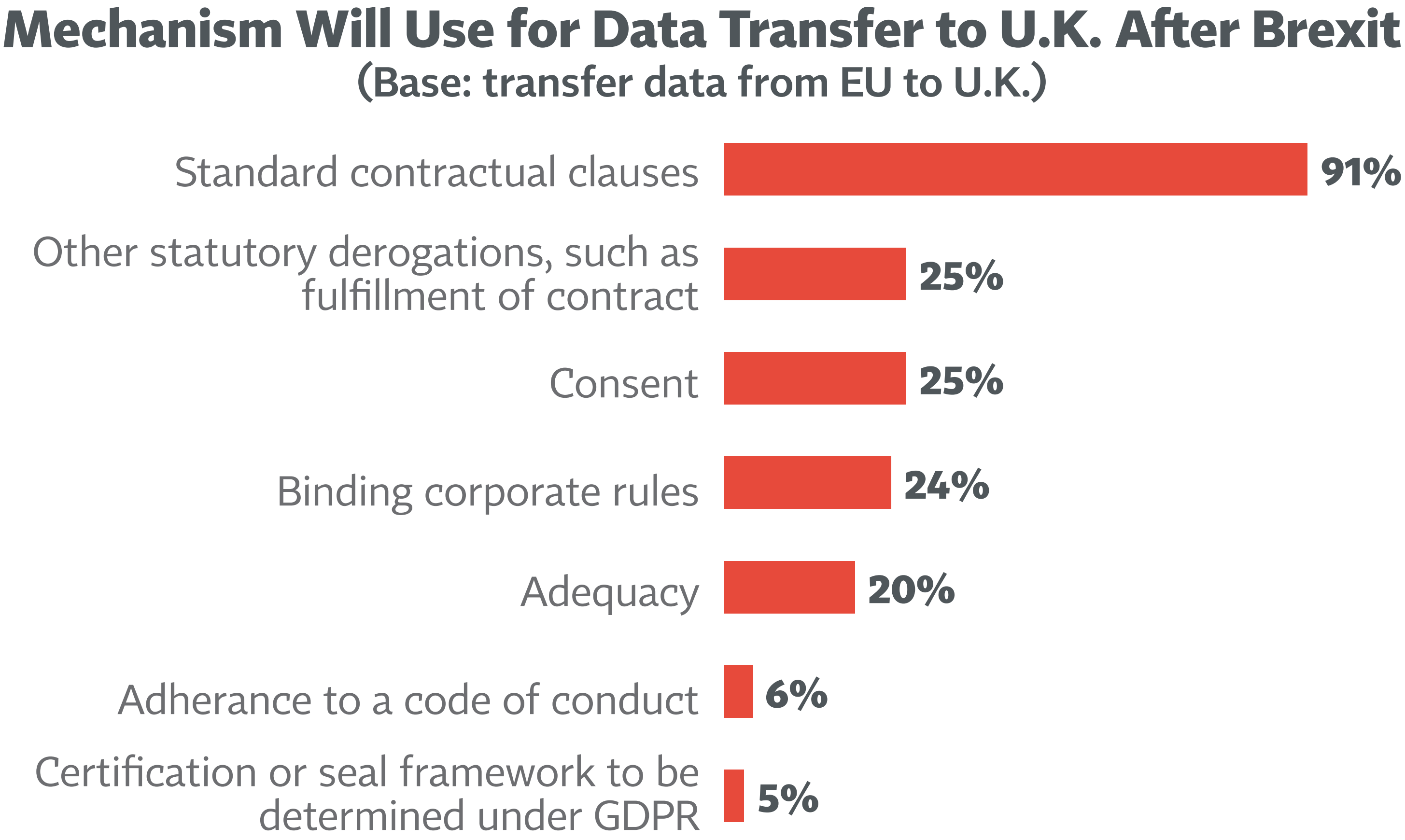
Z9: How would you describe your organization's level of preparedness for the U.K.'s exit from the EU?

While most do not think Brexit will affect privacy team, a few plan to find a new SA or create U.K. privacy team



