November 8, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce

In re: Request for Comments on Developing the Administration's Approach to Consumer Privacy

The International Association of Privacy Professionals (IAPP) respectfully offers its comments to the National Telecommunications and Information Administration (NTIA) Request for Comments on Developing the Administration's Approach to Consumer Privacy. The IAPP submits that in addition to considering privacy policies, rules and regulations, the Administration should recognize professionalization as a major tool for the advancement of improved data governance practices and privacy programs in organizations. Regardless of the Administration's choice between federal privacy legislation, self-regulation or a mix thereof, and the specific privacy policies contemplated under the Administration's approach, it is the appointment, training and resourcing of privacy professionals on the ground that will ultimately ensure corporate accountability and consumer privacy results.

At an age when personal data has become a central raw material for production, underlying new business models and driving research and innovation, managing personal data in organizations has become a full-fledged profession with a body of knowledge that includes legal, technical and management components. The role of Chief Privacy Officers (CPOs) has grown to a senior C-suite office in government agencies and in thousands of businesses, including not only Fortune 500 companies but also SMEs, across all industry sectors. In data intensive industries, such as technology and finance, privacy offices comprise dozens or even hundreds of privacy professionals. In Europe, under the 2016 General Data Protection Regulation (GDPR), public institutions and a large swath of industry are now required to appoint Data Protection Officers (DPOs). More than 20,000 such DPOs have already registered with European data protection agencies since the May 2018 implementation date of the new law.

The past two decades have seen the emergence of a privacy workforce that combines skills, qualifications and responsibilities from the fields of law, public policy, technology and business management. In their book *Privacy on the Ground*, Kenneth Bamberger and Deirdre Mulligan stressed, "the importance of the professionalization of privacy officers as a force for transmission of consumer expectation notions of privacy

Global Headquarters
Pease International Tradeport
75 Rochester Ave.
Portsmouth, NH 03801 USA
Tel: +1 603.427.9200 | 800.266.6501
iapp.org

European Office
Rue du Luxembourg 22
1000 Brussels, Belgium
Tel: +32.(0)2.761.66.86
europe@iapp.org

from diverse external stakeholders, and related 'best practices', between firms."[1] Indeed, Bamberger and Mulligan's thesis was that while Europe had privacy laws on the books, but little implementation or enforcement on the ground, the U.S. has seen the emergence of policies, processes and practitioners who ensured the development and deployment of privacy best practices in organizations.

Accordingly, today, data management should no longer be regarded as a role that employees in legal or HR departments fulfil off the side of their desk. Rather, it is a new profession with standards, best practices and norms, which are widely agreed upon not only nationally but also across geographical borders. Responsible practices for personal data management are not common knowledge. They require training, continuous education, and verifiable methods for identifying and recognizing acceptable norms. Put simply, the digital economy needs privacy professionals. Requiring organizations to implement internal governance programs that deploy such professionals will ensure higher professional standards and more responsible data uses, regardless of the specific rules ultimately chosen for data collection, processing or use.

To acknowledge and address the role of privacy professionals in organizations, the Administration should require businesses that process substantial amounts of consumer data to appoint a dedicated officer to devise, implement, oversee and audit privacy policies on the ground. Such an individual should be duly trained and qualified under an interdisciplinary body of knowledge, including privacy laws and regulations, management processes and technologies, which are utilized by privacy professionals in their day-to-day jobs.

The IAPP conducts an annual survey of its membership to document and benchmark the structure of corporate privacy programs, including their staffing, budgeting, reporting lines, areas of responsibilities, technological tools, and more.[2] As the survey demonstrates, "regulation by professionalization," which has a proven track record not only in privacy but also in fields as diverse as clinical psychology and electrical engineering, is not just an aspirational goal but rather also a reality on the ground.

[1] Kenneth A. Bamberger and Deirdre K. Mulligan, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe (1st edn, 2015).
[2] IAPP-EY Annual Governance Report 2018, https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf (previous annual reports are available online).

Global Headquarters
Pease International Tradeport
75 Rochester Ave.
Portsmouth, NH 03801 USA
Tel: +1 603.427.9200 | 800.266.6501
iapp.org

European Office
Rue du Luxembourg 22
1000 Brussels, Belgium
Tel: +32.(0)2.761.66.86
europe@iapp.org

The accountability principle

The need for development of a privacy profession finds doctrinal support in the concept of accountability, which stems from the 1980 Organization for Economic Cooperation and Development (OECD) Privacy Guidelines,[3] the first international effort to create a unified privacy framework. Under the OECD's accountability principle, "a data controller should be accountable for complying with measures which give effect to the principles stated above."[4] As further explained in the 2013 revisions to the OECD Guidelines, accountability means putting in place a privacy management program that is appropriate to the risks of an operation, provides for internal oversight and governance, includes plans for responding to inquiries and incidents, and is continuously updated and reviewed.[5] In Europe, the GDPR for the first time formally introduced the concept of accountability into EU law, both as an explicit principle and encoded in provisions throughout the Regulation.[6] The GDPR requires controllers to "implement technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation."[7]

In the U.S., even in the absence of formal legislation, accountability measures emerged as a mainstay of companies' efforts to protect brand reputation, respect consumer expectations, and reduce risks associated with the surge in collection and use of personal data. Over the past two decades, the Federal Trade Commission (FTC) has entered into more than 150 settlement orders in enforcement actions against consumer deception and unfairness focused on privacy and data security against companies across a plethora of industry sectors.[8] Although not an explicit feature of the FTC Act, which dates back more than a century, the agency depicted accountability as "embodied in the FTC's framework."[9] Importantly, in dozens of enforcement actions in the field of privacy and data security, the FTC ordered companies to set up elaborate accountability programs for data governance, including external third party audits for periods up to twenty years.

---

[3] Org. for Econ. Co-operation & Dev. [OECD], Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80)(58) Final (1 October 1980).
[4] Id. at art. 14.
[5] Org. for Econ. Co-operation & Dev. [OECD], Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), at art. 15.
[6] Article 5(2): 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')'.
[7] Article 24(1).
[8] Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy (1st edn, 2016).
[9] FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012).

Global Headquarters
Pease International Tradeport
75 Rochester Ave.
Portsmouth, NH 03801 USA
Tel: +1 603.427.9200 | 800.266.6501
iapp.org

European Office
Rue du Luxembourg 22
1000 Brussels, Belgium
Tel: +32.(0)2.761.66.86
europe@iapp.org

In 2012, the Administration's proposed Consumer Privacy Bill of Rights included explicit accountability measures,[10] as did amendments to the Health Insurance Portability and Accountability Act (HIPAA) in 2013, including mandatory investigations of possible violations and penalties even for inadvertent violations in the health sector.[11]

A profession emerges

In order to bind organizations to their privacy commitments—which include deployment of complex measures of data inventory, data mapping, consent management, de-identification, encryption and security—policymakers should require them to demonstrate accountability by hiring and deploying duly qualified privacy professionals. The promises and commitments in FTC consent decrees would be hollow without a privacy profession to implement them into the day to day activities of companies.

The concept of an internal privacy officer has risen to prominence as a cornerstone of the U.S. approach to privacy protection in the past two decades. In the late 1990s, with the growth of information technology, an emphasis on enhancing trust in the nascent digital economy forced companies to devote internal resources toward protecting consumer expectations. Companies that failed to satisfactorily address the public's privacy concerns—such as Eli Lilly, which mistakenly revealed the email addresses of hundreds of Prozac patients,[12] or DoubleClick, which proposed to combine clickstream data with offline personally identifying information[13]—met public scorn. The role of the CPO appeared in response, with companies creating internal positions for privacy specialists. In the decade that followed, a new profession arose focused on managing privacy risks and creating accountable data governance practices.

The privacy profession is thus built upon the bedrock principle of accountability – that the success of privacy protection depends not on the vindication of formulaic notice and consent but rather on securing the trust of those whose information is at stake through responsible data practices.[14]

---

[10] The White House, Consumer Data in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (February 2012).
[11] 45 CFR Parts 160 and 164, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act".
[12] FTC Press Release, Eli Lilly Settles FTC Charges Concerning Security Breach (January 18, 2002).
[13] Andrea Petersen, DoubleClick Reverses Course After Outcry on Privacy Issue, Wall Street Journal (3 March 2000).
[14] Andrew Clearwater and J. Trevor Hughes, In the Beginning . . . An Early History of the Privacy Profession, 74 Ohio St. L.J. 897 (2013).

Global Headquarters
Pease International Tradeport
75 Rochester Ave.
Portsmouth, NH 03801 USA
Tel: +1 603.427.9200 | 800.266.6501
iapp.org

European Office
Rue du Luxembourg 22
1000 Brussels, Belgium
Tel: +32.(0)2.761.66.86
europe@iapp.org

A professional association

The IAPP, born in 2000 to serve the small, but budding privacy profession, grew to 10,000 members in 2012 and more than 45,000 in 2018. A not for profit, non-policy professional association, the IAPP has worked to define, support and improve the privacy profession globally. The IAPP has developed and offered the only globally recognized, ISO/ANSI accredited, credentialing programs in information privacy: the Certified Information Privacy Professional (CIPP), the Certified Information Privacy Manager (CIPM) and the Certified Information Privacy Technologist (CIPT). The CIPP, CIPM and CIPT have been awarded to more than 21,000 professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice. The annual Global Privacy Summit now draws more than 5,000 participants; the Europe Data Protection Congress is the largest privacy conference in Europe with more than 2,000 attendees. With more than 120 local KnowledgeNet chapters in 50 countries, the IAPP provides daily networking and continuing education opportunities for thousands of privacy professionals across the globe.

Together with leading graduate programs in law, computer science and business, in the U.S. and abroad, the IAPP established the Privacy Pathways program, intended to serve as an on-ramp to the profession for students who take a group of courses in privacy, complete an externship or an internship and pass a certification exam. The IAPP's sections, the Privacy Law Bar and the Privacy Engineering Forum, convene professionals from these respective disciplines to advance knowledge and share best practices. Last year, the American Bar Association (ABA) accredited the IAPP to certify lawyers in the specialty area of Privacy Law. This means that U.S. attorneys who meet the IAPP's specialist designation requirements are permitted under the professional responsibility rules of more than 25 states to advertise their specialization in privacy law. To obtain the designation, an attorney must be admitted in good standing in at least one U.S. state; hold a CIPP/US as well as either a CIPM or CIPT designation; pass a special Ethics Exam administered by the IAPP (or submit a recent MPRE score of 80+); provide proof of "ongoing and substantial" involvement practicing privacy law; supply evidence of continuing education in privacy law; and provide at least five peer references from attorneys, clients or judges.

Global Headquarters
Pease International Tradeport
75 Rochester Ave.
Portsmouth, NH 03801 USA
Tel: +1 603.427.9200 | 800.266.6501
iapp.org

European Office
Rue du Luxembourg 22
1000 Brussels, Belgium
Tel: +32.(0)2.761.66.86
europe@iapp.org

Conclusion

To ensure that privacy policies do not remain on the books but are also implemented on the ground, the IAPP is working to define, support and improve the privacy profession globally. The Administration can support this mission by recognizing the contribution of privacy professionals and the importance of privacy qualifications, training, education and best practices, as integral parts of an ecosystem that promotes technological innovation while maintaining responsible data practices.

Respectfully Yours,

Omer Tene
Vice President, Chief Knowledge Officer

Global Headquarters
Pease International Tradeport
75 Rochester Ave.
Portsmouth, NH 03801 USA
Tel: +1 603.427.9200 | 800.266.6501
iapp.org

European Office
Rue du Luxembourg 22
1000 Brussels, Belgium
Tel: +32.(0)2.761.66.86
europe@iapp.org

IAPP-EY Annual Privacy Governance Report 2018

iapp

EY
Building a better working world

Introduction

May 25, 2018, came and went and the world did not end. While many a privacy professional may have been a bit absent on the homefront in the lead-up to the EU General Data Protection Regulation go-live date, working long hours to tighten up compliance programs and work with just about every team in the organization, we knew all along that the work was just beginning.

Indeed, while outside observers might find fault with the 56 percent of respondents to this year's Privacy Governance survey who say their organizations are not yet compliant with the GDPR, those of us in the job of privacy know just how tall a task GDPR compliance is for large organizations with reams of legacy data sets in everything from file cabinets to thumb drives to cloud services.

Is it impossible? Well, 19 percent of you say you'll never be fully compliant with the GDPR. That's either an acknowledgement of the fast pace at which technology moves or a cry of frustration. We'll let you be the judge.

However, the world of privacy moves as quickly as technology, and those of you who thought the privacy world would get a reprieve this summer had a rude awakening. Right on the heels of the GDPR came the California Consumer Privacy Act of 2018. Then a draft data protection bill out of India. Then a new GDPR-like privacy law passed in Brazil.

For those of you keeping track, that's four of the world's 10 largest economies with new data protection laws, right there. And now we hear the drums beating for a new federal privacy law in the United States that might stem the tide of new privacy bills we're seeing come from the likes of Vermont, Colorado, and Ohio, as they play catch up with California.

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.

As privacy compliance – or going beyond compliance – gets more complex, benchmarking your efforts against other similar programs gets more important. Are other organizations appointing data protection officers even if they're not legally mandated? Yes, they are. Nearly half of all those who have appointed a DPO say they did it because the role is valuable to the organization, not only because it was legally mandated.

Quite simply, privacy is no longer an issue solely for the legal and compliance departments to handle in their spare time. For 78 percent of our respondents, privacy is a board-level issue, in fact. And the board's concern is focused on long-term privacy compliance, not simply the latest data breach – though they still want to hear about breaches, to be sure.

When you spend an average of $3 million per organization getting to GDPR compliance, that's going to get boards paying attention, after all. As we move beyond the EU, and begin the work of complying with CaCPA and LGPD (that's Brazil; get to know those letters), the focus now will be on how much of the work put in for the GDPR translates to other jurisdictions.

Is it truly possible to create a globally flexible privacy program, ready to take on challenges and create trust around the world? It's time to find out.

Contents

Executive Summary

Survey findings: GDPR triggers privacy hiring, $3M in average spend; 1 in 5 say they'll never be compliant

Last year, the 2017 Privacy Governance Report welcomed the arrival of the European Union's General Data Protection Regulation, both the compliance efforts and the corresponding angst over how to accomplish a list of daunting, if not impossible, tasks. One year later, we see in the 2018 survey that organizations have bulked up their privacy teams, tackled the hard work of implementing GDPR programs, spent a lot of money to get there (an average of $1.3 million, with an additional $1.8 million expected), and learned many lessons along the way.

Indeed, there is still a long way to go: Fewer than 50 percent of survey respondents report they are "fully compliant" with the GDPR, and nearly one in five admit that full GDPR compliance is truly impossible. But there is good news: The GDPR looks a lot less complicated and confusing in practice than it initially did on paper. While privacy professionals are still struggling with certain tasks, difficulty scores have dropped considerably for every individual compliance process.

Like last year, of course, with the GDPR dominating the privacy narrative, we see considerable growth in the number of privacy professionals working for European organizations and responding to the survey. Membership in the IAPP has eclipsed 44,000 members — 14,000 more (47 percent growth) than last year at this time. Nearly 13,000 of the membership are domiciled in Europe. Commensurately, in this year's survey, 37 percent of respondents are from the European Union (including, for now, the United Kingdom), up from 22 percent in 2017 and 19 percent in 2016.

Those who have been following the governance report since its first year in 2015 will see shifts in the data corresponding to this shift in respondent demographics.

Further, the GDPR launches into the regulated arena many firms that were previously not regulated for data protection and privacy issues. It is, as privacy professionals now know, just the tip of a growing iceberg of global privacy regulations. Accordingly, we are seeing significant growth in the number of full time staff dedicated to privacy, with the global mean now at 10 full-time privacy staff.

One key finding is that privacy is increasingly a stand-alone issue of corporate significance, not tied as integrally to data breach as in previous years. Here are some other key results:

- 76 percent of all respondents believe their firm falls under the scope of the GDPR.
- Acquiring and maintaining business relationships is a key driver of GDPR compliance; B2B-focused businesses are far more likely than B2C and even than blended firms to have full-time privacy professionals working in their privacy programs.

- 25 percent of respondents have changed vendors in response to GDPR and 30 percent say they are considering future vendor changes.

- The most popular cross-border data transfer mechanism — by far — is Standard Contractual Clauses.

- More than half the respondents subject to GDPR (56 percent) say they are far from compliance or will never comply.

One of other important stories coming out of this year's report is a portrait of the role of the data protection officer. This position has exploded on to the scene, with 75 percent of respondent firms reporting they have appointed a DPO. Among those that haven't, most believe the GDPR simply doesn't apply to them.

Firms are split almost evenly as to their motivations for having a DPO. Slightly over half are just following the law, but 48 percent have created the position to serve a valuable business function. Almost six in 10 privacy leaders, those who oversee privacy decision-making at their organizations, have taken the DPO duties on themselves, and, where they haven't, the DPO more likely than not (65 percent of the time) reports to the privacy lead.

Given the above, it is perhaps not surprising that privacy professionals are enjoying more influence earlier and more often in the development and maintenance of products and services, as privacy by design takes hold as an organizational philosophy. They are developing and deploying firm-wide privacy training as a top priority and seeing their issues front and center with the Board of Directors.

In short, along with the GDPR, data protection officers have arrived.

GDPR IN PRACTICE:

Forty-four percent of organizations elevated the position of the privacy leader within the organization in response to the GDPR.

Contents

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 550 completed surveys, fully anonymous

The survey asked for a variety of detailed information on privacy budgets, staffing, department structures and priorities. Further, it explored how organizations are complying with the European Union's General Data Protection Regulation, as well as a variety of common privacy program tasks, such as cross-border data transfer and vendor management.

Those who self-identified as doing the work of privacy within an organization continued beyond initial demographic questions, while those working as external counsel, consultants, for technology vendors, and other privacy professionals were filtered out.

WEIGHTING: The 2018 results were statistically weighted to match the employee size distribution of firms answering the 2017 survey. This distribution matching allows us to make apples to apples comparisons between findings from the two years.

SEGMENTS: Segments of the sample with fewer than 20 respondents have been flagged as "small sample size." Results from these segments should be considered directional and suggestive rather than statistically definitive.

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 (B2B), business-to-consumer (B2C), 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 the C-suite.

Full-time vs. 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. Only that they spend 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 General Data Protection Regulation.

Privacy leader: We ask respondents to self-report whether they are the "leader" 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.

Regulated vs. Unregulated industries: For the purposes of comparison, we categorize traditionally "regulated" industries as anything in the health care or financial services fields.

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

Privacy staffing has grown and will accelerate

Make no mistake: The GDPR has created a significant demand for privacy professionals, especially in firms that are facing privacy regulation for the first time.

In this fourth iteration of the IAPP-EY Privacy Governance Report, we see a significant increase in the number of privacy professionals working full time in dedicated privacy programs — the global mean number of employees working full time in privacy programs has climbed over last year from 6.8 to 10 full-time privacy employees.

In terms of raw numbers, the firms with the largest privacy staffs are (unsurprisingly) the largest and wealthiest firms. Companies that we call "unregulated" because (unlike the health, pharmaceutical, finance, and insurance industries) they have not previously been heavily regulated for privacy and data protection, are the most likely to have large, dedicated, full-time privacy teams — on average more than 14 employees — and are also most likely to have privacy professionals working part-time in internal business units.

Employees Dedicated to Privacy

2018

	Mean	Median
Full-time privacy, in privacy program	10.0	2
Full time privacy, in internal service centers	3.5	0
Full time privacy, in revenue based business units	4.0	0
Part time privacy, in privacy program	4.6	1
Part time privacy, in internal service centers	6.2	2
Part time privacy, in revenue based business units	7.6	1

Profile of Survey Respondents

The English-language survey was sent to subscribers of the IAPP's Daily Dashboard, roughly half of whom are IAPP members. We limited our survey to those who hold in-house privacy positions and did not gather data from outside attorneys or consultants, similar to years past. Accordingly, this year's survey results reflect primarily the experiences of in-house privacy professionals in the private sector (81 percent), with a modest showing of government-based privacy pros (11 percent).

For the first time since this survey was launched four years ago, more respondents are from outside of the United States than within. Only 43 percent of privacy professionals responding to the survey are from the U.S., while 37 percent are from the European Union (including 13 percent from the United Kingdom), up 15 points from last year and 18 points from the 2015 survey.

continued on xi

Firms located in the U.S. are more likely to have more full-time staff in privacy programs than their EU counterparts, while EU firms are more likely to have part-time privacy staff working throughout the organization. However, much of the variation comes at the top of the scale — looking at the median program size shows half of all programs on both sides of the Atlantic only have two full-time, and four part-time, employees with privacy work on their desks. Or fewer.

One of the primary reasons for having a privacy program at all, according to this year's survey, is to respond to demands from business partners. The GDPR's mandatory requirements for vetting and entering contracts with data processors creates increased demand on privacy professionals for B2B-related transactions. Accordingly, we see that the B2B-focused businesses are far more likely than B2C and even than blended firms to have full-time privacy professionals working in their privacy programs.

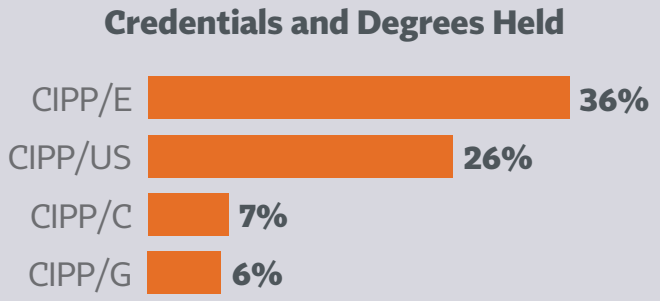
So-called "regulated" firms — health, pharma, finance, and insurance — generally have fewer people on the core privacy team, but they expect many people in the firm to participate in privacy functions. Although a survey respondent working in the health sector is more likely than not working full-time in privacy, the general trend among financial, insurance, health, and pharma firms is to have a smaller dedicated privacy team and to place privacy responsibility on the shoulders of employees in business units distributed throughout the firm.

There are two factors at work here. On one hand, data is a strategic driver of revenue for many of these "unregulated" organizations; social media, gig-sharing apps, and many of the companies of the Digital Age need privacy to help understand how to monetize their data. On the other hand, this logically reflects the idea that building a new privacy compliance program requires an initial full-time effort, but that over time some regulatory compliance and data governance responsibilities can and should be distributed deeper and wider within the firm. As discussed later, this is also reflected in increased privacy training and awareness activities, many of which are now required of employees who will only be dedicated part-time to privacy.

continued from x

Europe's presence in this survey is palpable. It influences the overall staffing and budget scores, the GDPR compliance analysis, and the role of privacy leaders and their staff. It even influences IAPP certifications. Whereas in 2017 the CIPP/US continued to be the most popular certification among survey respondents, with 38 percent holding the credential, this year CIPP/E has top billing at 36 percent, with only 26 percent of survey respondents holding the CIPP/US certification. Even those holding the CIPM credential — important to serving the data protection officer role mandated by the GDPR — eclipse the CIPP/US ranks at 30 percent of all respondents.

Fewer respondents work in industries we call "regulated," such as health



continued on xii

As for future growth, survey respondents are much more likely to anticipate additional staffing growth this year than they were last year, with 41 percent expecting an increase in full-time privacy professionals in the 2018 survey, compared with 28 percent in 2017.

Privacy professionals may have less budget to work with, however. The average spend to come into GDPR compliance was $1.3 million last year, including work to adapt products and services, with an additional expected spend of $1.8 million. The average privacy budget, however, has dropped from $2.1 million in 2017 to $1 million this year. This can be attributed to multiple factors: First, we see a significant drop in the spend by large companies, who spent a great deal on the massive GDPR preparation cycle and now are cutting back significantly. While the largest organizations in our survey last year spent as much as $6 million and $7 million annually, this year the largest size bands report average budgets in the $1-$2 million range. Second, there is the anecdotal story many in privacy are telling: They spent well over budget last year, as GDPR compliance costs ran high, and are now facing a smaller budget to compensate.

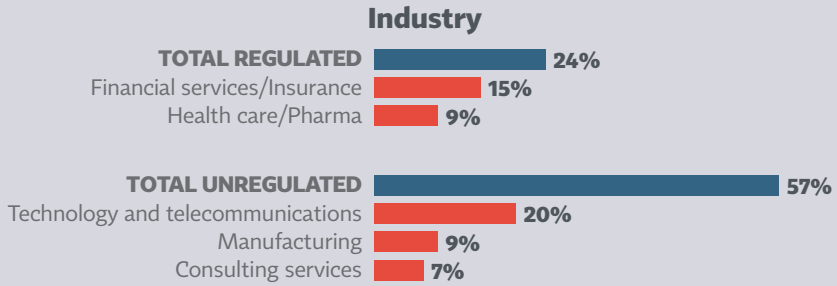
One interesting metric we've provided this year is spend per employee, which you'll see throughout the various ways we slice the data. What it makes clear is that while spend increases with the size of the company, it does not increase linearly. There would appear to be a base cost to privacy compliance that is not overly different between a company with 5,000 or 50,000 employees.

GDPR IN PRACTICE: Colorado has a new privacy law that mandates data destruction when it's no longer needed for a business purpose. If the GDPR is any indication, privacy law can indeed provide the necessary incentive to encourage firms finally to implement what has long been considered a sound privacy (and security) practice. In our survey, 76 percent of firms report GDPR has motivated them to delete data, while another 21 percent intend to soon.

In general, we are seeing that disruptive new regulation like the GDPR requires a significant initial program development investment and then a lower budget for ongoing compliance and maintenance over time. We expect

continued from xi

care, pharmaceuticals, financial services and insurance (24 percent) than in "unregulated" industries (57 percent). Breaking out the regulated industries, only 15 percent represent financial services or insurance, while 9 percent are in health care or pharma. The bulk of respondents from unregulated industries work in the technology



or telecommunications sectors (20 percent). Government employees represent 11 percent of survey respondents.

Although the geographic mix has shifted decidedly toward Europe, the Privacy Governance Report continues to reflect a healthy mix of business models, company size by

continued on xiii

this to play out in response to the new California Consumer Privacy Act (aka CaCPA) as well, which affects any company doing business with California residents. Indeed, privacy professionals are busy comparing their GDPR compliance efforts to CaCPA, looking to leverage existing programs, while waiting to see if the U.S. passes a comprehensive federal privacy law in the coming months.

If the $3 million average spend for GDPR compliance is any indication, CaCPA, or a pre-emptive federal U.S. law, will likely have significant business impact.

Privacy leadership and the DPO

Privacy functions continue their steady spread throughout the firm beyond the dedicated privacy staff and privacy leadership roles. They also continue to migrate out of the legal and compliance departments — which are still by far their most popular spots — to information security, information technology, and "other" departments.

We asked respondents to identify themselves as the person in charge of privacy for their organization (a "privacy leader"), the person who makes decisions on privacy operations and budget allocation. This year, privacy leaders comprise two out of every three survey respondents (similar to 2017). They are most likely:

- Located in Legal (43 percent).
- Also busy with matters other than privacy (61 percent).
- Also fulfilling the DPO function, especially if working for an EU-based firm (67 percent); a health-care company (85 percent); or a company with fewer than 5,000 employees (75 percent).

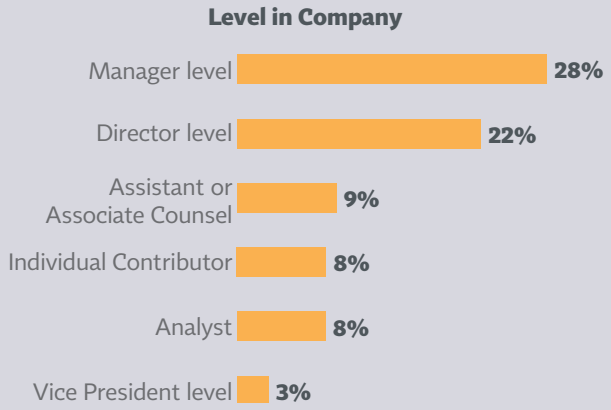
Privacy leaders fill the DPO role 56 percent of time for organizations that have the function (75 percent have a DPO, 45 percent of those have more than one). Where the leader isn't the DPO, the DPO reports to the privacy leader 65 percent of the time.

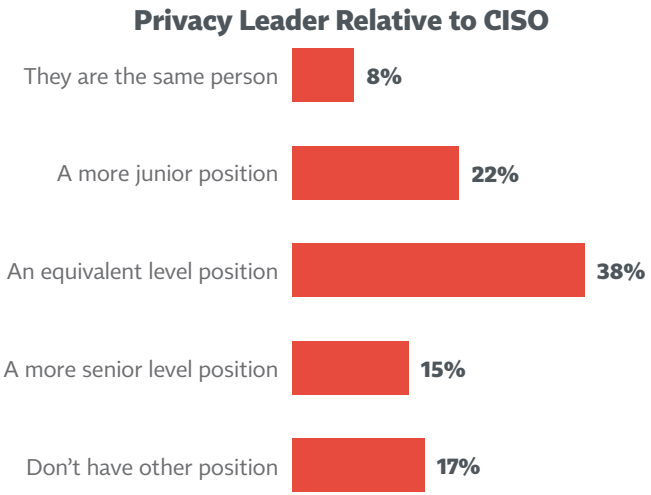
Maybe it's not surprising, then, that 44 percent of DPOs have at least some dedicated staff, and when the privacy leader is the DPO, 37 percent of them have full-time staff.

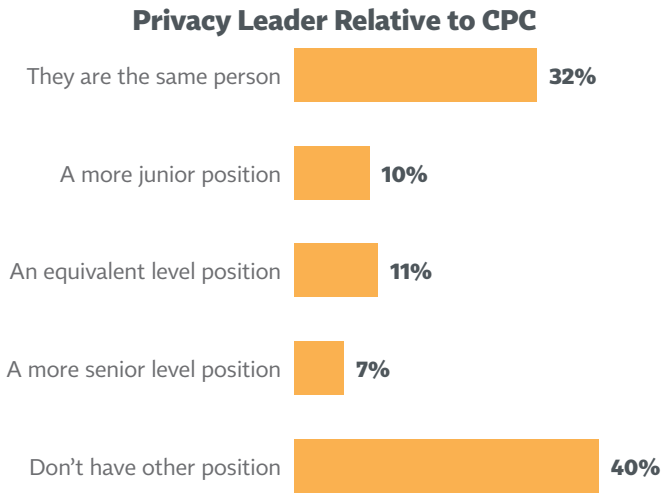
continued from xii

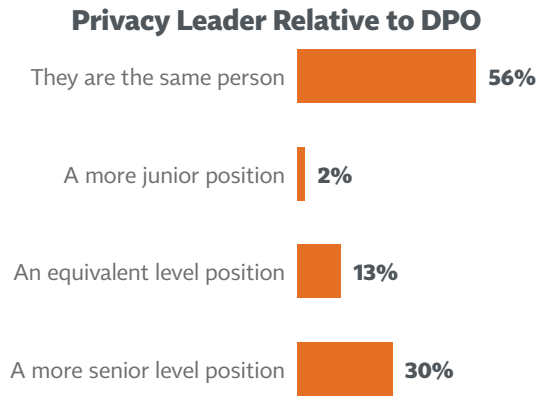
employees, and company size by revenues. Slightly more than three in 10 companies focus on the B2B market, while just under 20 percent are exclusively B2C, and nearly half (48 percent) work in a blended field.

Like last year, those most likely to respond to the survey hold manager-level positions (28 percent, up from 20 percent in 2016). This year's survey reflects more responses from directors than last (22 percent over 17 percent in 2017). Most likely due to the influence of European voices in this year's survey, we see a directional decline in the number holding the "assistant or associate counsel" title (down to 9 percent from 12 percent last year), the "general counsel" title (down 7 points to just 4 percent of respondents), and the "vice president" title (down from 7 percent to just 3 percent of this year's survey).









Nearly one in three privacy leaders serve the chief privacy counsel function, and one in four privacy leaders reports directly to the general counsel. Higher still in the organization, almost one in five report directly to the CEO.

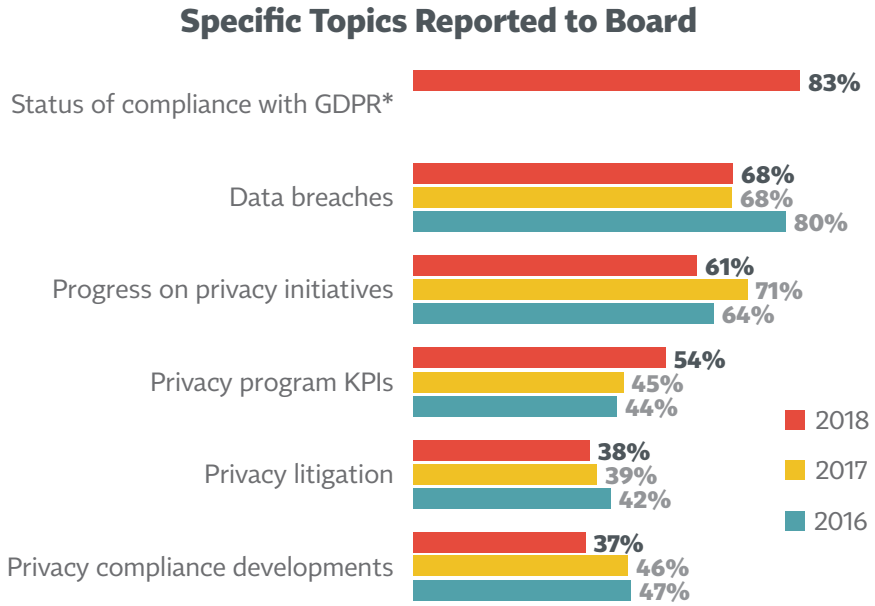
Privacy leaders very rarely also serve the function of a chief information security officer (only 8 percent do), but find they frequently (38 percent) work at the same level, while 15 percent are senior to the CISO, and 22 percent are junior. When we dive into U.S. versus EU structures, we predictably see U.S. companies are more likely than EU firms to even have a CISO, and U.S. privacy leaders are directionally more likely than their EU counterparts to be equal to the CISO.

> **GDPR IN PRACTICE:** Article 37 of the GDPR mandates that certain firms appoint a DPO. Of those firms who appointed a DPO in response to the GDPR, nearly half (48 percent) did so even though they were not obliged because it serves a valuable function for the firm.

Privacy leaders are making themselves heard at the highest levels of management, with 37 percent personally reporting privacy issues to the Board of Directors. This year, 78 percent of respondents say the Board wants to hear about privacy, compared to 72 percent in 2016. The Board seems to care the most about whether the firm has its GDPR house in order and progress on compliance (83 percent) and next most about data breaches (68 percent) and progress on privacy initiatives (61 percent).

Data breaches remain a Board-level privacy concern, but they have given way to GDPR compliance efforts as the top Board topic and they are significantly less important than they were two years ago, when 80 percent reported that breaches were a Board-level topic.

Interestingly, where the privacy leader is the DPO, privacy is reported to the Board 92 percent of the time.



GDPR compliance is less daunting this year, but 56 percent not yet ready

Three out of four survey respondents report that their firm falls under the scope of the GDPR, despite only 31 percent of respondent-companies being headquartered in the European Union. And, indeed, firms invested heavily in 2017 to prepare for GDPR. That investment took the form of hiring new people — on average 2.8 full-time and 2.5 part-time employees just for GDPR compliance, with the largest firms (over 75,000 employees) hiring more than six full-time and six part-time people for GDPR tasks.

GDPR compliance also involved promoting others from within the firm to do the job of privacy; more than half the firms either gave or plan to give the privacy leader an elevated status within the firm in response to GDPR. Eighty-nine percent of EU firms have appointed a DPO in response to the GDPR, while 67 percent of U.S. firms have done so.

That compliance effort also included engaging outside consultants and attorneys to help create GDPR compliance strategies and operational plans and draft new policies and vendor contracts. Three out of four companies complying with GDPR had to adapt their products and services to the new regulation.

Overall, firms report they will spend a total average of $3 million to address GDPR when all is said and done, and although their spending is slowing down it is not about to stop.

Distribution of Additional GDPR Compliance Budget
(Among Companies Saying They Must Comply with the GDPR)

All that investment has paid some dividends. Privacy is more involved in every stage of ongoing activities and new initiatives, reflecting privacy's new priority in product development, risk assessments for new projects, and as a top compliance and consumer trust concern.

GDPR IN PRACTICE: Standard Contractual Clauses are far and away the top mechanism for cross-border data transfers, used by 89 percent of all respondents. Privacy Shield is the next most popular, used by just under half of all respondents, even though those in the health and finance sectors are ineligible for the program. However, each mechanism is subject to validity challenge in EU courts, putting these popular tools on shaky ground. Binding corporate rules, largely considered the "safest" of transfer mechanisms, are only used by 28 percent of companies, reflecting the difficulty of getting them approved by an EU supervisory authority.

Encouragingly, GDPR does not seem to be quite as complicated to privacy professionals this year as it did in last year's survey. We asked respondents this year and last to rate how difficult they found several GDPR requirements on a 10-point scale, with 10 representing the highest level of difficulty. This year, difficulty scores went down for each GDPR-related compliance responsibility compared to 2017.

Data portability, for instance, once the most daunting issue, fell from a difficulty score of 6.3 out of 10 to just 5.3, reflecting perhaps the fact that businesses no longer expect consumers to invoke this right frequently. Gathering explicit consent — rating third most difficult on last year's scale with a 5.9 rating — fell to fifth at 4.6. This likely reflects an overall rejection of consent as the primary lawful basis for data processing. It also likely reflects the fact that although consent-based processing often requires reconfiguring consumer interfaces, developing consent record-keeping tools, and working collaboratively with many departments in the firm —

Controller v Processor

Among the 75 percent of respondents reporting that the GDPR applies to them, more than nine in 10 consider themselves a "controller" — defined in the GDPR as the natural or legal person that determines the purposes and means of personal data processing. Nearly seven in 10 (69 percent) consider themselves a "processor" — defined as the natural or legal person that processes personal data on the controller's behalf.

Obviously, many companies are sometimes a controller, and sometimes a processor, depending on the circumstances. But nearly one in three companies (27 percent) claim they are never a processor.

These distinctions are significant because they establish the ultimate responsibility for GDPR compliance and liability vis-à-vis the data subject, which rests principally with the controller.

Controllers are responsible for selecting trustworthy processors, of course, and, if a business relationship between two parties involves an exchange of personal data, defining the parties' roles in advance is crucial. If one is a controller and the other a processor this triggers obligations under GDPR Article 28 to select "only processors providing sufficient guarantees to implement appropriate

continued on xvii

difficult tasks for sure — many firms have now faced those responsibilities, tackled them head-on, and are on the other side of the business problem.

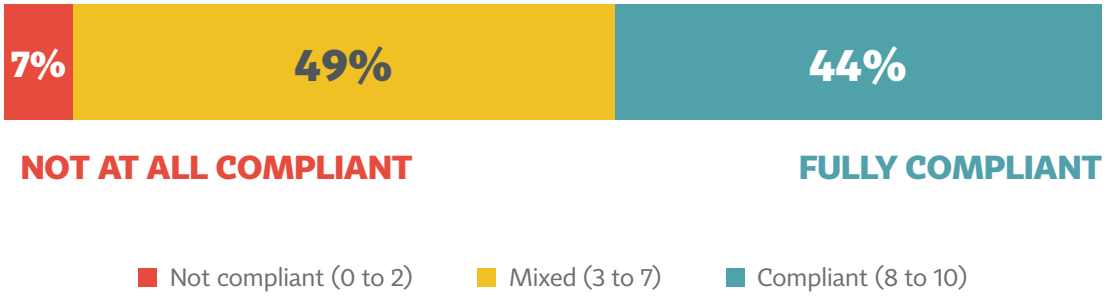
"We may be seeing an overall rejection of consent as the primary lawful basis for processing."