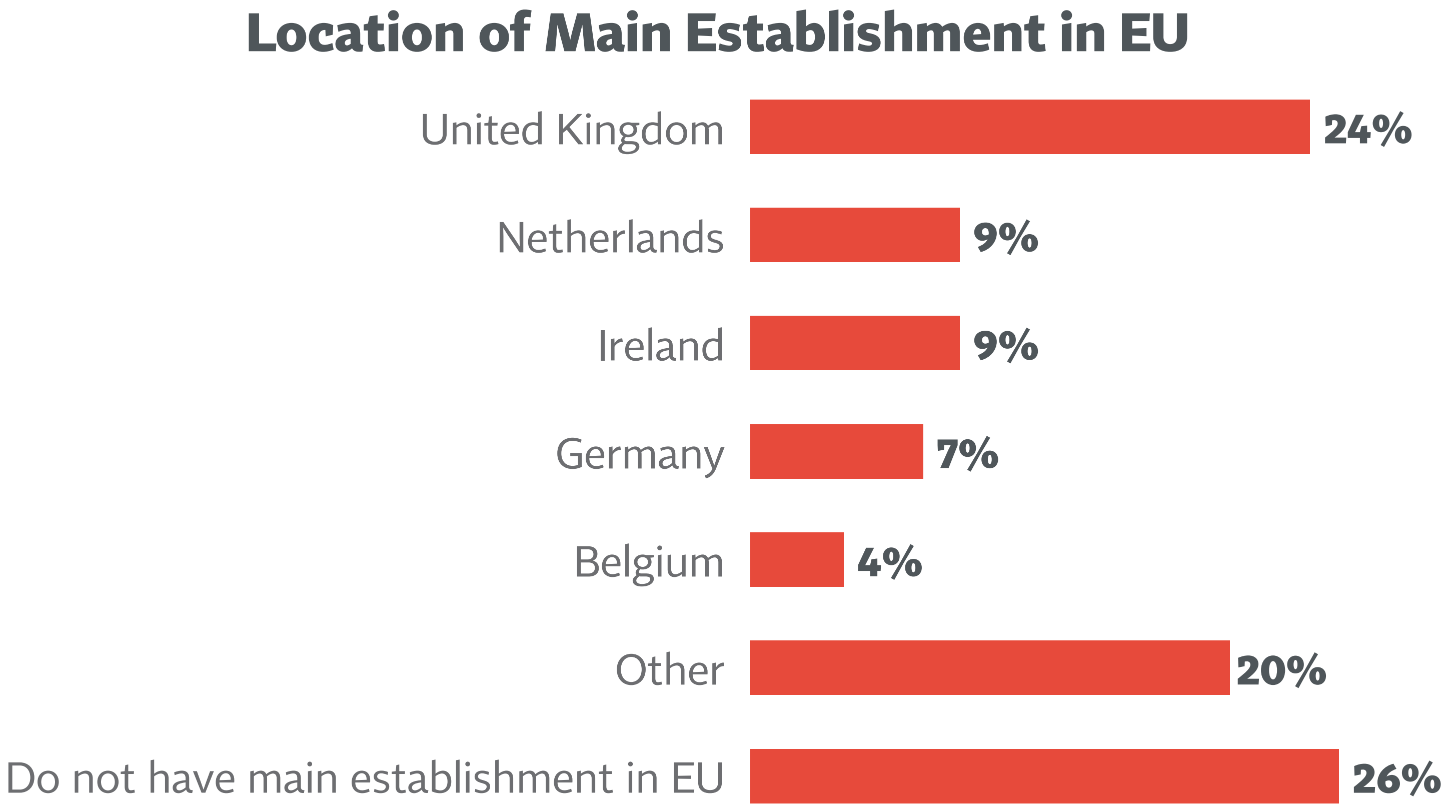
Z10: In what ways might Brexit affect the organization of your privacy team?

Most will use SCCs to transfer to U.K. after Brexit, but consent, BCRs and adequacy will still have roles



Z14: In the aftermath of Brexit, what mechanisms is your company likely to use to transfer data from the EU/EEA to the U.K.?

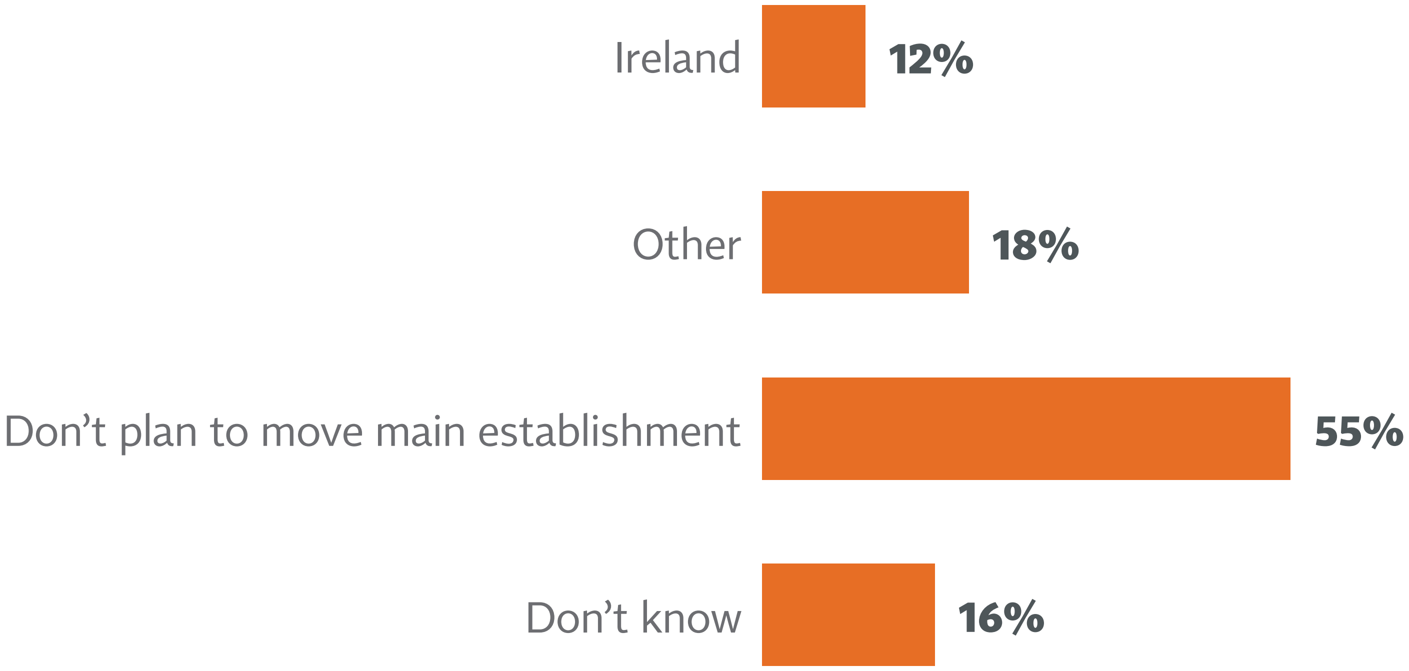
U.K. is most popular choice for main EU establishment; the Netherlands and Ireland come next



Z5: What is the current location of your organization's main establishment in the European Union?