When we isolate U.S. firms, we find reported difficulties scores are higher across the board. U.S. privacy professionals are most concerned about the right to be forgotten, which they rate a 6.6 on a 10-point difficulty scale, reflecting, perhaps, the legal and perhaps even constitutional challenges this new right faces in the U.S. Permanently deleting customer data is contrary to most firm's practices and often made very difficult by their database of record.

U.S. privacy pros are also concerned about fulfilling data subject access requests, assigning this task a 6.2 on a difficulty scale of 10. This is a subject they will have to master as California's new Consumer Privacy Act also provides data access rights to consumers. And explicit consent is more difficult for U.S. firms — they give it a 5.5 difficulty rating compared to 4.2 assigned this task by their EU counterparts.

GDPR Compliance Status

(Among Companies Saying They Must Comply with the GDPR)

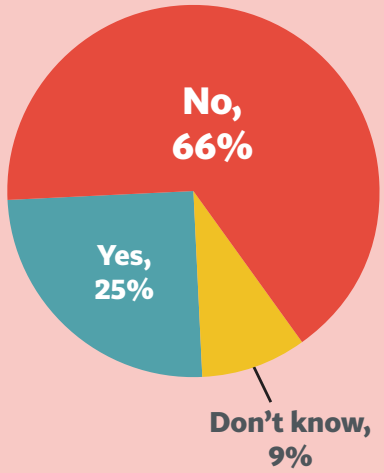


continued from xvi

technical and organizational measures" to meet the GDPR's obligations and "ensure the protection of the rights of the data subject."

Article 28 restricts whom the processor can engage as sub-processors and requires the parties to enter into a binding contract with specific stipulations. When these contracts stand alone, or are appended to master agreements, they have come to be called a "data processing agreement" or "data processing addendum" (DPA).

Changed Processors



According to our survey, nearly everyone — 95 percent of respondents — at some point engages another company to process data. This means companies are required by GDPR to vet the processor's "technical and organizational measures," confirm its GDPR compliance, and sign a DPA. We wanted to know whether the new burdens on these relationships changed

continued on xviii

A remarkable 19 percent — nearly one in five companies — feel full compliance is impossible.

It is often said that GDPR compliance is a journey, not a destination. The data this year agrees: Although 44 percent of firms give themselves a score of 8 or higher on the "fully compliant" scale, 56 percent admit that they have many steps yet to take to reach the destination. A select 7 percent rated themselves between 0 and 2 on the compliance scale.

What is more, although 81 percent of respondents have confidence they will eventually reach the GDPR compliance destination, a remarkable 19 percent — nearly one in five companies — feel full compliance is impossible.

When we separate out U.S. firms, however, we see confidence levels rise considerably. Even though more EU-based respondents report taking affirmative steps toward GDPR compliance in nearly every category, more than half of the respondents from the U.S. (53 percent) gave themselves an 8 or higher score on full GDPR compliance. Among their EU counterparts, meanwhile, this number drops to 38 percent.

Is this more "cowboy bravado" from U.S. organizations? Do EU firms better understand the complexity of successfully navigating EU regulation? Have U.S. firms made compliance more of a strategic goal, as non-compliance risks losing access to the EU marketplace?

continued from xvii

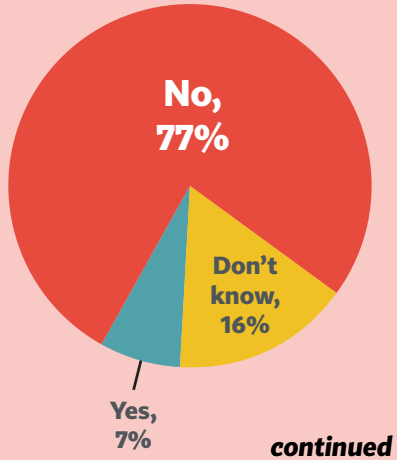
how controllers engaged with processors. Did controllers bring data processing in-house? Did they switch from one processor to another, perhaps one that was better prepared for GDPR? Did processors lose business because of the GDPR?

Our research found that if controllers were already outsourcing data processing, they continued to do so, and if they were already processing in-house they also stayed the course.

One quarter, however, of all respondents report they changed processors due to GDPR. This is not contradicted by responses from those who identified as a processor; 77 percent said they did not lose any business due to GDPR, but seven percent admitted that they did and a full 16 percent said they did not know.

A 25 percent shift in any market can cause major disruption. And the future may be highly unstable for data processors who fall

Lost Processing Business



continued on xix

Privacy training is hot, technology investments cooling

Although 2017 was a preparation year for GDPR, privacy professionals are still incredibly focused on the subject in 2018 and investments in many responsive steps is up over last year.

Nearly eight in 10 firms list training investments as their top GDPR compliance priority for the year.

Specifically, investments in training employees has shot up — widening its lead over other tasks by a considerable margin. Nearly eight in 10 firms list training investments as their top GDPR compliance priority for the year. Training is also high among privacy professionals' top priorities for their privacy programs overall. After creating privacy policies and governance programs (the top priority for 94 percent of respondents), the next most important task for privacy pros is "company privacy-related awareness and training" (90 percent). Eight out of 10 respondents also listed "development and training for privacy staff" as highly important.

What is more, while investing in technology was in second place in 2017 as a GDPR preparation task last year, it has slipped to third place this year. More than half of the respondents (57 percent) plan to invest in technology this year for GDPR preparation and compliance, but the need for those investments has remained flat with last year while many other preparations tasks have shot up in frequency.

continued from xviii

behind in their GDPR compliance efforts. Fewer than half of respondents are confident they will keep their existing processors, while 30 percent plan to change vendors. A meaningful 26 percent are still on the fence.

One in four have changed processors as a result of the GDPR.

This loudly signals that processors are well served to take the GDPR seriously if they'd like to hold on to their customers.

VENDOR MANAGEMENT

As the Facebook/Cambridge Analytica scandal revealed, data controllers have legal and ethical responsibility to know what happens to personal data shared with third parties including vendors.

Year over year, privacy professionals responding to the Governance Survey by and large report that their firms have vendor management programs in place. The proportion of respondents reporting such a program has dropped slightly since 2016, but this is likely explained by the change in the geographic makeup of our survey — U.S. respondents are 12 percent more likely than EU firms to have such a program and we have more EU respondents this year than last.

continued on xx

GDPR IN PRACTICE: Just two percent of companies report their data subject access request processes are fully automated, while 30 percent report the process is partially automated. More than half the respondents report their SAR process is entirely manual.

In spite of the significant rise in the privacy technology sector, 56 percent of respondents report they are still performing such tasks as data inventory and mapping manually and informally, while 33 percent report using an internally developed system. The market for commercial software isn't small, of course: 38 percent also use commercial software designed for these privacy tasks and another 31 percent use a commercial GRC tool customized to fit their needs.

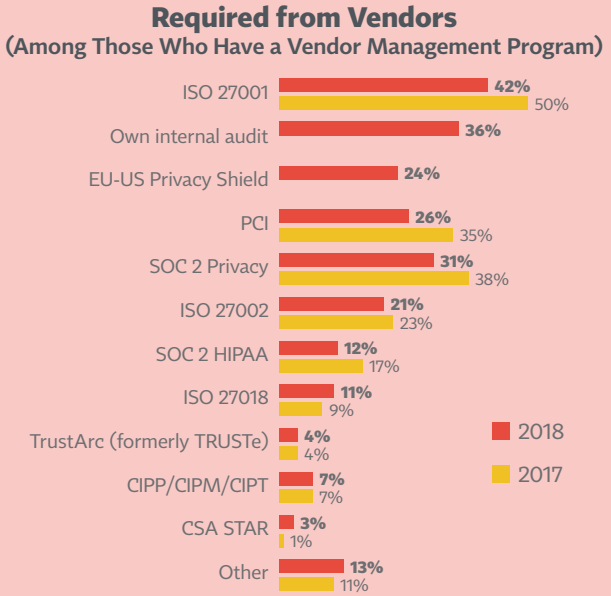
continued from xix

We also have a younger batch of companies this year, with the average privacy program age at five years, almost two years less than last year. While 87 percent of self-reported "mature" privacy teams have vendor management programs in place, it's just 61 percent for those in early-to-mid stage.

Vendor management programs vary among firms. Some delegate the program to procurement, which may often simply send out a stock questionnaire to the vendor that is not tailored to the transaction.

Some programs check for third-party certification, such as demonstrated compliance with ISO 27001 (42 percent) or SOC2 privacy (31 percent).

Many, however, engage in their own internal audit and investigation, likely consisting of reviewing privacy and security policies, conferring with the vendors' privacy and security counterparts, and perhaps even conducting on-site visits for major data transactions. Indeed, 50 percent of privacy professionals report that meeting business partner expectations is a major privacy function.



Nonetheless, the results suggest that while technology investments are made early in compliance programs, investments in people is important for the long term. Indeed, appointing a privacy professional in the form of a DPO is ahead of investing in technology (64 percent) as privacy pros prioritize GDPR compliance, while increasing privacy staff is tied for importance with technology investments this year (57 percent).

CONCLUSION

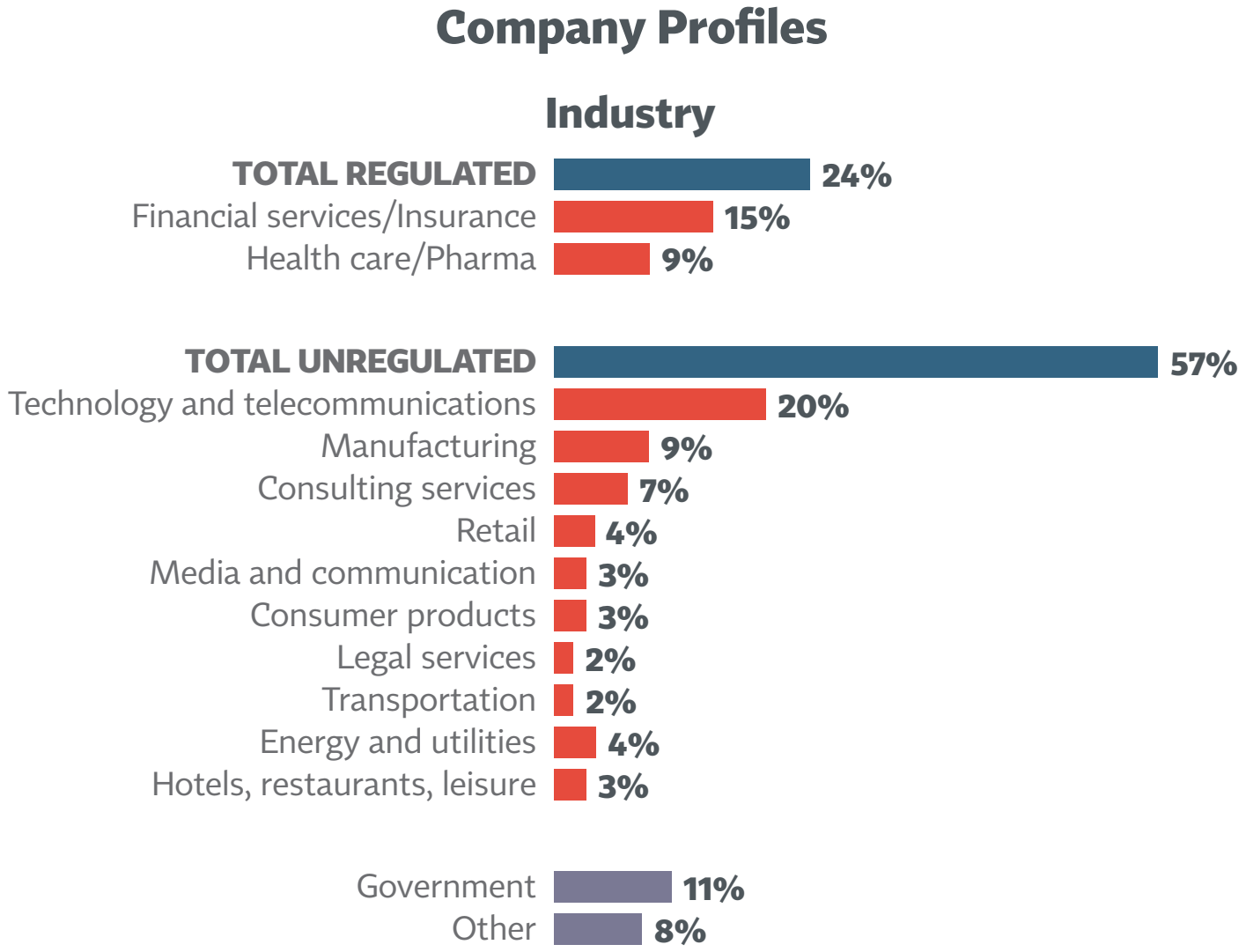
The EU's GDPR is driving significant investments in privacy personnel and technology. It is disrupting supply chains as data controllers shop for GDPR-savvy processors — up to 30 percent of controllers may be on the hunt for new processors in the coming year. One key to winning the controller client will be a willingness to sign standard contractual clauses — still by far the number one data transfer mechanism, in spite of the uncertainty plaguing this tool.

With 76 percent of all respondents believing they must comply with GDPR, it is obviously creating massive demand for privacy professionals, especially those prepared to serve the DPO role. It is also prompting major investments in privacy by design and internal privacy training. This is crucial to helping the 56 percent of companies not yet in compliance drag themselves closer to the goal.

While privacy budgets decline after last year's GDPR-bump, the demand for privacy staffing accelerates, especially in B2B firms. The GDPR is inspiring other governments to pass legislation mimicking many of its major priorities, including data processor privacy and security obligations, consumer rights of access and erasure, mandatory data protection officers, and data deletion requirements. This will keep privacy professionals busy for many years, whether or not GDPR results in much-feared enforcement action.

Contents

The largest portion of the data was gathered from tech and financial services companies

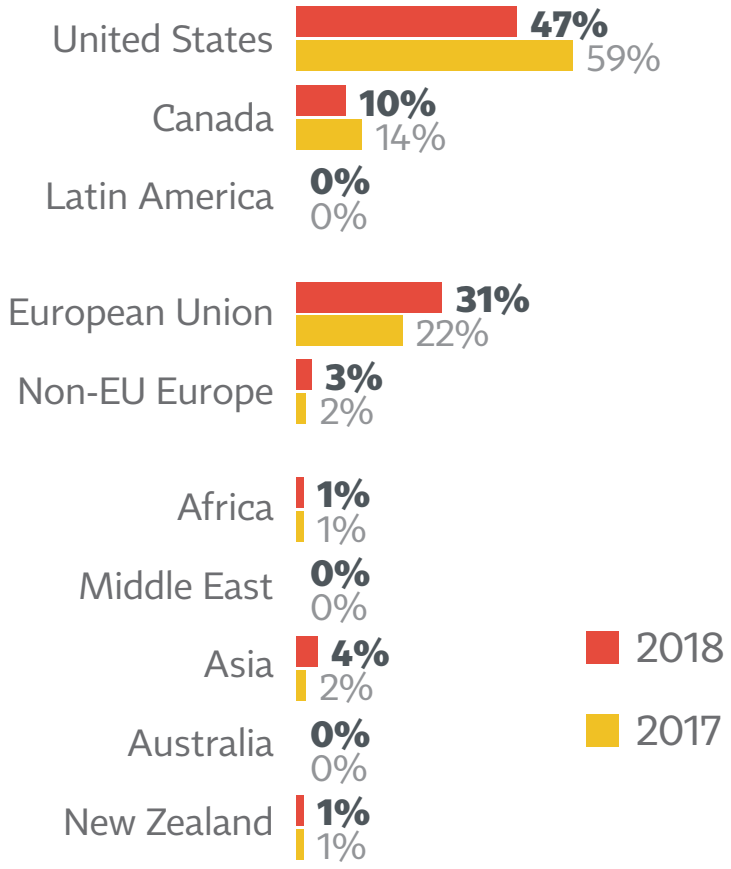


A1a. Which sector listed below best describes how your company would be classified?

They are globally diverse, with a larger proportion of European data than in past reports

Company Profiles

HQ Location



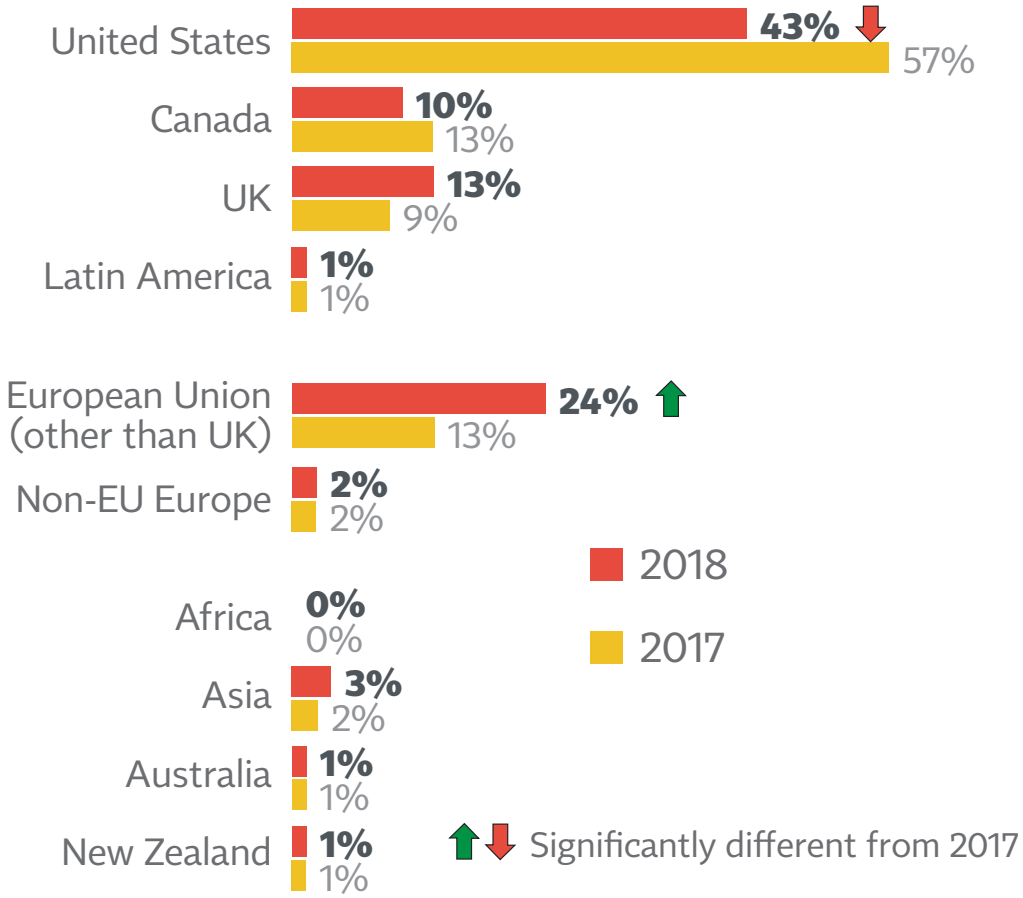
A4. What is the primary location of your company's headquarters?

Similarly, the individual respondents completing the surveys are more geographically diverse than in past years

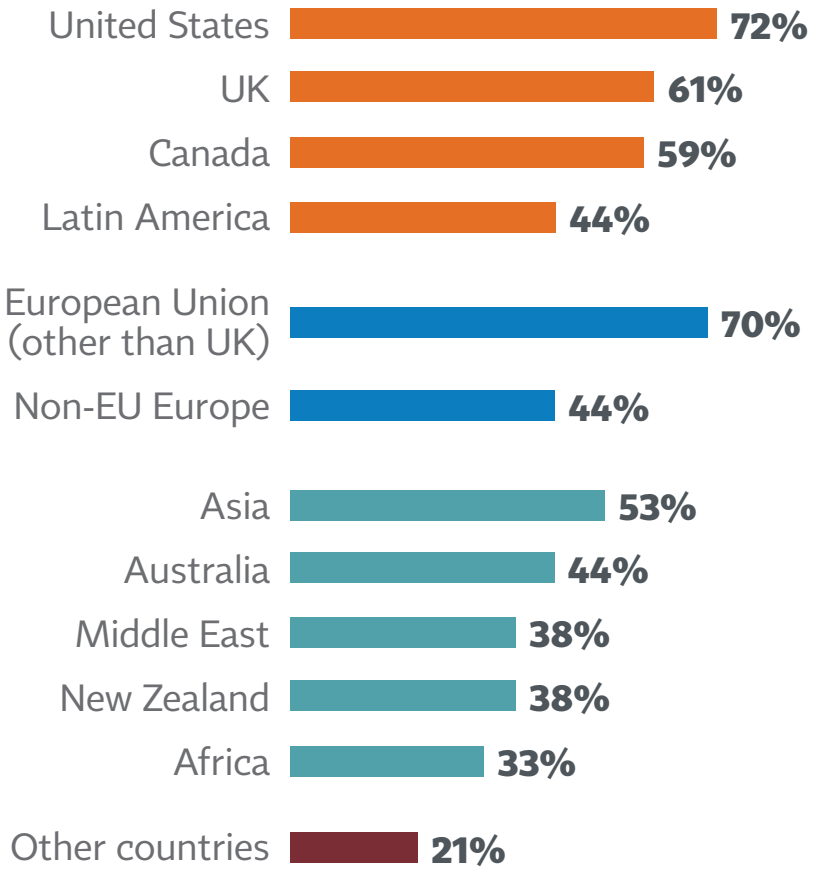
… and their organizations work beyond their national borders, with data subjects equally likely to be in the U.S. as the EU

Company Profiles

Location of Respondent



Where Data Subjects Reside

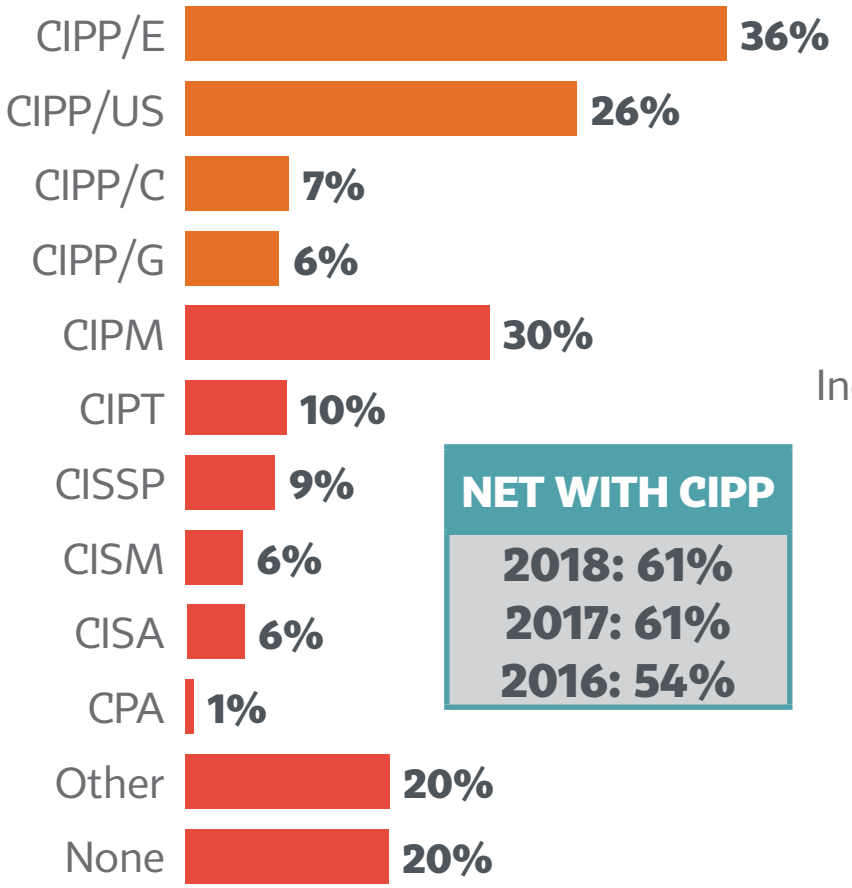


A5. In what region and country are you currently based?
A6. Do you collect personal data from data subjects in any of the following regions and countries?

These are privacy professionals, with a fair amount of technical proficiency …

… who do the work of privacy largely at the manager and non-board director level

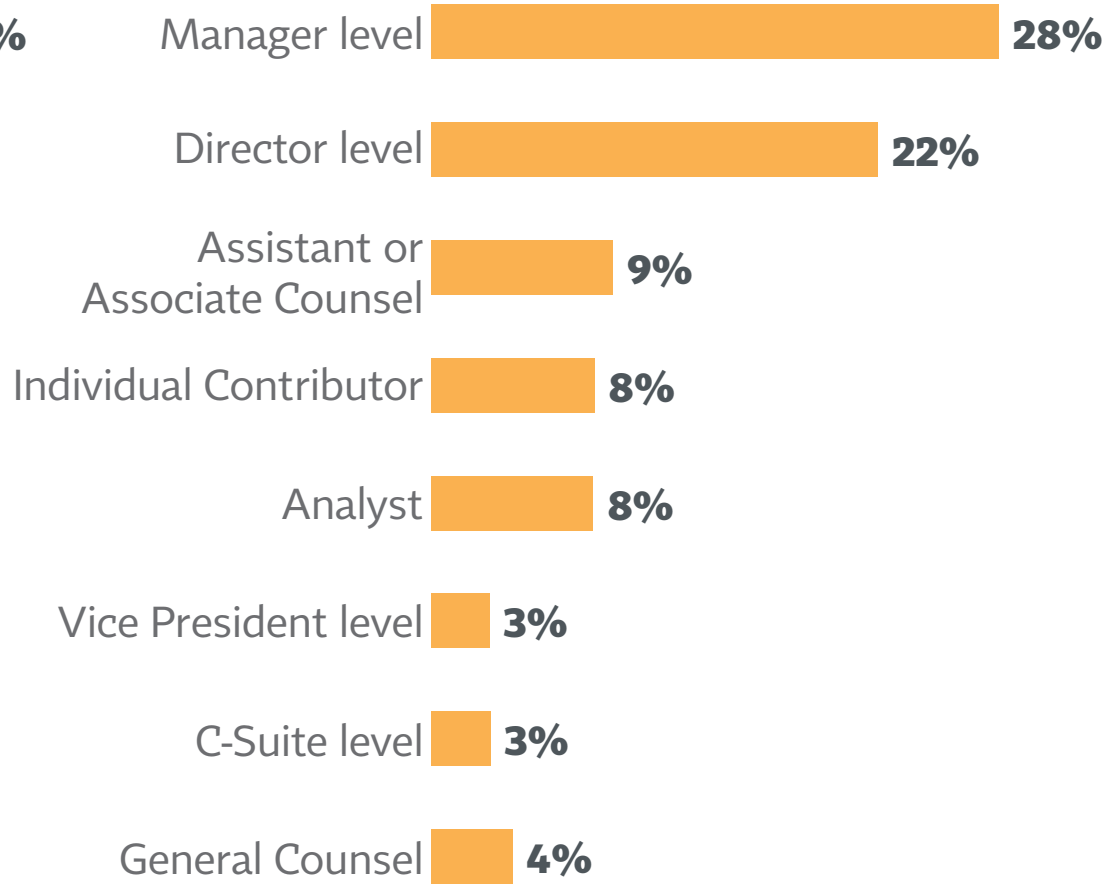
Credentials and Degrees Held



NET WITH CIPP

2018: 61%
2017: 61%
2016: 54%

Level in Company

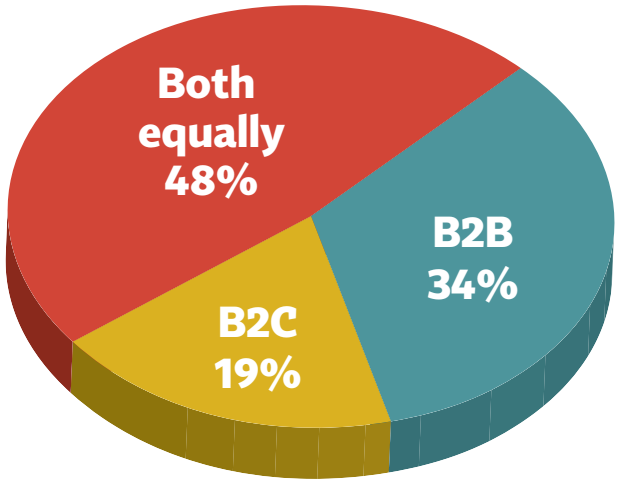


I1: Which certifications do you hold?
D2: Which of the following levels best describes your position in your company?

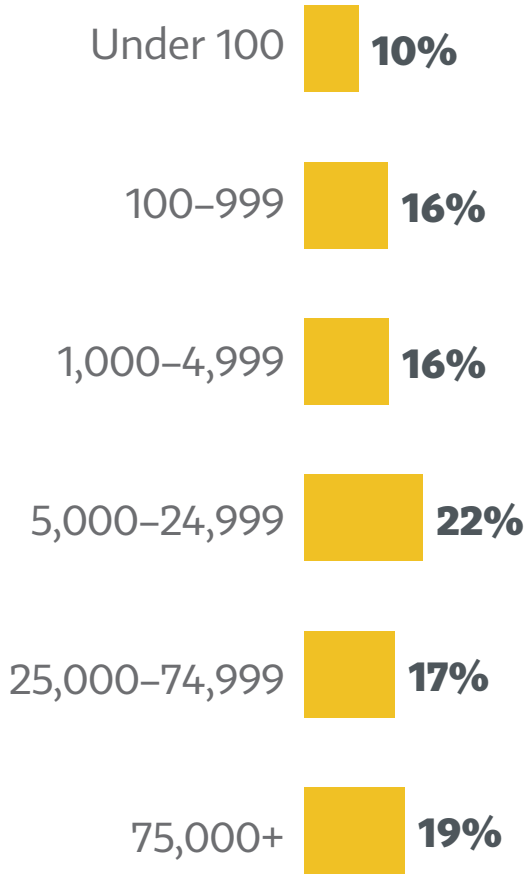
We are also able to analyze the data by business type and size

Company Profiles

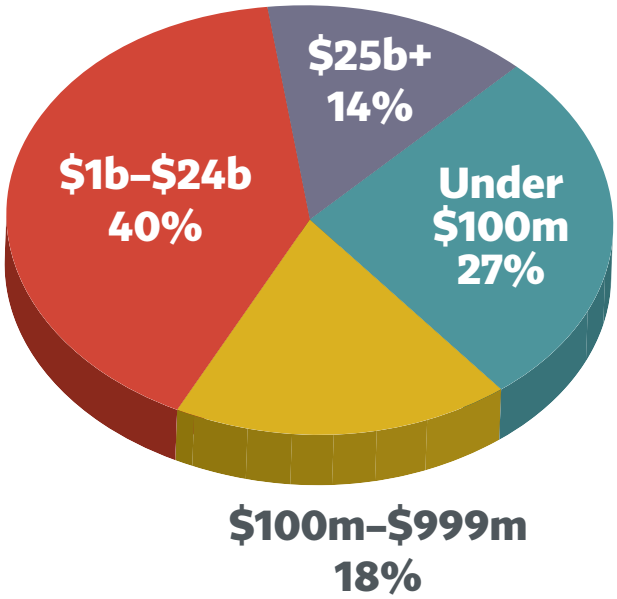
Customer Target



Employees



Revenue

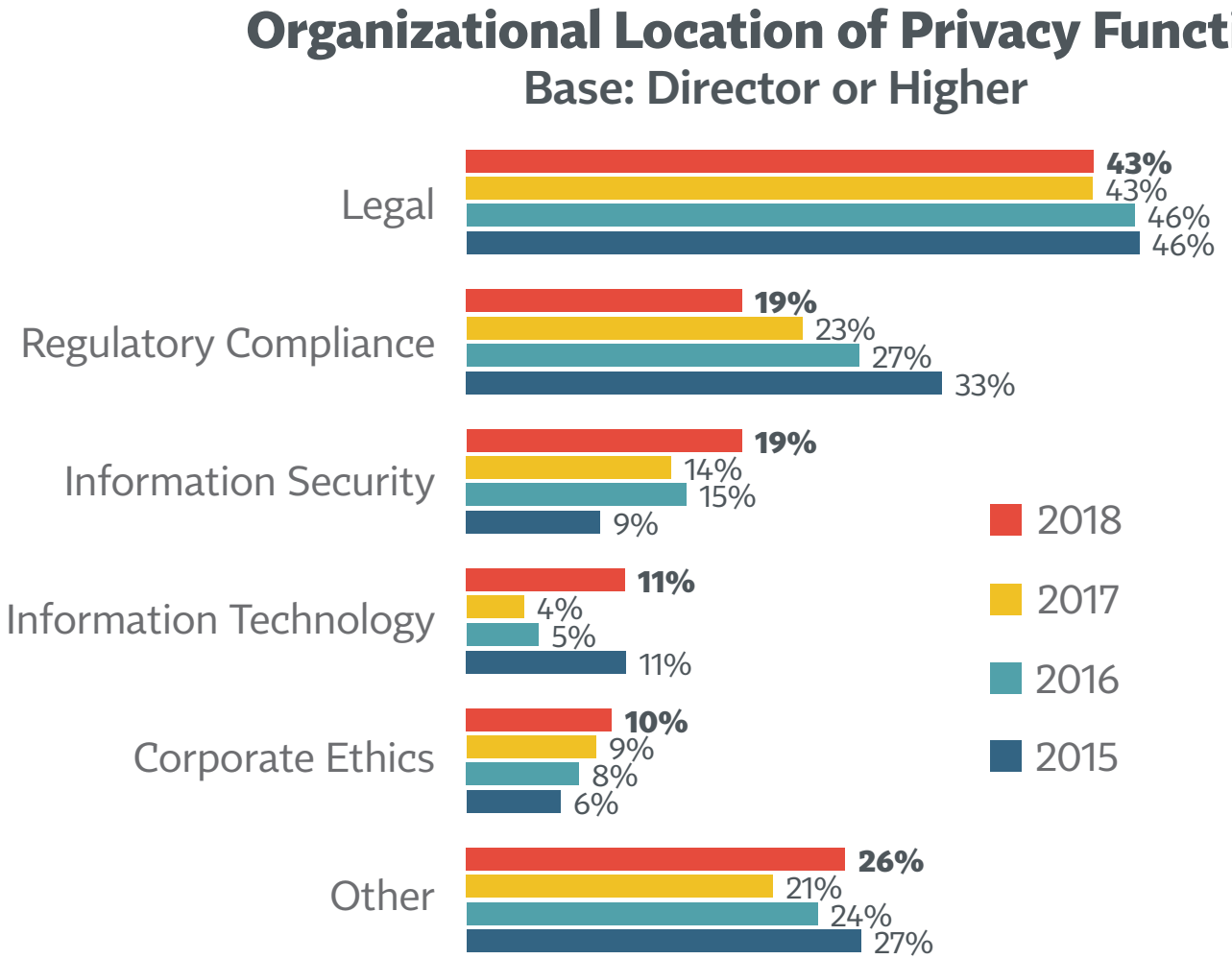


A1b. Does your company primarily serve:
A3. What is the total number of employees in your company (full-time and part-time)?
A2. Please tell us (as accurately as you can) your company's annual revenue.

Contents

Since 2015, the privacy function has moved away from compliance and toward IT and IS – and ethics

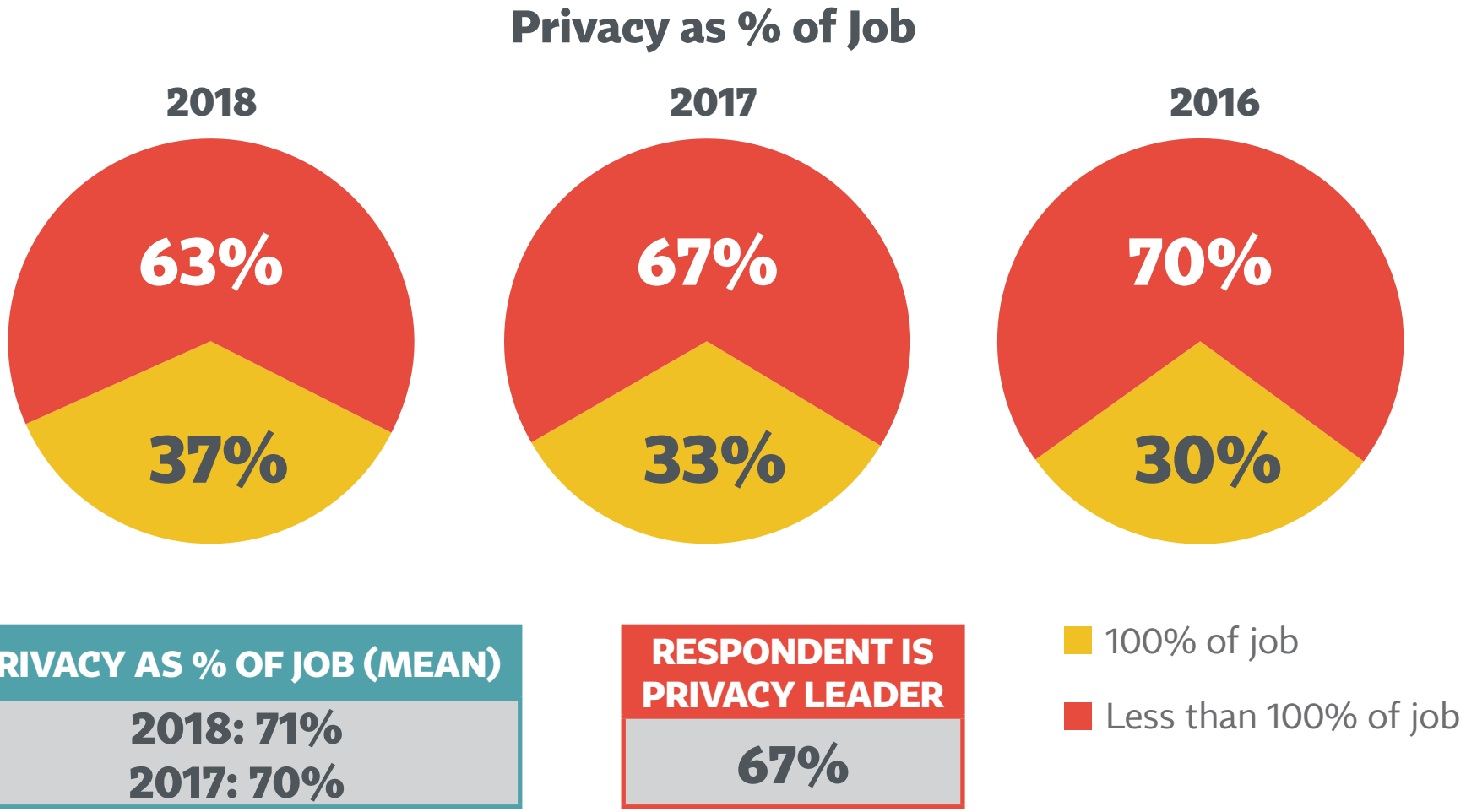
However, legal remains the functional area in which the privacy function is most likely to be housed



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

Further, the proportion of privacy professionals working full time on privacy has been increasing since 2016

Fewer than 4 in 10 work full time on privacy, but they spend 71% of their time on privacy matters; roughly 2/3 are their organization's privacy leader



PRIVACY AS % OF JOB (MEAN)
2018: 71%
2017: 70%

RESPONDENT IS PRIVACY LEADER
67%

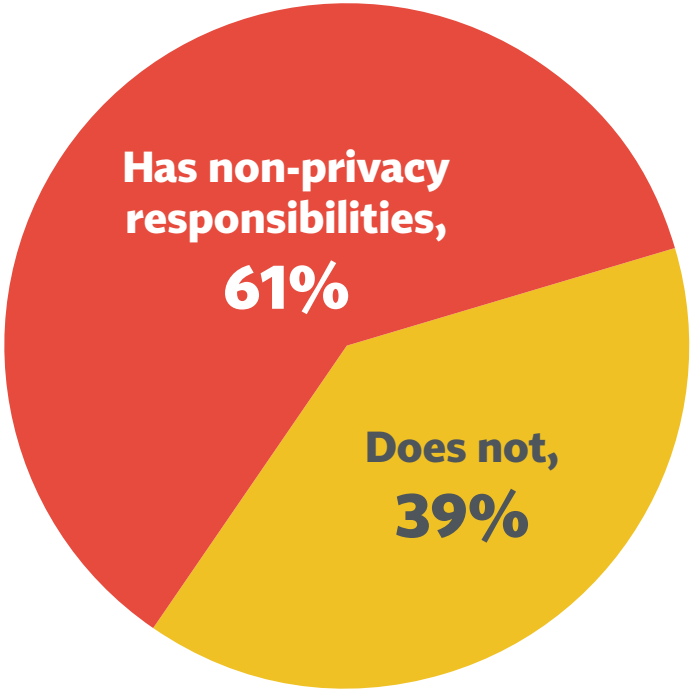
D1: About what percentage of your work at your company is made up of privacy responsibilities?