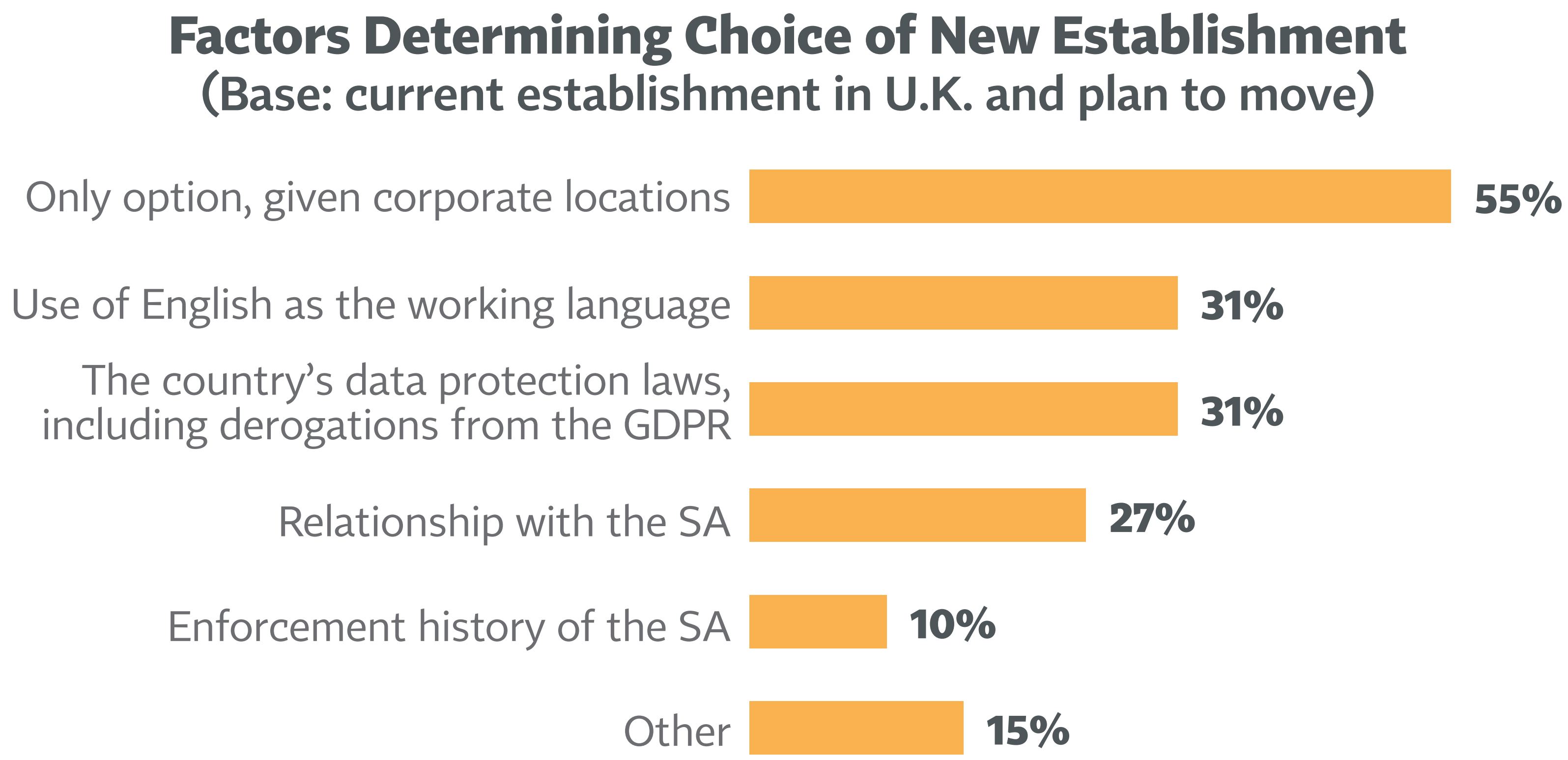
For those with main establishment in the U.K., more than half are not planning to move after Brexit

Location of Main Establishment in EU after Brexit
(Base: have current establishment in U.K.)



Z6: Upon the U.K. leaving the European Union, to where would your company move its main establishment in the EU, if need be?