Privacy Leaders are no more likely to work full time on privacy than other privacy professionals

Though the proportion of privacy leaders who only work on privacy has been creeping up since 2016

Whether Privacy Leader Has Non-Privacy Responsibilities

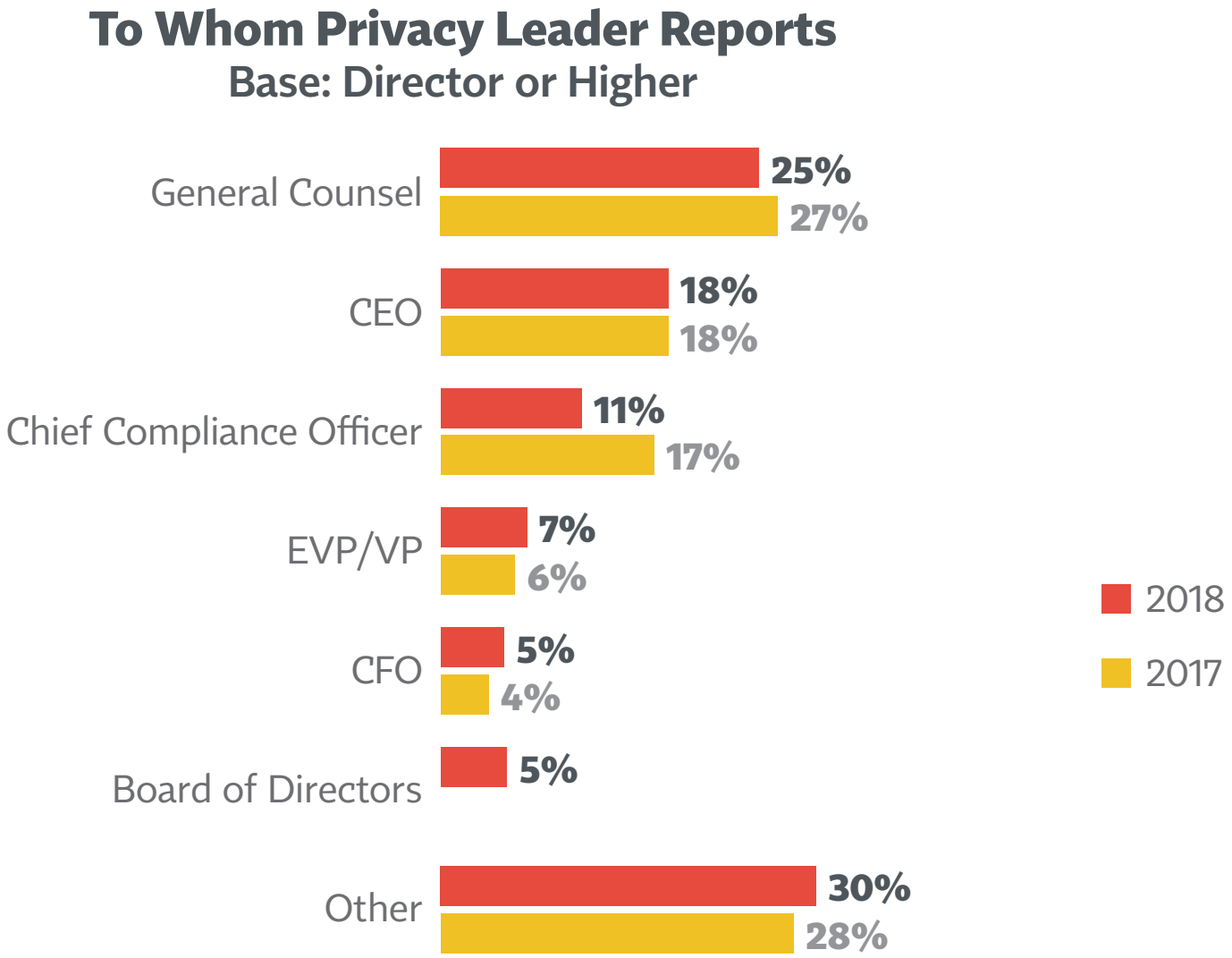
Base: Director or Higher



% WHERE PRIVACY LEADER ONLY WORKS ON PRIVACY
2018: 39%
2017: 37%
2016: 36%

F24: Does the individual designated as your company's privacy leader have responsibilities other than privacy?

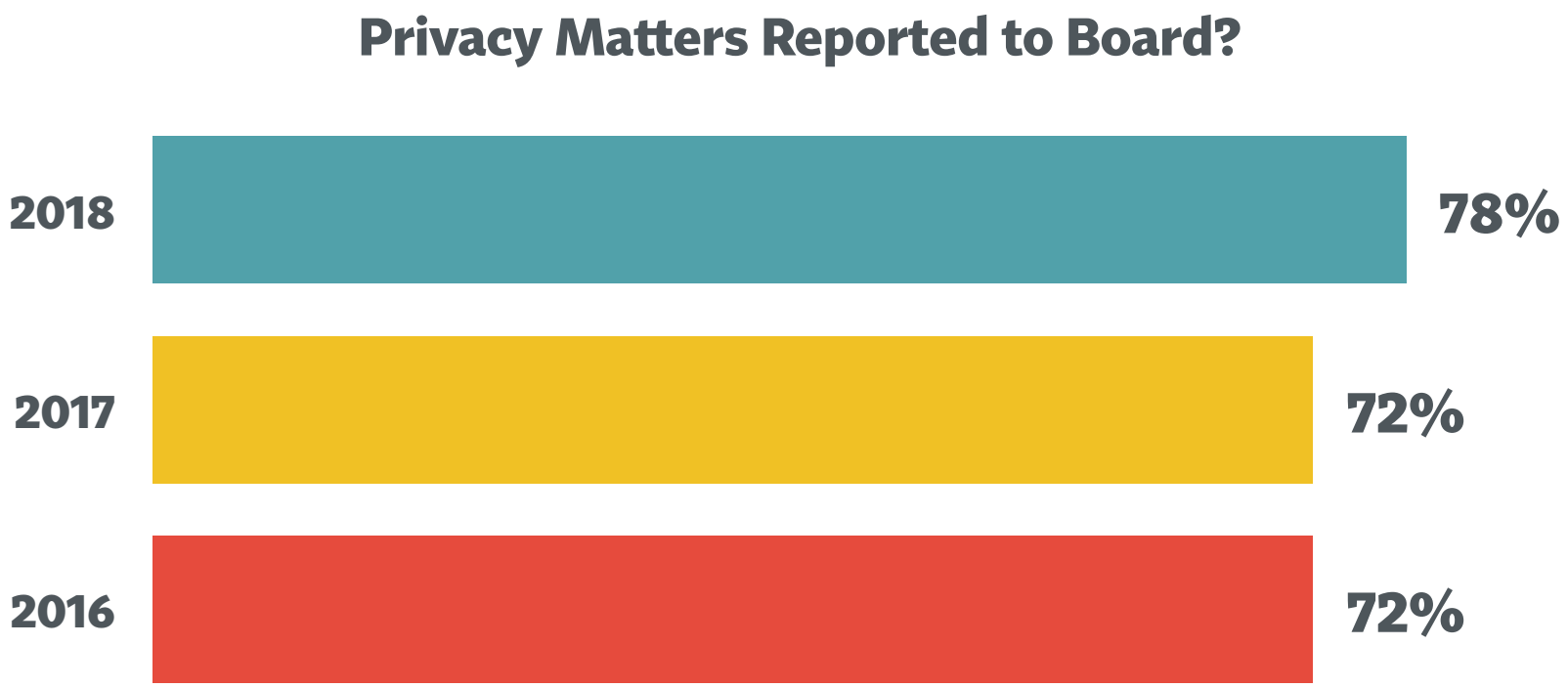
Privacy leaders are most likely to report to their firms' General Counsel or CEO, similar to 2017



F25. To whom in your company does the Privacy Leader report?

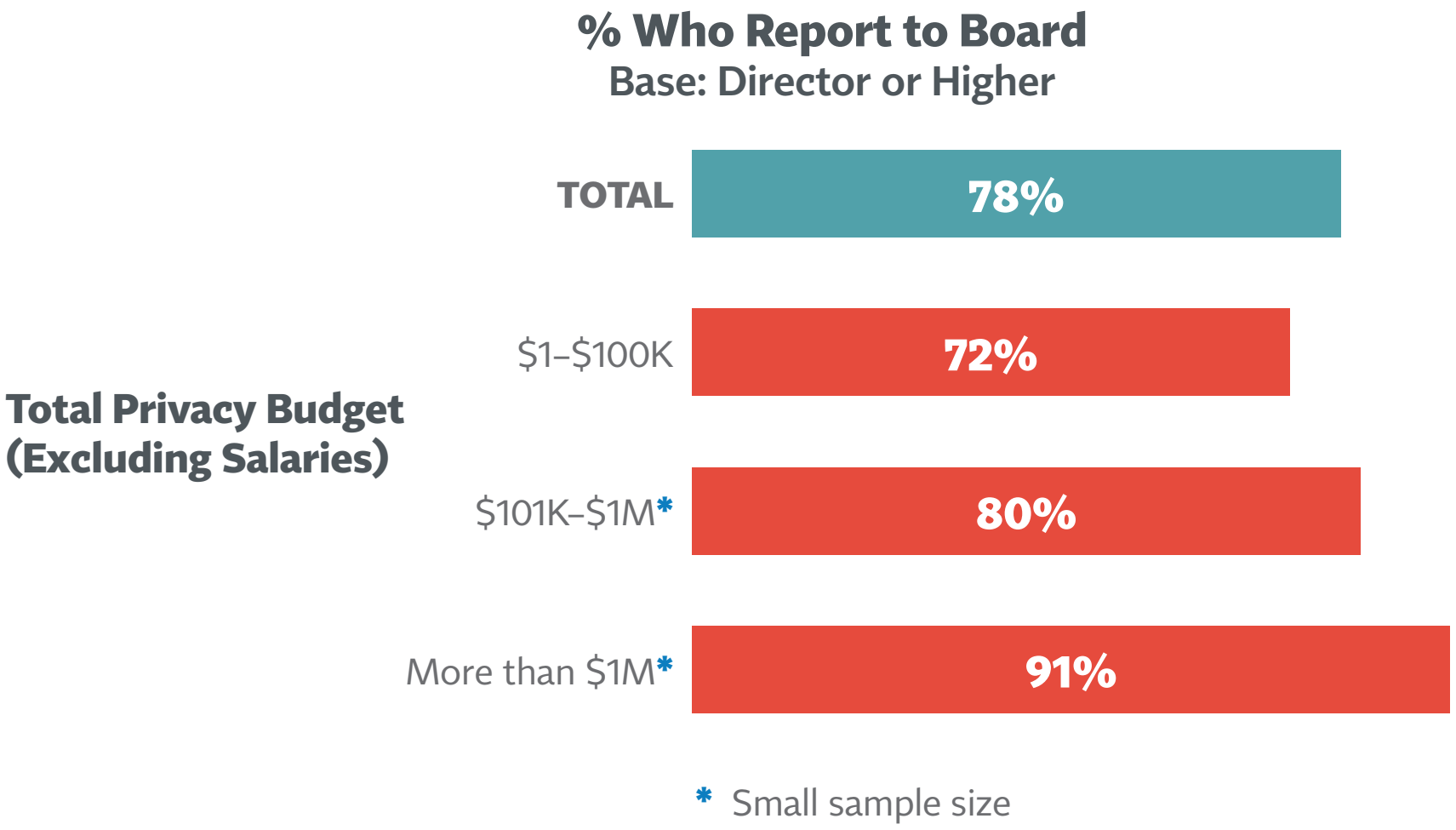
Nearly 8 in 10 respondents say privacy matters are reported to the company's board

That proportion is the highest it's been in three years



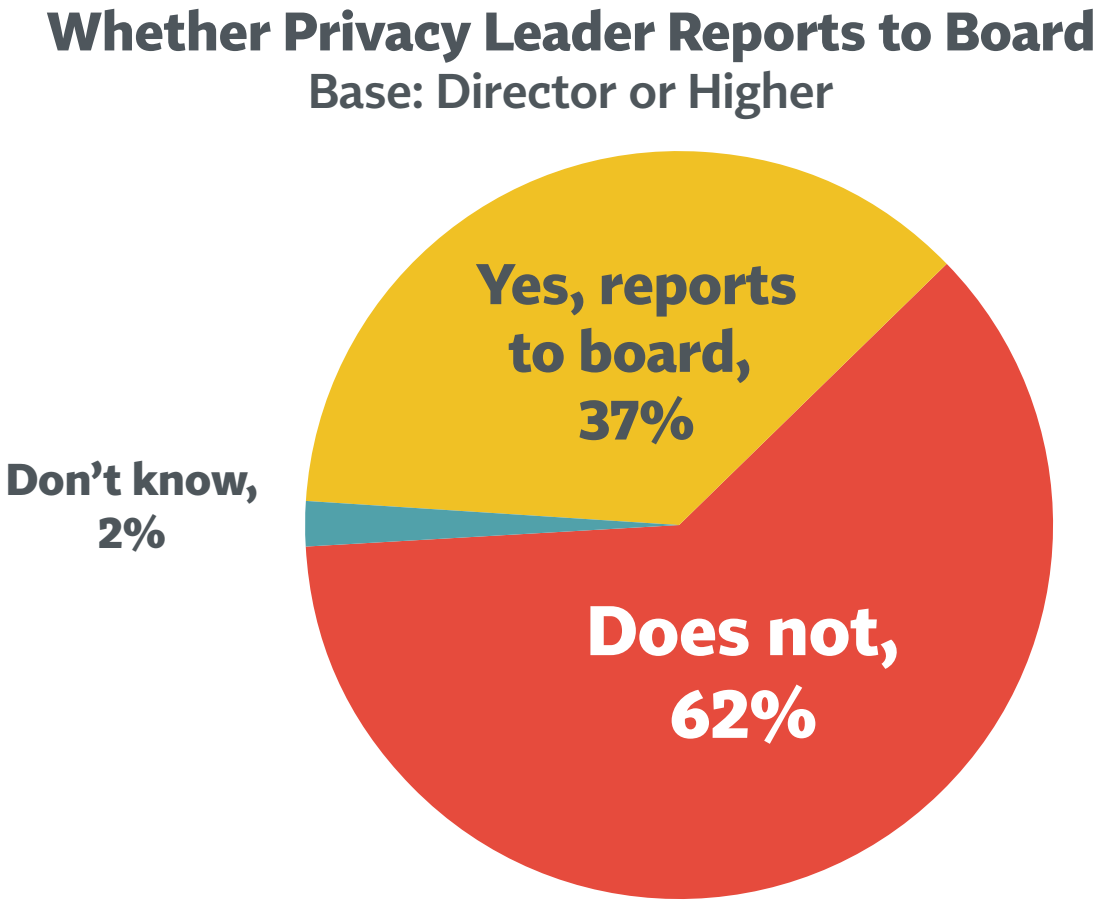
F38: Are privacy-related matters at your organization reported to the board of directors or the board level generally?

And where privacy is a board-level matter, budgets are correspondingly larger



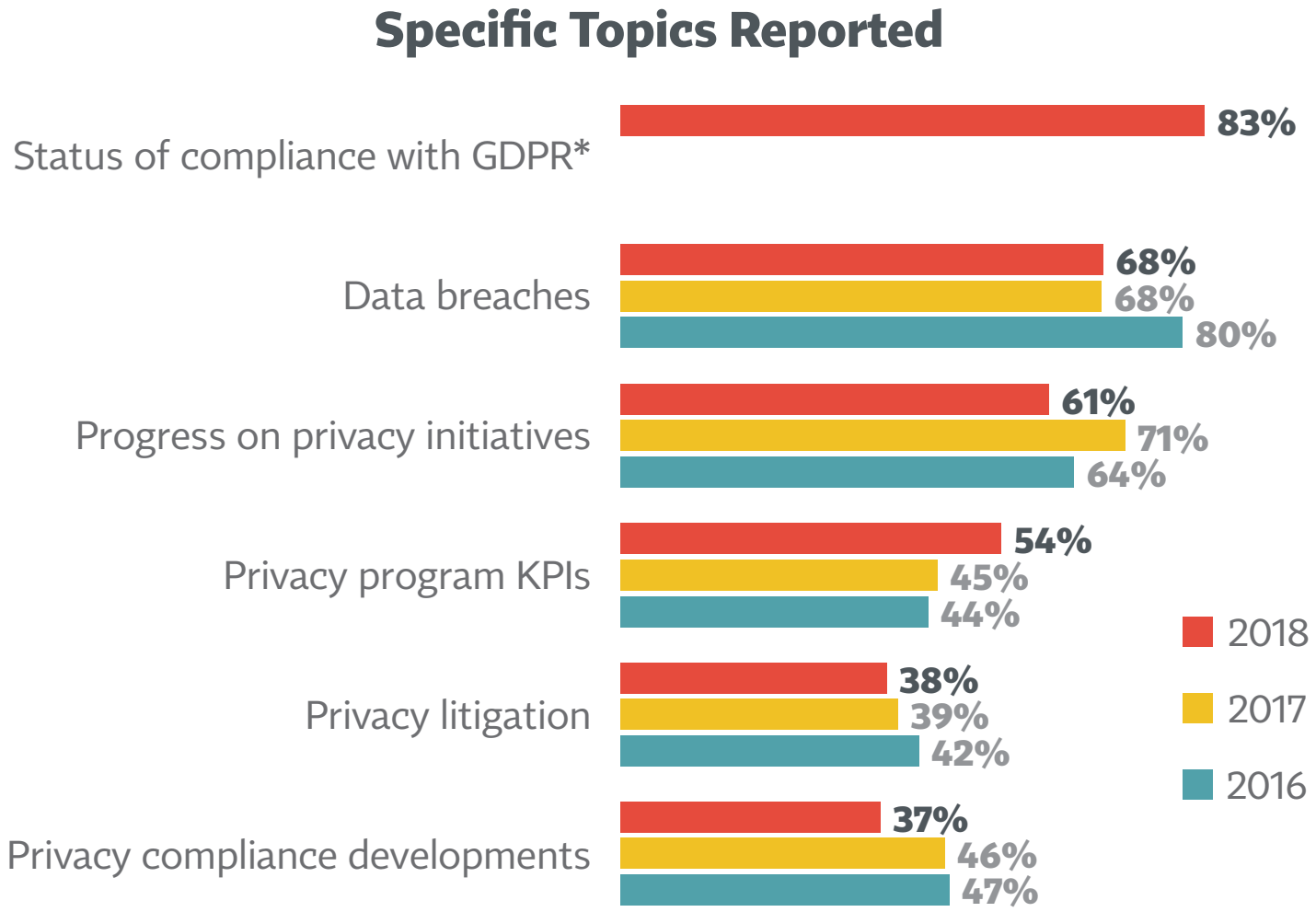
F38: Are privacy-related matters at your organization reported to the board of directors or the board level generally?

Where privacy matters are reported to the board, 37% say the Privacy Leader does the actual reporting



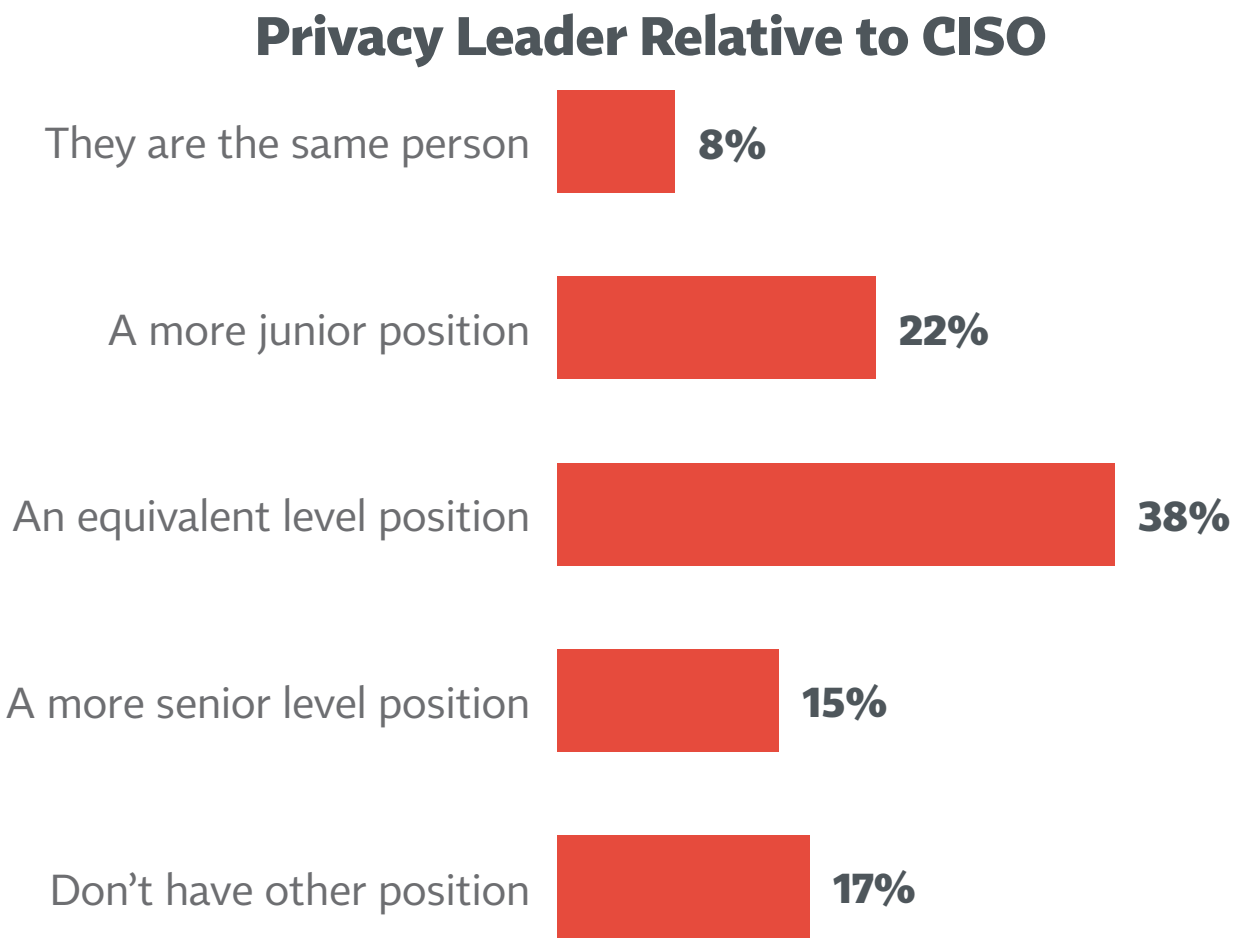
F26: Does the privacy leader report to your company's board of directors?

GDPR compliance status has leapt to the top of topics reported to the board, while privacy metrics gain steam



**Not asked in prior waves*
F39: What privacy topics are reported at the board level?

The Privacy Leader is slightly more likely to be junior to the CISO than senior, but they are most often peers



F22: How does the position of the Privacy Leader compare with your company's chief information security officer or the highest level information security person in the company?

US firms are more likely to have a CISO; the CISO is more likely to be junior to the Privacy Leader than senior

Privacy Leader vs. Chief Information Security Officer

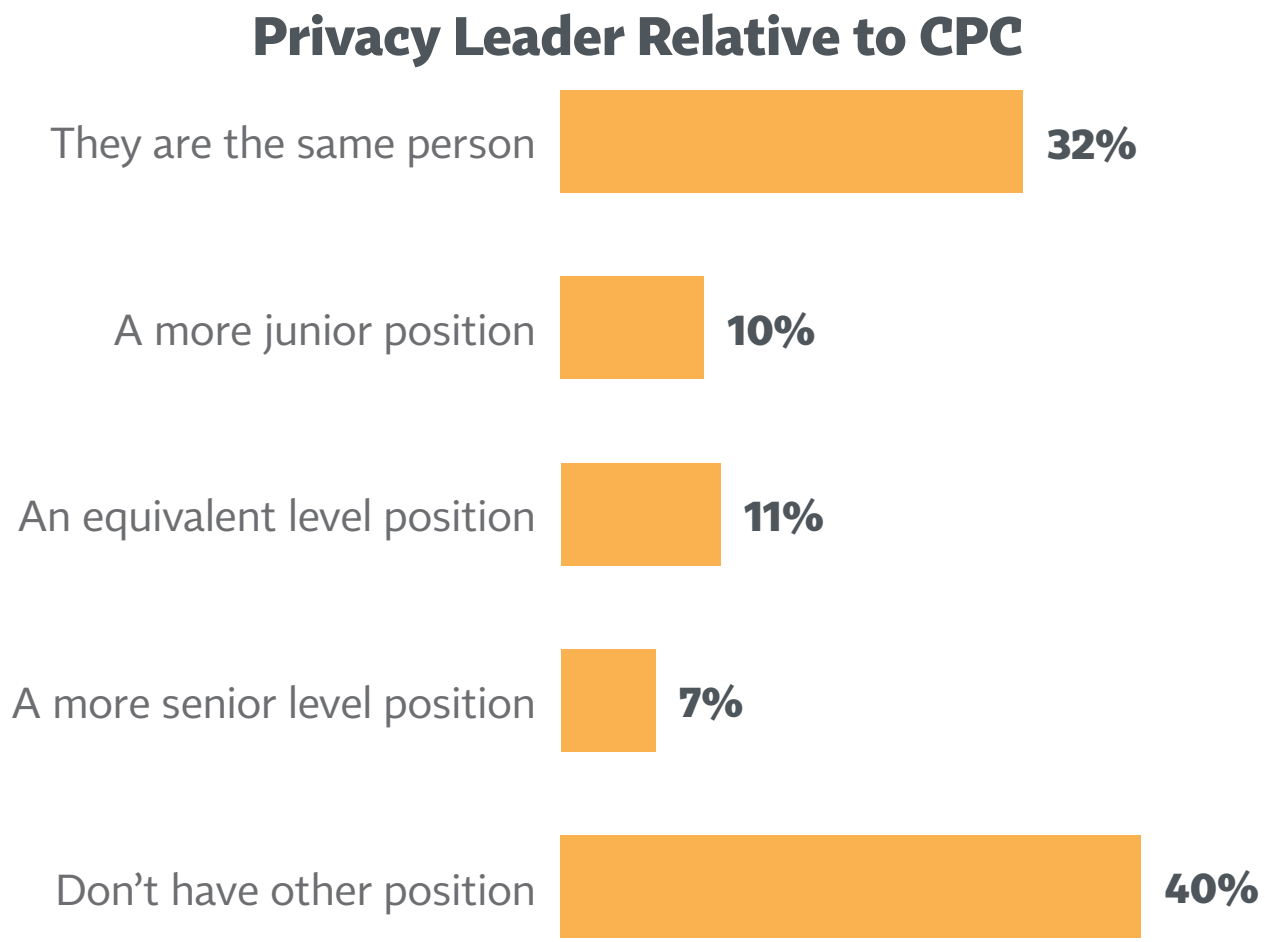
Responding: Director or Higher

BY GEOGRAPHY

	US	EU
Same Person	7%	9%
Junior to CISO	**28%**	15%
Equal to CISO	39%	38%
Senior to CISO	14%	17%
Don't have CISO	12%	21%

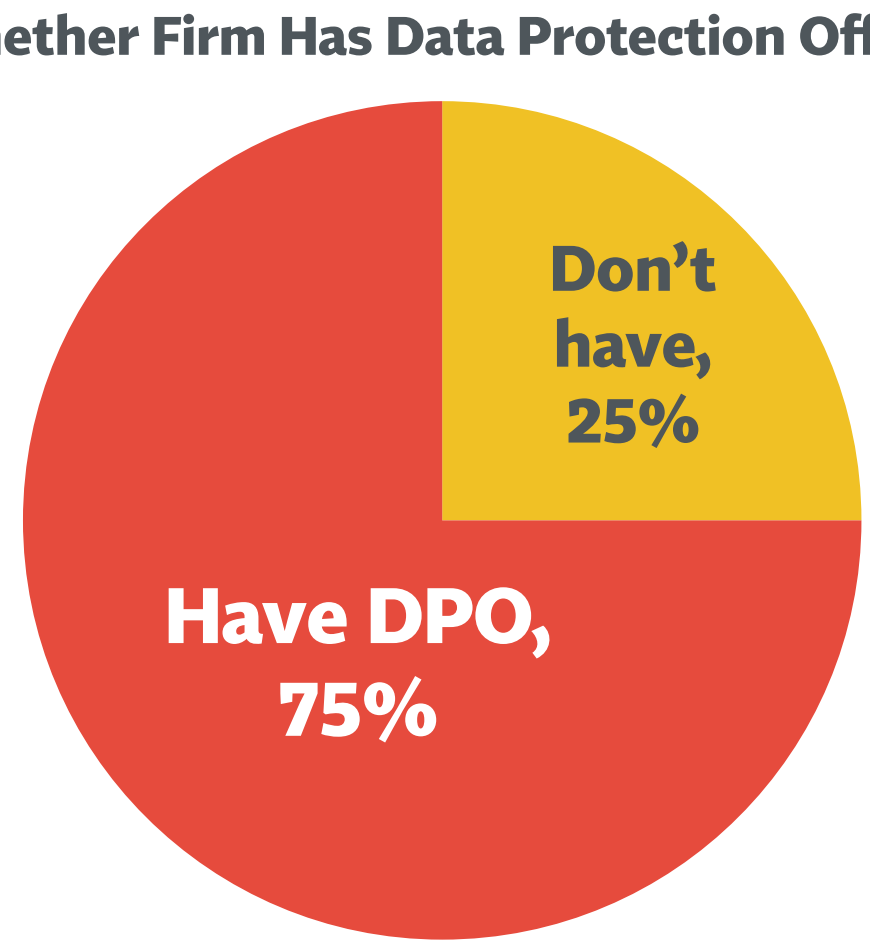
Significantly higher than total

More than a quarter of organizations split the Privacy Leader role out from the Chief Privacy Counsel



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

Further, 75% of firms now say they have appointed a Data Protection Officer

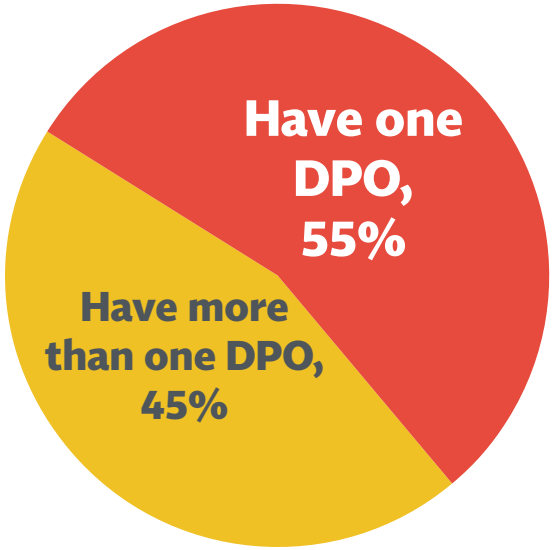


F28: How does the Privacy Leader compare with your company's data protection officer (DPO), if any? The Privacy Leader is …

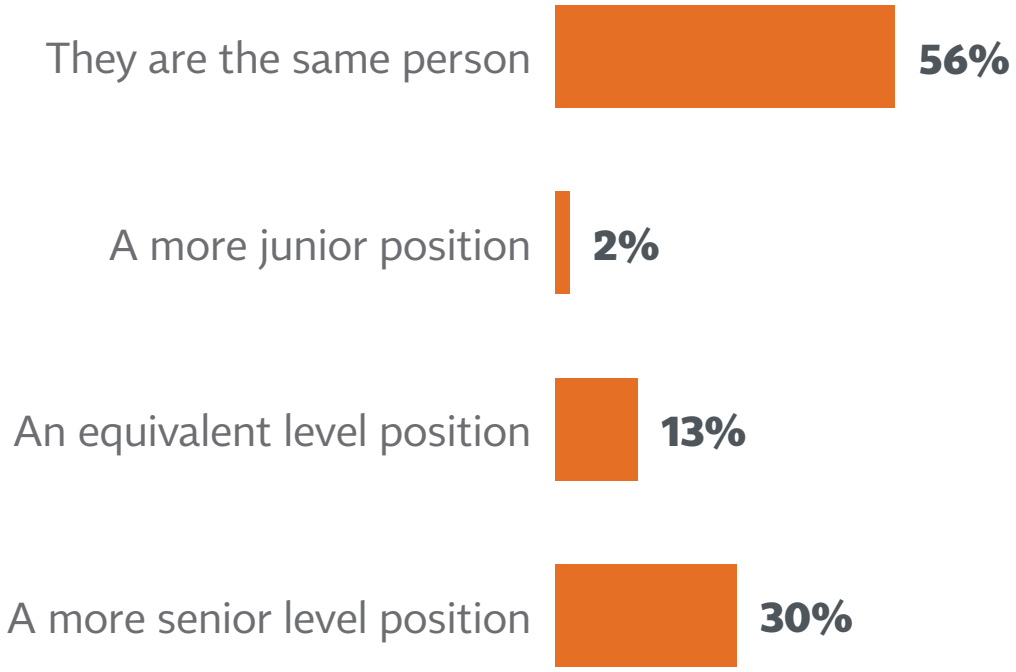
In fact, 45% of organizations have more than one Data Protection Officer

And 56% of Privacy Leaders serve as a Data Protection Officer, while 30% of DPOs sit under the Privacy Leader

Number of DPOs
Base: Director or higher, have DPO



Privacy Leader Relative to DPO
Base: Director or higher, have DPO



F30: Does your company have only one data protection officer 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 data protection officer (DPO), if any?

In the EU, the Privacy Leader tends to also be the DPO; in the US, the Privacy Leader is more senior

Privacy Leader vs. Data Protection Officer

Responding: Director or Higher, have DPO

BY GEOGRAPHY

	US	EU
Same Person	39%	**67%**
Junior to DPO	3%	3%
Equal to DPO	14%	14%
Senior to DPO	**45%**	16%

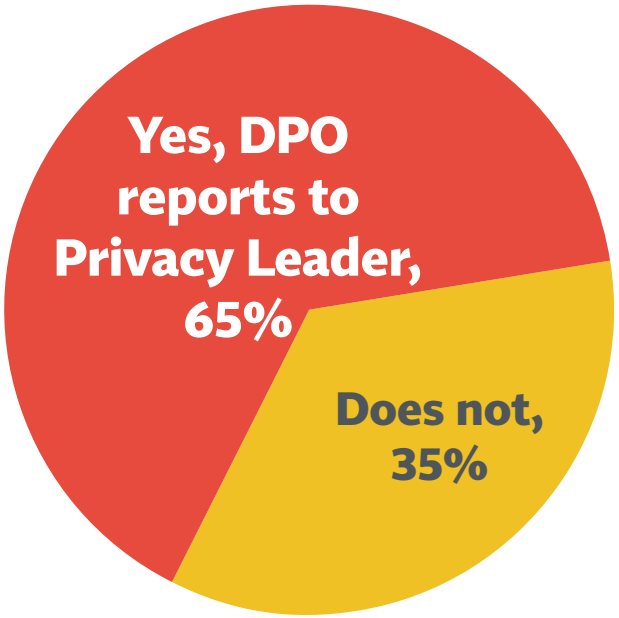
Significantly higher than total

Where the DPO and Privacy Lead are different, the DPO reports to the Privacy Leader 65% of the time

For those who don't report to the Privacy Leader, most report to someone in the firm's legal function

Whether DPO Reports to Privacy Leader

Base: Director or higher, DPO is not Privacy Leader



Other Levels DPO Reports To

(Among Those Reporting to More than Privacy Leader)

Most Common Responses (note: small sample size):

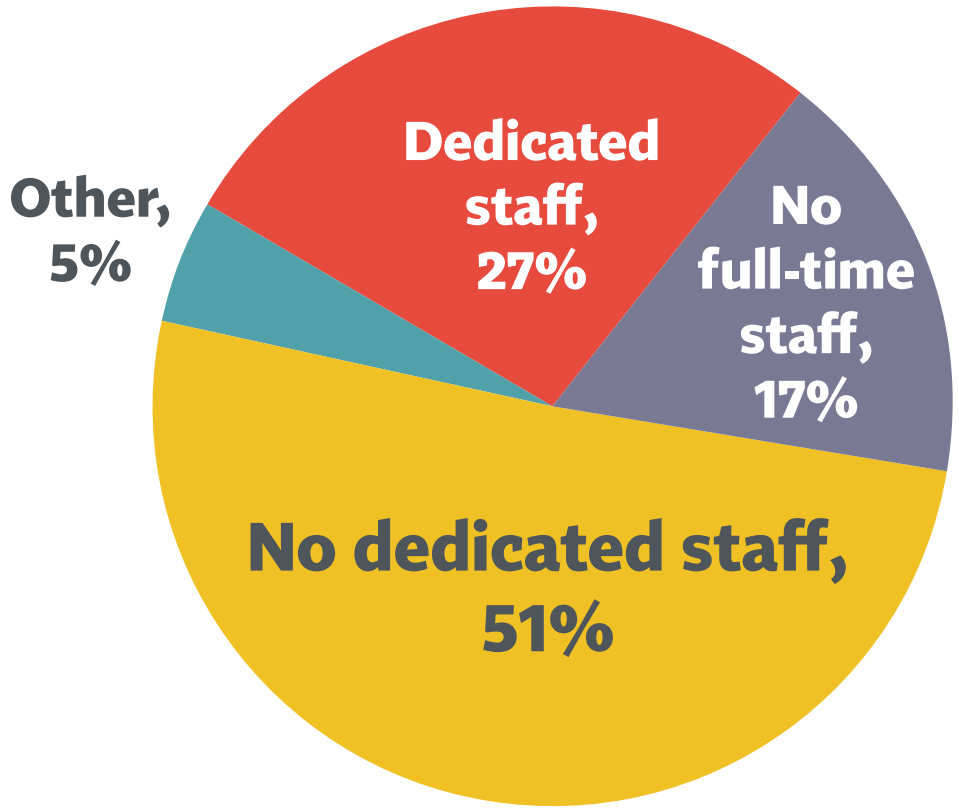
- General Counsel/Chief Legal Officer/Chief Privacy Counsel
- CEO
- CIO/CTO

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

Just 27% of DPOs have dedicated, full-time staff; half of organizations have no one reporting to the DPO

Whether DPO Has Dedicated Staff

Base: Director or higher, have DPO

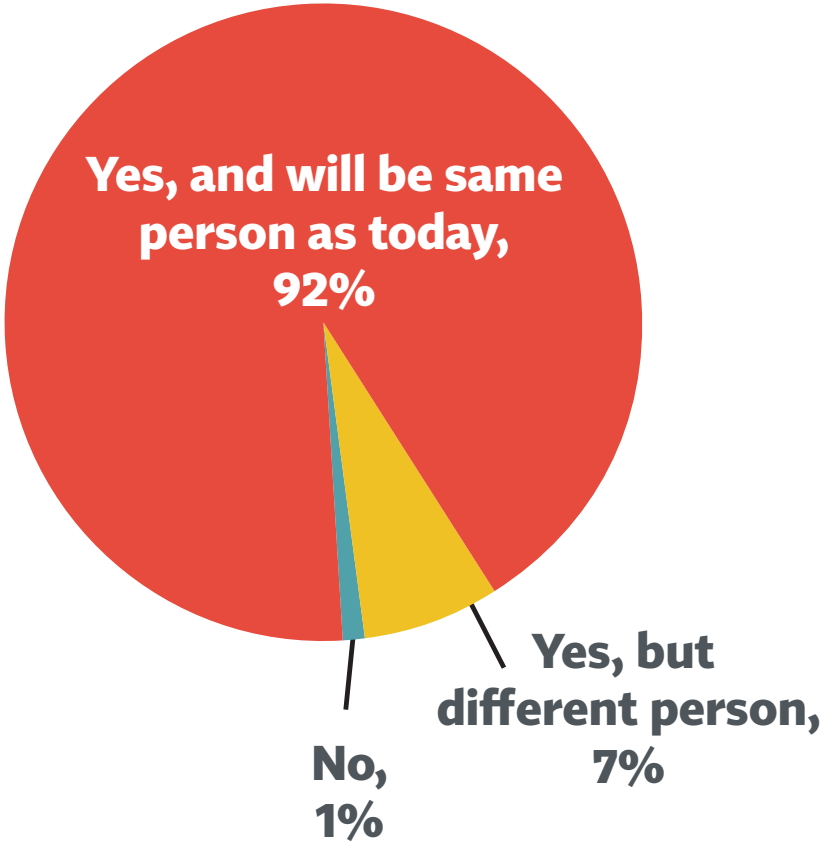


F34: Does your company have a separate, dedicated staff reporting to the data protection officer?