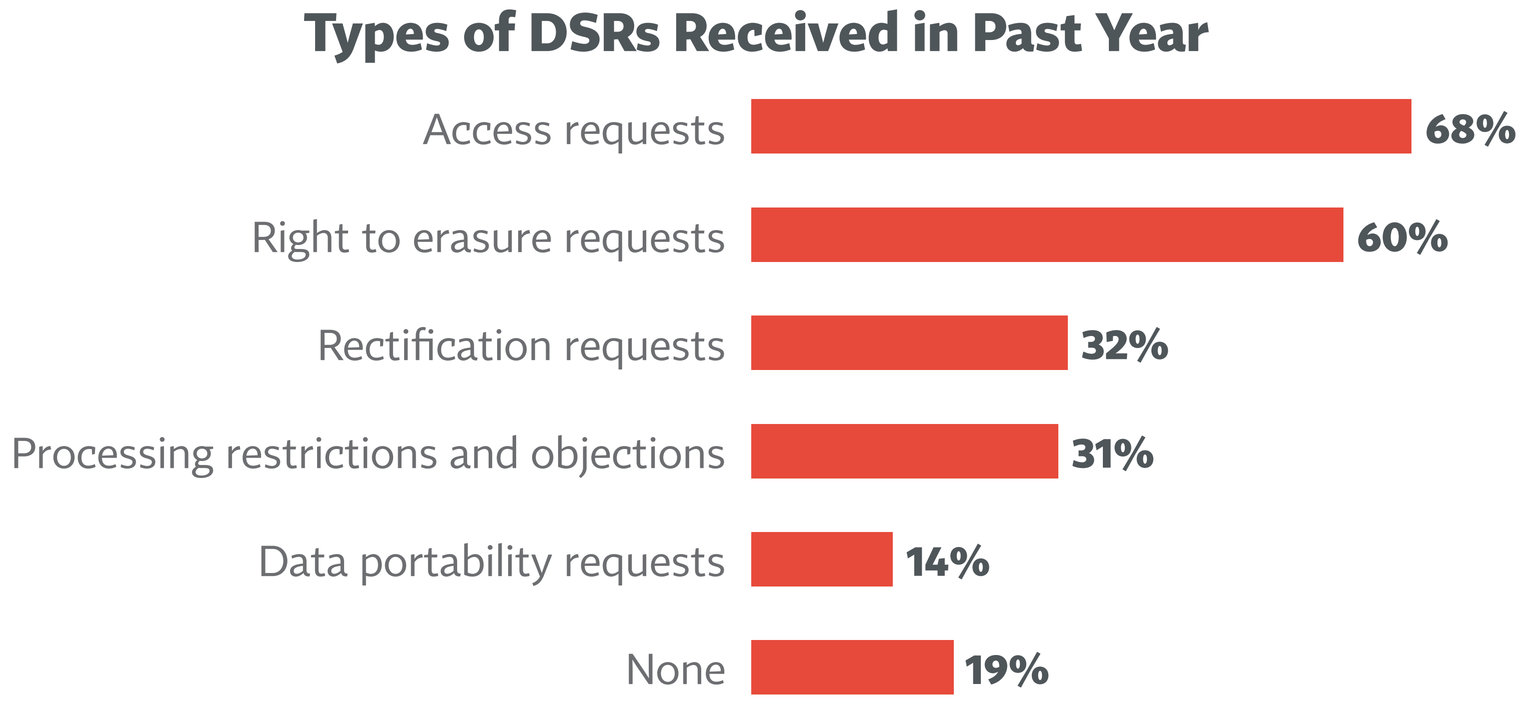
For firms that will move, derogations and relationship with SA will be important factors in their choice



Z7: What factors would go into the decision about which country to relocate your company's main establishment in the EU?

Contents

More than half of firms have received access and right to erasure requests in the past year



R2: Which types of DSRs has your organization received over the past year?

EU-based firms more likely to receive DSRs, while U.S.-based less likely to, compared to others globally

BY HQ LOCATION

	U.S.	EU
DSRs received		
Access requests	**59%**	**76%**
Right to erasure requests	**50%**	**72%**
Rectification requests	**22%**	39%
Processing restrictions and objections	25%	37%

BY TARGET

	B2B	B2C	Both
DSRs received			
Access requests	**59%**	63%	**76%**
Right to erasure requests	52%	51%	**67%**
Rectification requests	23%	27%	**40%**
Processing restrictions and objections	22%	26%	**37%**

🟥 Significantly different than other segments

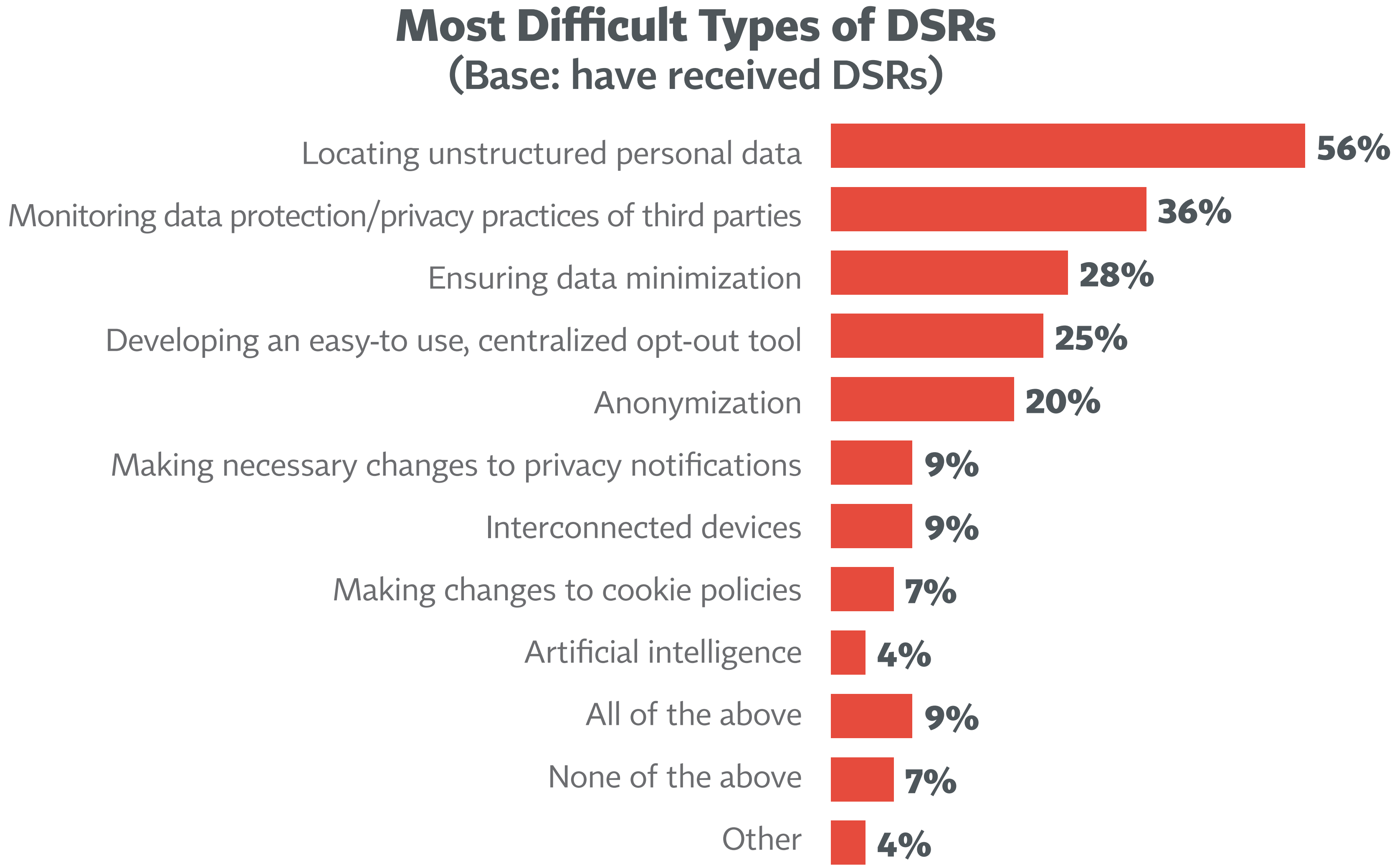
Those who find it difficult to handle access requests tend to fulfill fewer of them