Nearly half of organizations say the DPO is more than just a compliance obligation

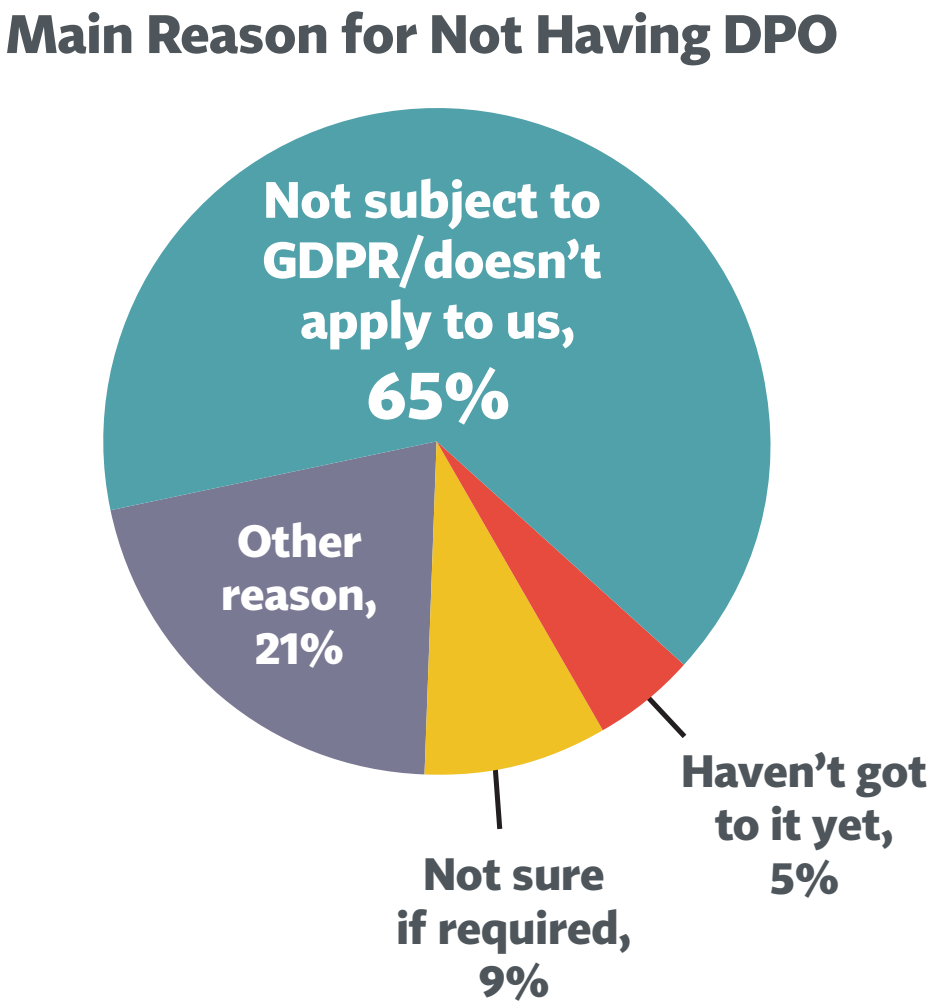
Main Reason for DPO

Will DPO Remain After GDPR?



F35: Which of the following best describes the MAIN reason why your company has a data protection officer?
F36: Once GDPR duties are completed in your company, will you continue to have a data protection officer?

For those without a DPO, the main reason, by far, is that GDPR does not apply to the firm



F37: What is the main reason you do not have a data protection officer in your company?

Privacy leaders are much more likely to report privacy matters to the board in the EU; tech is more likely to house Privacy in Information Security

Privacy Group Structure:

BY GEOGRAPHY

	US	EU
Privacy Leader is junior to the CISO	**28%**	18%
Privacy Leader reports to board	19%	**59%**
Privacy matters reported to board	68%	**93%**

BY INDUSTRY

	Average	Finance	Health*	Tech
Privacy team is in Compliance	19%	**39%**	**50%**	11%
Privacy team is in IS	11%	12%	14%	**33%**

Significantly higher than total

* Small sample size

Those in the EU and health care are most likely to have a DPO, and most likely to have DPO as Privacy Leader

DPO Characteristics:

	BY HQ LOCATION		BY INDUSTRY			
	US	EU	Average	Finance	Health*	Tech
Have DPO	67%	**89%**	75%	74%	**93%**	81%
AMONG THOSE WITH DPO:						
Has one DPO	59%	52%	55%	73%	46%	64%
Privacy Leader is DPO	43%	**67%**	56%	59%	**85%**	65%
DPO reports to Privacy Leader†	59%	**78%**	65%	61%	50%	60%
DPO has dedicated staff	19%	34%	44%	15%	48%	23%
Established DPO b/c required by law	51%	55%	52%	52%	49%	49%

Significantly higher than total * Small sample size

† Among organizations reporting DPO is not privacy leader

Large firms are more likely to have a DPO; small firms are more likely to have DPO who's also Privacy Leader

DPO Characteristics

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+*
Have DPO	66%	71%	76%	**100%**
AMONG THOSE WITH DPO:				
Has one DPO	**90%**	41%	8%	43%
Privacy Leader is DPO	**75%**	44%	38%	46%
DPO reports to Privacy Leader†	63%	33%	**88%**	76%
DPO has dedicated staff	20%	41%	31%	25%
Established DPO b/c required by law	48%	52%	46%	61%

Significantly higher than total * Small sample size

† Among organizations reporting DPO is not privacy leader

This holds true when we look at size by revenue as well

DPO Characteristics:

BY COMPANY REVENUE

	Under $100 million	$100–$999 million	$1–$24 billion	$25 billion or more*
Have DPO	69%	61%	80%	**91%**
AMONG THOSE WITH DPO:				
Has one DPO	**85%**	**89%**	42%	31%
Privacy Leader is DPO	**78%**	**79%**	39%	33%
DPO reports to Privacy Leader†	63%	75%	63%	74%
DPO has dedicated staff	24%	23%	33%	32%
Established DPO b/c required by law	43%	44%	60%	51%

Significantly higher than total * Small sample size

† Among organizations reporting DPO is not privacy leader

Further, while mature firms are more likely to have a DPO, they are less likely to appoint the Privacy Leader as DPO

DPO Characteristics:

BY MATURITY

	Early/Middle Maturity	Mature
Have DPO	71%	83%
AMONG THOSE WITH DPO:		
Has one DPO	53%	59%
Privacy Leader is DPO	61%	46%
DPO reports to Privacy Leader†	69%	60%
DPO has dedicated staff	26%	28%
Established DPO b/c required by law	57%	41%

Significantly higher than total * Small sample size

† Among organizations reporting DPO is not privacy leader

When the Privacy Leader does serve as DPO, they are more likely to have staff, work outside the U.S., and report to the Board

DPO Characteristics:

BY DPO STATUS

	Privacy Leader Is Also DPO	Privacy Leader Is Not DPO
Has dedicated staff	**37%**	14%
Has CIPP/E	**55%**	33%
Works in non-U.S. firm	**61%**	27%
Privacy structure changed due to GDPR	**57%**	27%
Privacy matters reported to board	**92%**	70%
Privacy Leader reports to board	**51%**	20%

Significantly higher than total

* Small sample size

Contents

The number of professionals working full-time in privacy programs has increased since last year

The mean, however, is pulled significantly higher than the median by large programs at the top end of the scale

Employees Dedicated to Privacy

	2018		2017	
	Mean	Median	Mean	Median
Full-time privacy, in privacy program	10.0	2	6.8	2
Full time privacy, in internal service centers	3.5	0	5.2	0
Full time privacy, in revenue based business units	4.0	0		
Part time privacy, in privacy program	4.6	1	6.7	1
Part time privacy, in internal service centers	6.2	2	15.6	3
Part time privacy, in revenue based business units	7.6	1		

NOTES: Outliers over 999 removed.
Before 2018, employees in internal service centers and revenue based business units were combined.

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

As one would expect, privacy program staff is larger in companies with the most employees

Mean Privacy Staff By Company Employees

	<5K	5–24.9K	25–74.9K	75K+*
Full-time privacy, in privacy program	3.8	6.6	6.3	**35.1**
Full time privacy, in internal service centers	1.5	3.1	1.1	11.6
Full time privacy, in revenue based business units	2.1	12.2	0.9	1.0
Part time privacy, in privacy program	1.7	7.8	7.6	5.2
Part time privacy, in internal service centers	2.4	5.9	4.0	20.2
Part time privacy, in revenue based business units	1.7	5.2	4.4	**32.2**

Significantly higher than total

* Small sample size

NOTE: Outliers over 999 removed.

However, the median shows the differences aren't always so large, and there is a wide distribution of staff sizes at the higher levels

Median Privacy Staff By Company Employees

	<5K	5–24.9K	25–74.9K	75K+*
Full-time privacy, in privacy program	1.0	2.0	5.0	**15.0**
Full time privacy, in internal service centers	0.0	0.0	0.0	0.0
Full time privacy, in revenue based business units	0.0	0.0	0.0	0.0
Part time privacy, in privacy program	1.0	1.0	3.0	0.0
Part time privacy, in internal service centers	1.0	2.0	3.0	**10.0**
Part time privacy, in revenue based business units	0.0	0.5	1.0	**10.0**

Significantly higher than total * Small sample size

NOTE: Outliers over 999 removed.

Privacy staffs are also largest in firms with the highest levels of revenue

Mean Privacy Staff By Company Revenue

	Under $100 million	$100–$999 million	$1–$24 billion	$25 billion or more*
Full-time privacy, in privacy program	5.7	0.9	6.6	**47.0**
Full time privacy, in internal service centers	2.1	0.8	2.2	16.2
Full time privacy, in revenue based business units	1.7	3.5	7.4	1.4
Part time privacy, in privacy program	1.4	1.3	7.5	9.3
Part time privacy, in internal service centers	1.9	2.2	9.6	12.2
Part time privacy, in revenue based business units	1.7	2.0	10.4	8.3

Significantly higher than total * Small sample size

NOTE: Outliers over 999 removed.

Traditionally unregulated and B2B firms have by far more privacy professionals than other types of firms

Mean Privacy Staffing

	INDUSTRY			CUSTOMER TARGET		
	Regulated	Unregulated	Gov't*	B2B	B2C	Both
Full-time privacy, in privacy program	3.8	**14.1**	1.2	**14.0**	2.5	7.2
Full time privacy, in internal service centers	1.2	4.8	0.9	5.1	0.8	2.2
Full time privacy, in revenue based business units	1.1	2.2	0.0	6.8	0.0	1.7
Part time privacy, in privacy program	6.1	4.7	0.9	3.5	8.8	4.7
Part time privacy, in internal service centers	4.8	7.7	2.3	6.1	2.5	7.2
Part time privacy, in revenue based business units	11.1	8.0	0.5	8.6	2.3	7.9

Significantly higher than total

* Small sample size

NOTE: Outliers over 999 removed.

US-based firms have more full-time privacy employees, while EU-based firms have more part-time staff

Mean Privacy Staff Size by Location

BY HQ LOCATION

	US	EU
Full-time privacy, in privacy program	12.7	2.0
Full time privacy, in internal service centers	4.7	2.2
Full time privacy, in revenue based business units	5.9	1.9
Part time privacy, in privacy program	3.5	6.6
Part time privacy, in internal service centers	3.7	10.3
Part time privacy, in revenue based business units	2.8	15.5

NOTE: Outliers over 999 removed.

However, median numbers show both sides of the Atlantic have wide variations and that average numbers are pulled higher by a small number of big staffs

Median Privacy Staff by Geography

	US	EU
Full-time privacy, in privacy program	2.0	2.0
Full time privacy, in internal service centers	0.0	0.0
Full time privacy, in revenue based business units	0.0	0.0
Part time privacy, in privacy program	1.0	1.0
Part time privacy, in internal service centers	2.0	2.0
Part time privacy, in revenue based business units	1.0	1.0

NOTE: Outliers over 999 removed.

Respondents are much more likely to say privacy staff will increase, full- and part-time, than in 2017

Expected Employee Change in Coming Year

	% Saying Increase		% Saying Decrease		% Saying Stay the Same		Net % Change	
	2018	2017	2018	2017	2018	2017	2018	2017
Full-time privacy, in privacy program	41%	28%	1%	4%	58%	68%	+17%	+13%
Full time privacy, in internal service centers	14%	18%	1%	2%	84%	80%	+7%	+5%
Full time privacy, in revenue based business units	12%		0%		87%		+5%	
Part time privacy, in privacy program	24%	13%	2%	3%	74%	84%	+11%	+6%
Part time privacy, in internal service centers	28%	38%	3%	3%	70%	59%	+11%	+12%
Part time privacy, in revenue based business units	25%		3%		72%		+9%	

NOTES: Outliers over 999 removed.
Before 2018, employees in internal service centers and revenue based business units were combined

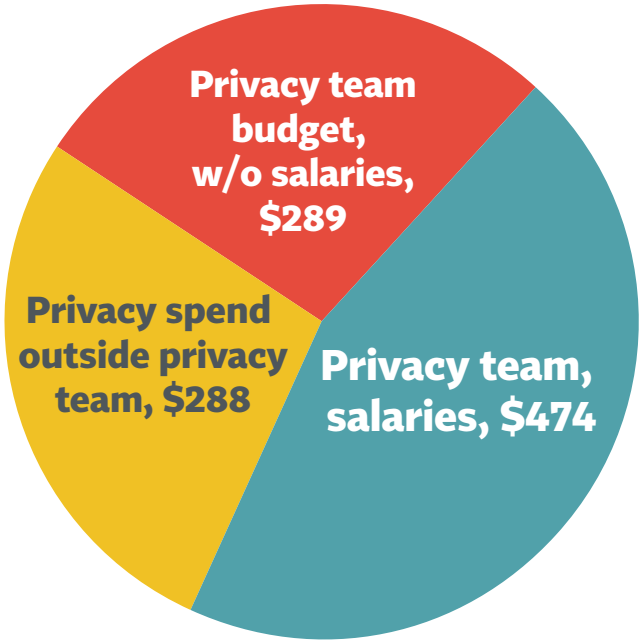
F2: In the coming year, do you expect the number of employees in each of these categories to increase, decrease, or stay the same? If increase or decrease, please enter your estimate of the percentage change you expect.

In the aftermath of the GDPR implementation date, mean privacy spend has dropped since last year

- Mean spend has gone from $2.1 million in 2017 to $1.0 million in 2018, driven by cuts to the biggest organizations' budgets as a result of the conclusion of GDPR compliance projects
- However, spending per employee has only declined $7 since last year

TOTAL PRIVACY SPEND
2018 MEAN: 1.0M 2017 MEAN: $2.1M 2018 MEDIAN: $400,000 2017 MEDIAN: $571,500
Mean spending per employee: 2018: $140 2017: $147

Estimated Privacy Spend (000)



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

Total privacy spending is highest in the largest firms; spending *per employee* is highest in the smallest firms

Estimated Privacy Spend

BY EMPLOYEE SIZE

	Under 5K	5–24.9K	25–74.9K	75K+*
Privacy Team Budget, w/o Salaries (000)	$174.4	$235.4	$309.5	$645.7
Privacy Team Salaries (000)	$167.9	$517.0	$688.4	$1,026.8
Spend Outside Privacy Team (000)	$123.4	$561.0	$180.9	$480.8
Total Privacy Spend (000)	$465.7	$1,292.0	$1,178.7	$2,153.4
Privacy Spend per Employee	**$305**	$122	$25	$15

Significantly higher than total

* Small sample size

A similar dynamic holds when firm size is defined by revenue: higher per-employee spending in smaller firms

Estimated Privacy Spend

BY COMPANY REVENUE

	Under $100 million*	$100–$999 million*	$1–$24 billion	$25 billion or more*
Privacy Team Budget, w/o Salaries (000)	$134.7	$295.5	$428.7	$291.6
Privacy Team Salaries (000)	$184.3	$195.5	$698.7	$769.1
Spend Outside Privacy Team (000)	$100.4	$216.0	$509.4	$117.1
Total Privacy Spend (000)	$419.4	$707.0	$1,636.8	$1,112.5
Privacy Spend per Employee	**$254**	**$264**	$120	$7

Significantly higher than total

* Small sample size

In 2018, total privacy spending is directionally highest in traditionally unregulated and B2B/B2C firms

Estimated Privacy Spend

	BY INDUSTRY CATEGORY			BY CUSTOMER TARGET		
	Regulated	Unregulated	Gov't.*	B2B	B2C	Both
Privacy Team Budget, w/o Salaries	$195.2	$370.3	$22.7	$282.4	$39.0	$367.6
Privacy Team Salaries	$432.6	$537.8	$242.9	$458.0	$330.8	$532.8
Spend Outside Privacy Team	$377.1	$291.3	$159.5	$270.6	$478.6	$256.4
Total Privacy Spend (Mean)	$1,004.8	$1,189.7	$425.1	$1,010.9	$848.4	$1,141.0
Privacy Spend per Employee	$138	$132	$132	$147	$209	$115

* Small sample size

Overall privacy spending is somewhat higher for organizations headquartered in the EU than for those in the US

Estimated Privacy Spend
Base: Director or Higher

	US	EU
Mean spending on privacy (000)	$850.0	$1,445.0
Mean spending on privacy per employee	$114.0	$182.0

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

When broken out by company size, it's clear the drop in spending is driven by cuts at the largest firms

This suggests a greater effort at larger companies to come into GDPR compliance and now a resetting of budget needs going forward