BY “DIFFICULTY” SCORE GIVEN TO FULFILLING SUBJECT ACCESS REQUESTS

	More Difficult Than Average	Less Difficult Than Average
Median # of each types of DSR in past year (includings 0s)		
Access requests	12	25
Right to erasure requests	10	10
Rectification requests	10	5
Processing restrictions and objections	5	5
Data portability requests	1	5

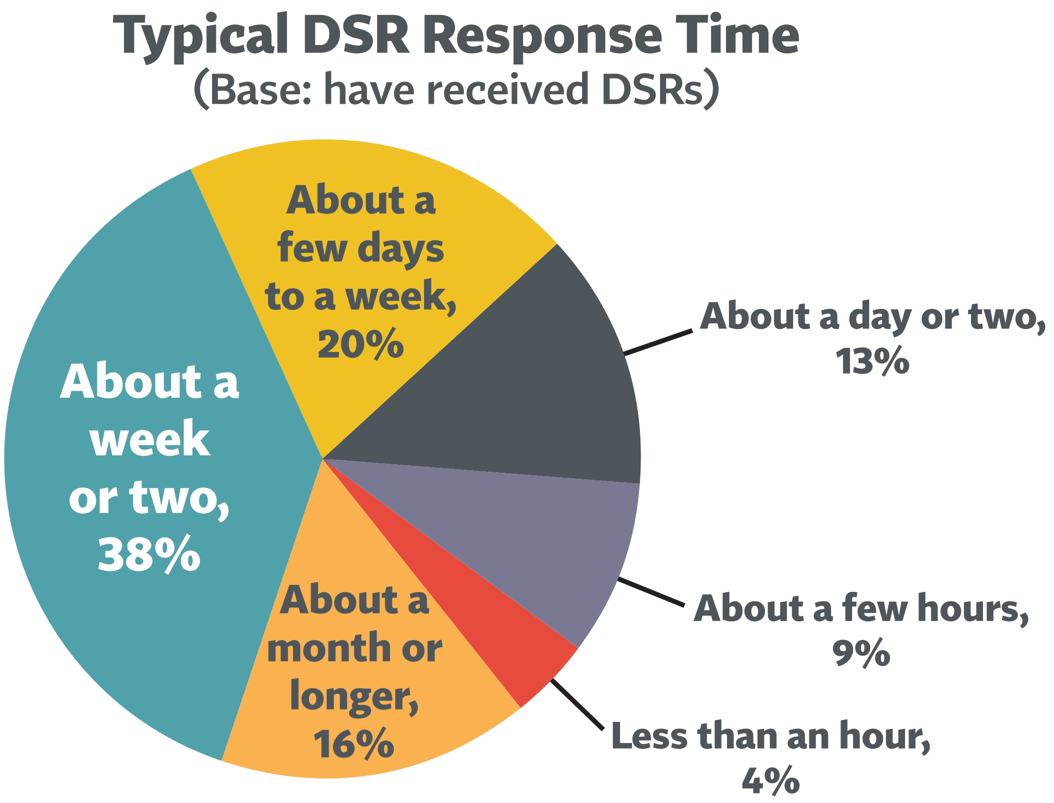
R3: Over the prior year, approximately how many of each of the following DSRs did your organization receive?

By a wide margin, the most difficult type of DSRs involve locating unstructured personal data



R7: Which of the following DSR-related issues are the most difficult to deal with?

About a quarter respond to DSRs within a day or two, but more than half take at least a week



R5: For most DSRs, approximately how long does it take your organization to respond?

Those who see fulfilling requests as difficult generally take longer to respond

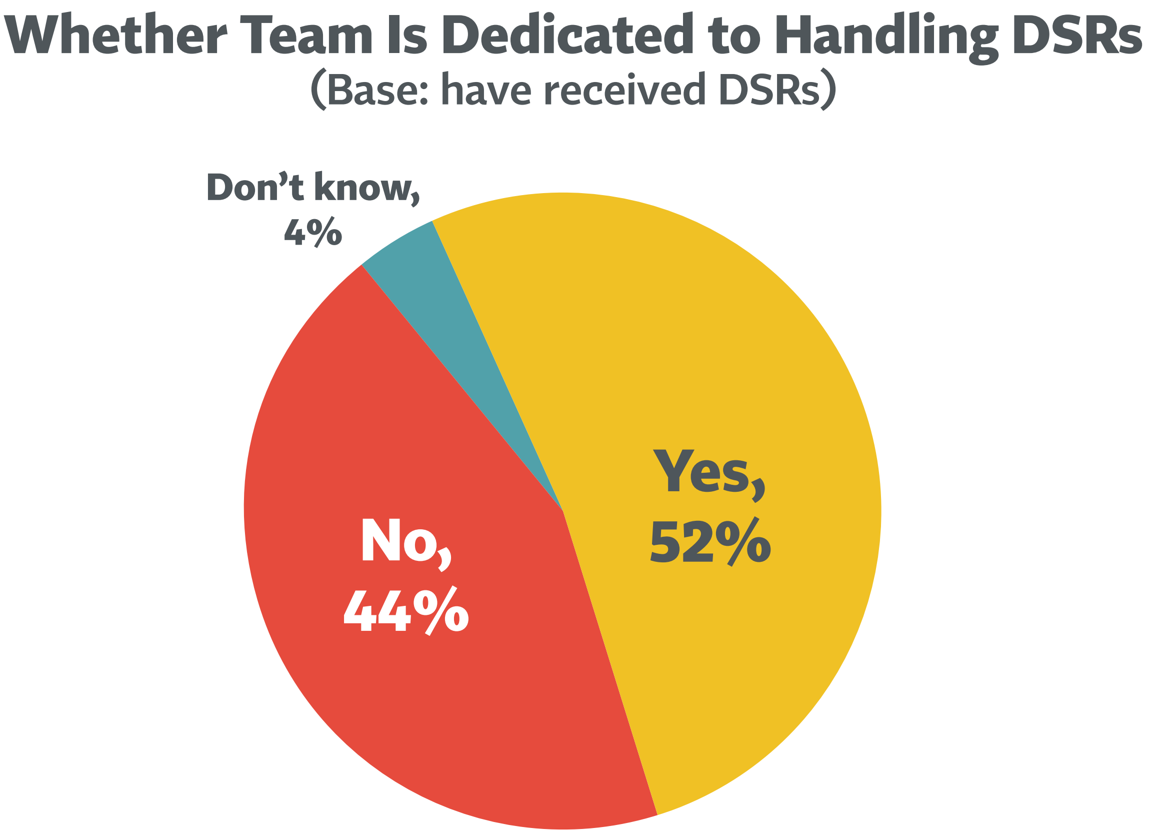
BY "DIFFICULTY" SCORE GIVEN TO FULFILLING SUBJECT ACCESS REQUESTS

	More Difficult Than Average	Less Difficult Than Average
Length of time to respond to DSRs		
Less than an hour	1%	6%
About a few hours	4%	12%
About a day or two	10%	14%
About a few days to a week	15%	24%
About a week or two	45%	36%
About a month or longer	**25%**	8%

🟥 Significantly different than other segments

R5: For most DSRs, approximately how long does it take your organization to respond?

Half of firms receiving DSRs say they have a dedicated team for handling these requests



R6: Is there a team at your company dedicated to handling DSRs?

Those who find requests difficult are less likely to have a team dedicated to fulfilling them

BY "DIFFICULTY" SCORE GIVEN TO FULFILLING SUBJECT ACCESS REQUESTS

	More Difficult Than Average	Less Difficult Than Average
Have team dedicated to DSRs	**40%**	**61%**
Most difficult types of DSRs		
Locating unstructured personal data	58%	60%
Monitoring the practices of third parties	38%	34%
Ensuring data minimization	30%	28%
Developing an easy-to use, centralized opt-out tool	31%	22%
Anonymization	20%	21%
Making necessary changes to privacy notifications	10%	10%
Interconnected devices	12%	9%
Making changes to cookie policies	5%	9%
Artificial intelligence	3%	4%

R6: Is there a team at your company dedicated to handling DSRs?
R7: Which of the following DSR-related issues are the most difficult to deal with?

Those saying access requests are difficult are more likely to use manual and ad hoc processes

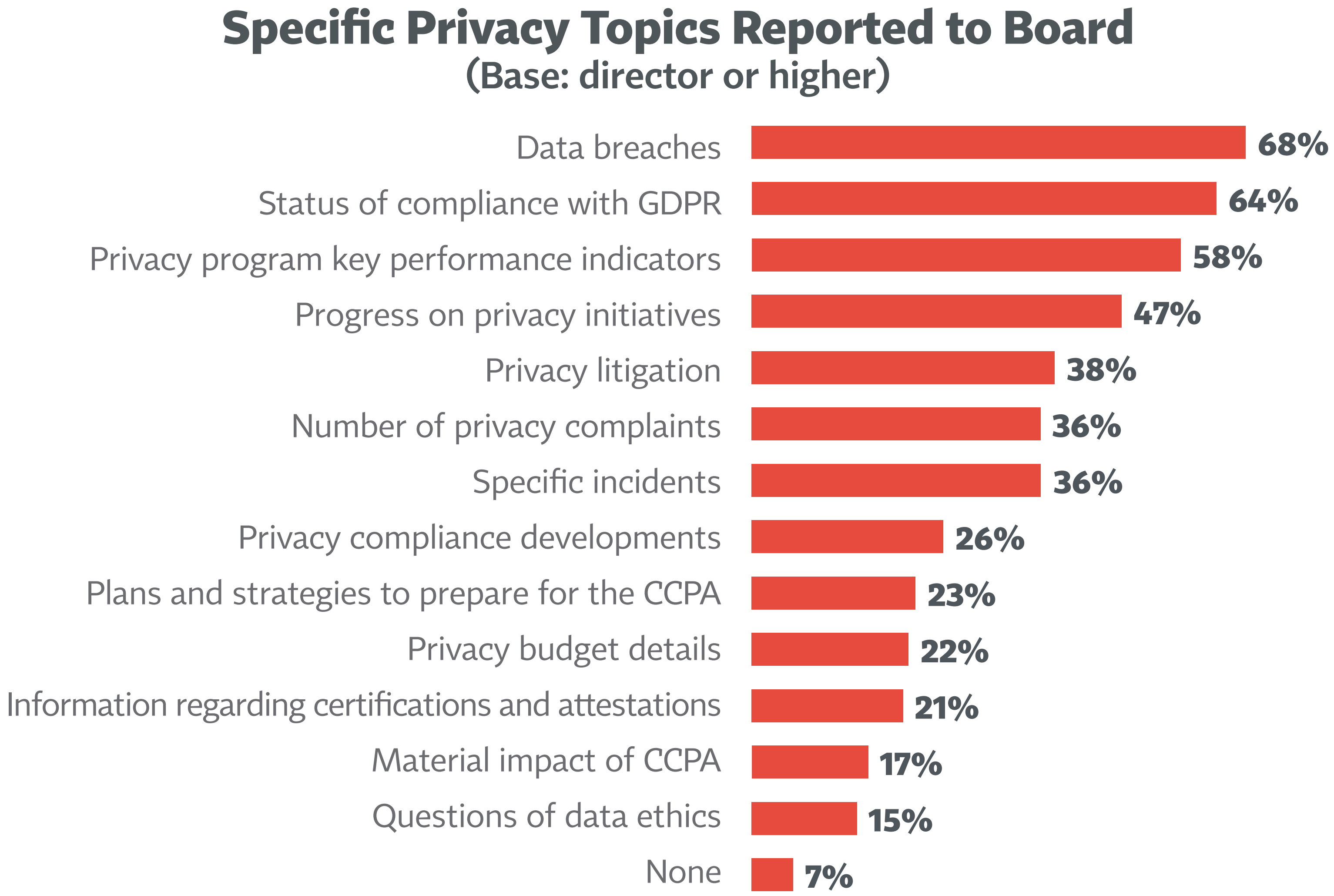
BY "DIFFICULTY" SCORE GIVEN TO FULFILLING SUBJECT ACCESS REQUESTS

	More Difficult Than Average	Less Difficult Than Average
How DSR requests are handled		
The process is automated	0%	2%
The process is partially automated	17%	33%
The process is entirely manual but mature	33%	35%
The process is entirely manual and ad hoc	38%	23%
The process is still being designed	9%	5%
We haven't taken steps to address these requests	3%	1%

J23: How is your company addressing DSRs, such as access, portability, right to be forgotten requests or objections to processing?

Contents

When privacy topics are reported to the board, it’s usually related to data breaches or GDPR compliance

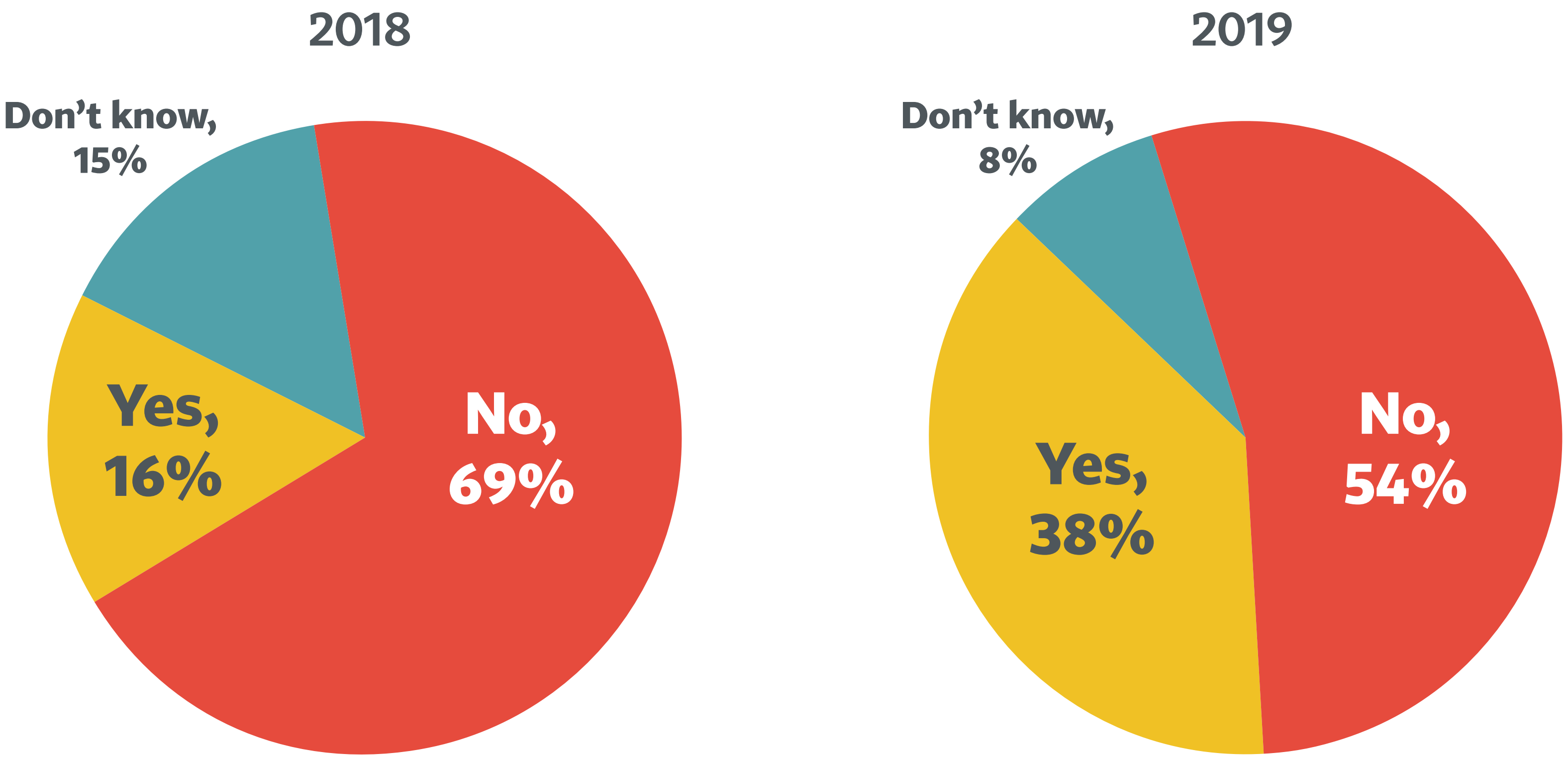


F39: What privacy topics are reported at the board level?

Twice as many firms subject to GDPR have reported a data breach this year compared to last

Notified Authorities of Security Breach?

(Base: must comply with the GDPR)



J28: Pursuant to the GDPR, has your company notified any supervisory authorities of a data security breach?

EU-based firms are more likely than U.S.-based ones to have notified a lead authority of a data breach

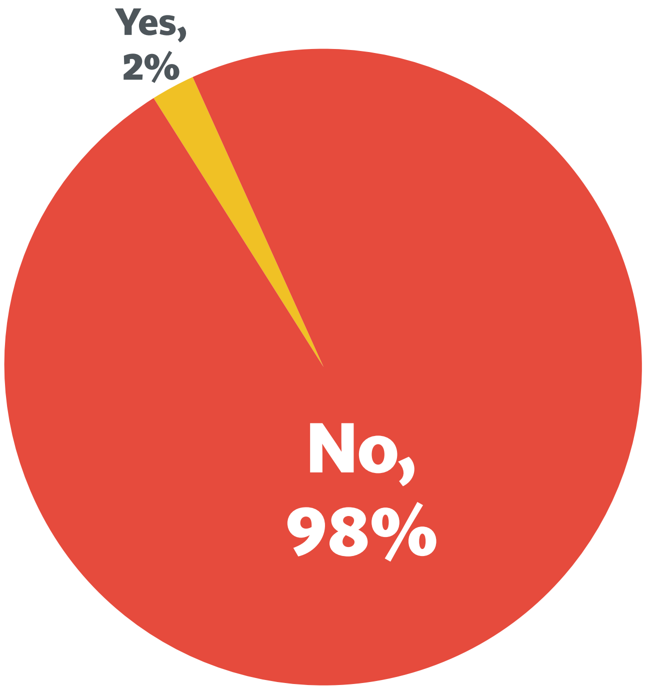
BY HQ LOCATION

	U.S.	EU
Have notified authority of breach	22%	**52%**

■ Significantly different than other segments

Only 2% of firms that have reported a breach to a supervisory authority have been fined

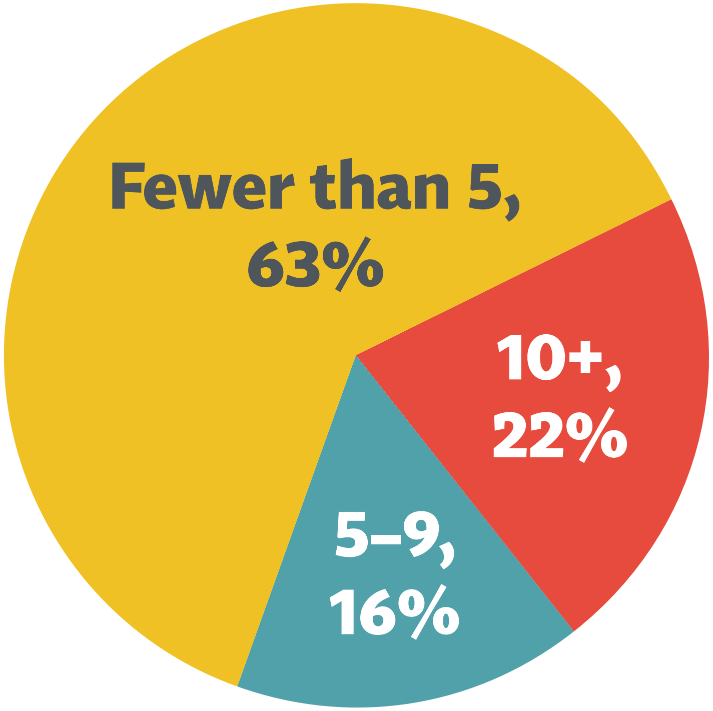
Whether Fines Have Been Imposed For Breaches
(Base: notified SA about breaches)



J30: Has a supervisory authority imposed any fines on your company pursuant to the GDPR for a data security breach?

Most of those reporting a breach say they've reported fewer than 5, although 22% have reported 10 or more

Number of Data Security Breaches
(Base: notified SA about breaches)



MEDIAN NUMBER OF BREACHES (INCLUDING 0)

REGULATED: 4
UNREGULATED: 2
GOVERNMENT: 7

J29: Approximately how many data security breaches has your company notified a supervisory authority about?