Estimated Privacy Spend

	Under 5K		5–24.9K		25–74.9K		75K+*	
	2018	2017	2018	2017	2018	2017	2018	2017
Privacy Team Budget, w/o Salaries (000)	$174.4	$142.5	$235.4	$176.6	$309.5	$1,260.5	$645.7	$1,586.8
Privacy Team Salaries (000)	$167.9	$266.6	$517.0	$427.9	$114.0	$1,024.6	$1,026.8	$2,700.6
Spend Outside Privacy Team (000)	$123.4	$245.8	$561.0	$135.9	$114.0	$494.2	$480.8	$2,927.3
Total Privacy Spend (000)	$465.7	$654.9	$1,292	$740.4	$114.0	$2,779.3	$2,153.4	$7,214.8
Privacy Spend per Employee	$305	$312	$122	$80	$114	$72	$15	$49

* Small sample size

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

The drop in budget is even more stark when we look at company size by revenue

Estimated Privacy Spend

	Under $100 million*		$100–$999 million*		$1–$24 billion		$25 billion or more*	
	2018	2017	2018	2017	2018	2017	2018	2017
Privacy Team Budget, w/o Salaries (000)	$134.6	$226.2	$295.5	$128.2	$428.7	$676.1	$291.6	$1,527.4
Privacy Team Salaries (000)	$184.4	$224.3	$195.5	$259.3	$698.7	$768.5	$769.5	$2,507.6
Spend Outside Privacy Team (000)	$100.4	$90.1	$216.0	$46.7	$509.4	$633.3	$633.3	$2,307.2
Total Privacy Spend (000)	$419.4	$540.6	$707.0	$434.2	$1,636.8	$2,077.9	$2,077.9	$6,342.2
Privacy Spend per Employee	$254.0	$312.0	$264.0	$221.0	$120.0	$95.0	$7.0	$84.0

* Small sample size

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

Privacy staffing jumps dramatically once firms reach $1 million in privacy budget

Mean Privacy Employee Size
Base: Director or Higher

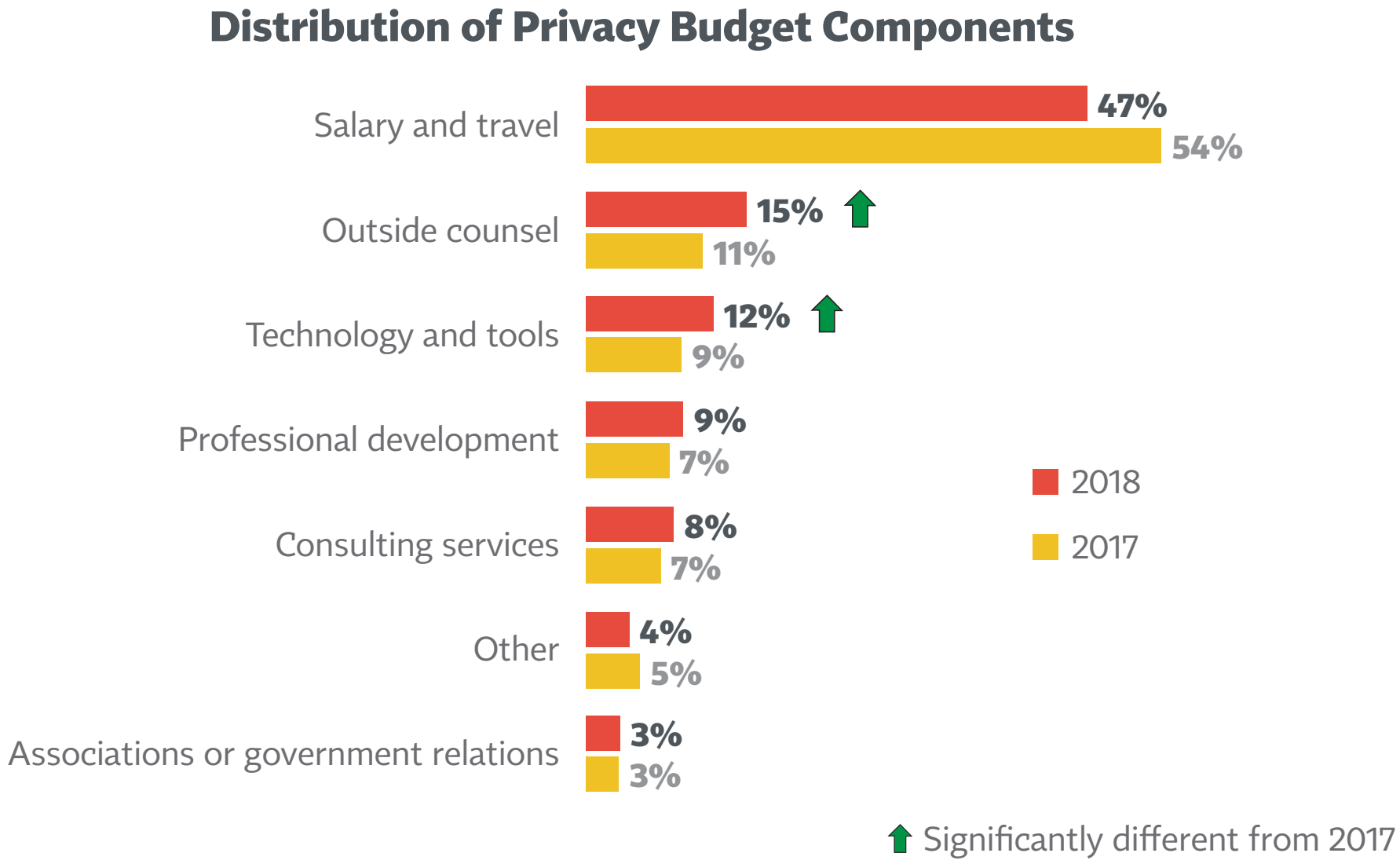
BY PRIVACY BUDGET (Excluding Salaries)

	$1-$100K	$101K-$1M	More than $1M*
Full-time privacy, in privacy program	6.2	6.3	16.7
Full time privacy, in internal service centers	0.8	2.1	4.0
Full time privacy, in revenue based business units	1.5	1.8	1.4
Part time privacy, in privacy program	1.7	7.5	10.1
Part time privacy, in internal service centers	3.1	8.2	17.3
Part time privacy, in revenue based business units	2.4	15.7	13.4

NOTE: Outliers over 999 removed.

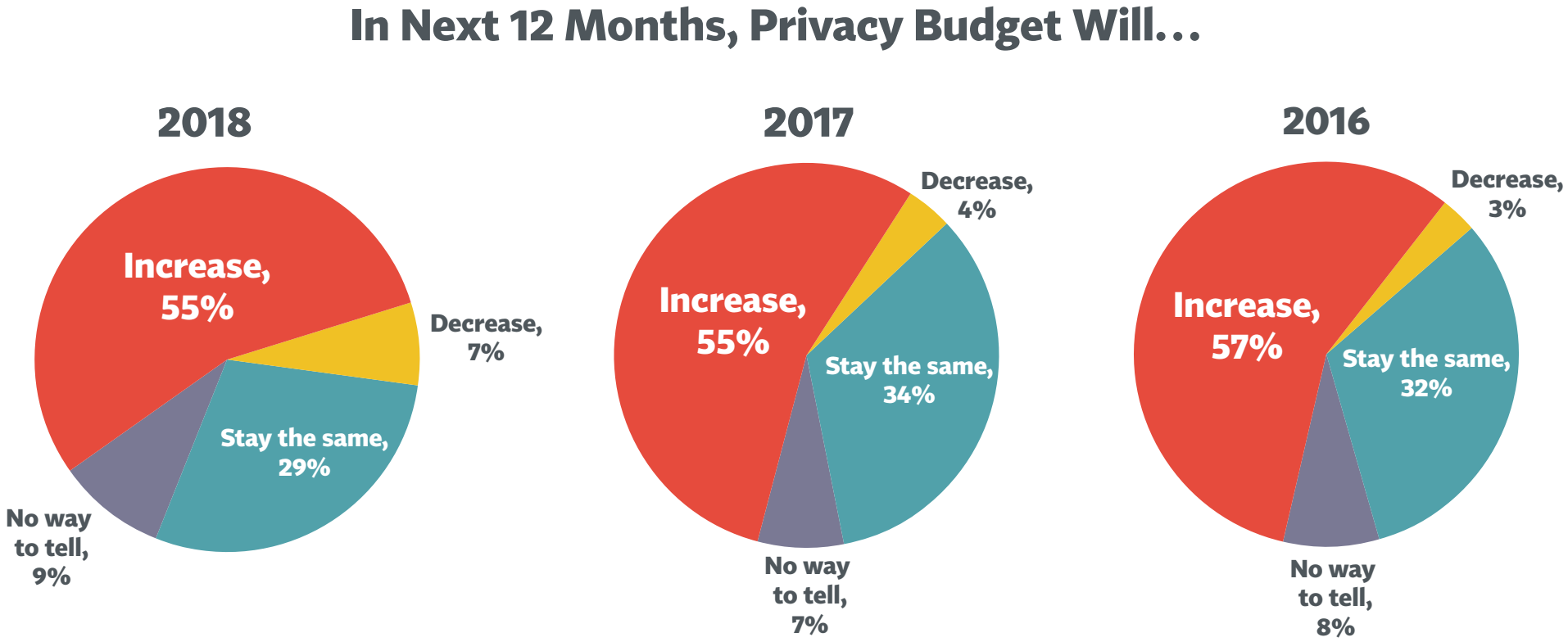
* Small sample size

Compared to 2017, a greater share of privacy spending today goes to outside counsel and technology



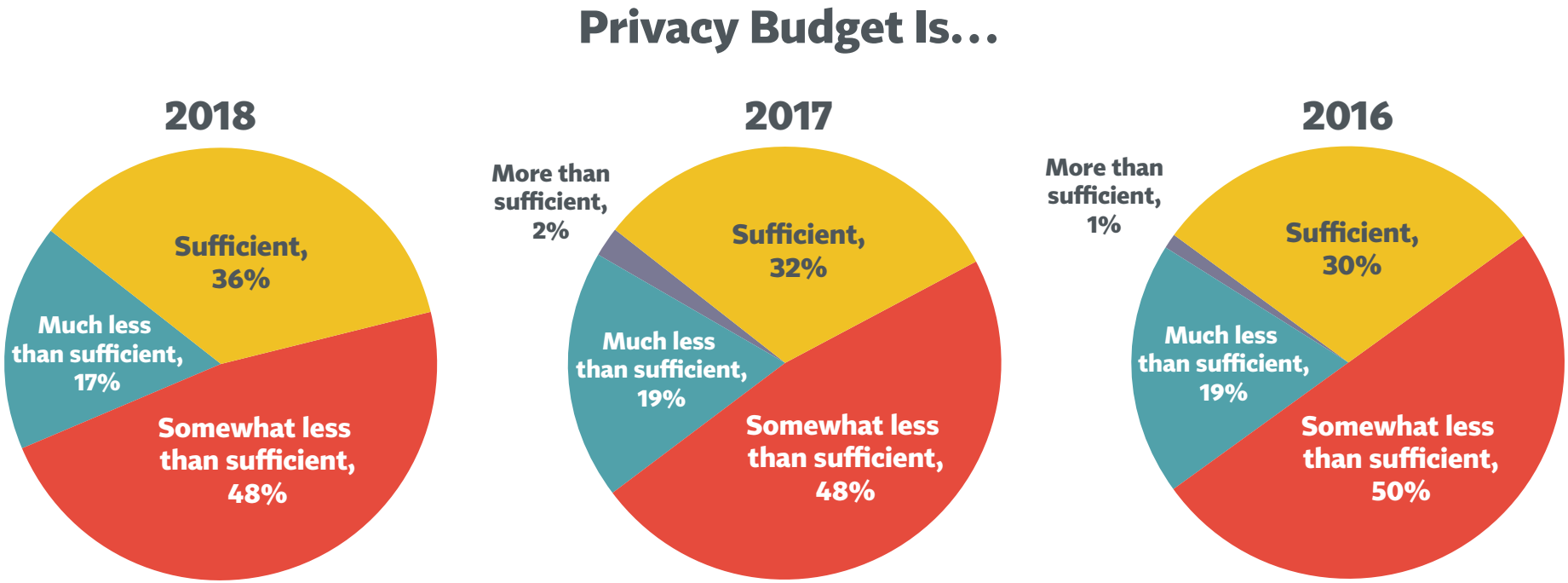
F3: What percent of your company's total privacy budget is allocated to each of the following components?

Despite the drop since last year, there's been no change in those saying spending will increase next year



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

There's also been little change in perceptions of budget sufficiency: 65% feel their budget is not enough



NET LESS THAN SUFFICIENT
2018: 65%
2017: 67%
2016: 69%

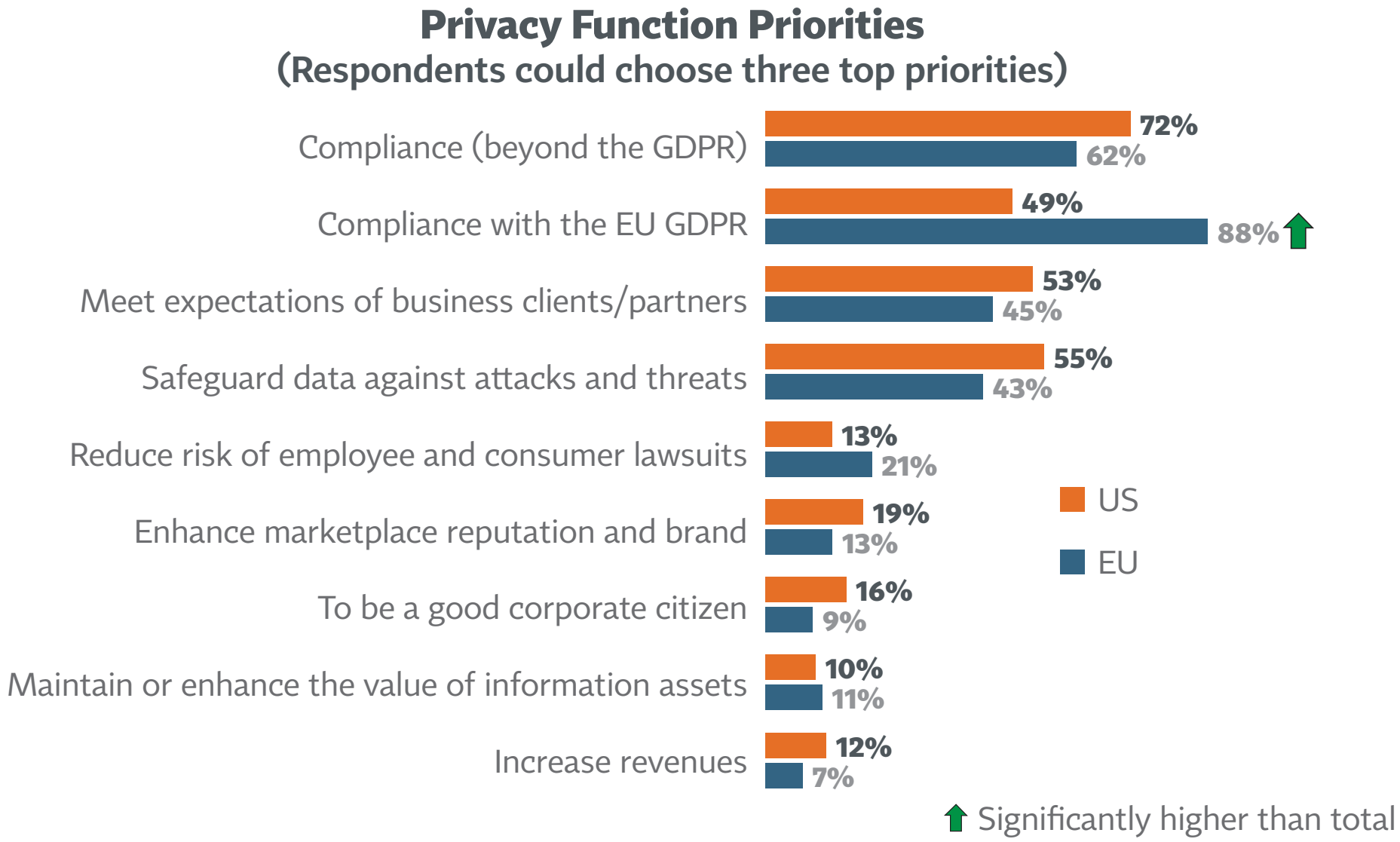
F6: In your opinion, your company's privacy budget is …to meet your privacy obligations

Contents

Privacy programs this year prioritized GDPR compliance above all else

E3: Please rank the following in terms of their priority for your company's privacy program.
NOTE: Question asked differently in 2018 vs. prior years.

Unsurprisingly, compliance with GDPR is much more likely to be a top priority in the EU

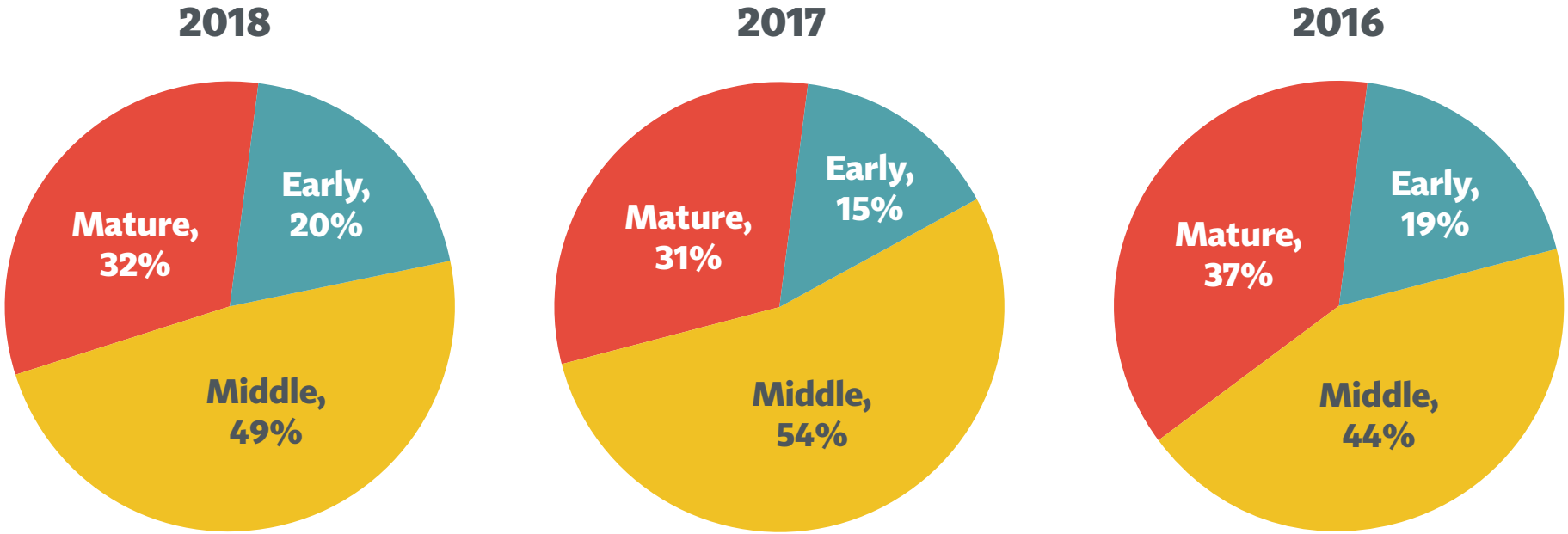


E3: Please rank the following in terms of their priority for your company's privacy program.
NOTE: Question asked differently in 2018 vs. prior years.

The GDPR has brought many new programs into existence, resulting in younger privacy programs on average

Privacy Function Lifecycle Stage

(Respondents were asked to self-evaluate the maturity of their programs)



YEARS WITH PRIVACY (MEAN)	2018: 5.0 2017: 6.4 2016: 6.5

E1: Please select the maturity stage of your company's privacy program.
E2: For how many years has your company had a dedicated privacy program?

Maturity is most strongly correlated with employee size; bigger companies have been doing privacy longer

Privacy Maturity Stage

BY EMPLOYEE SIZE

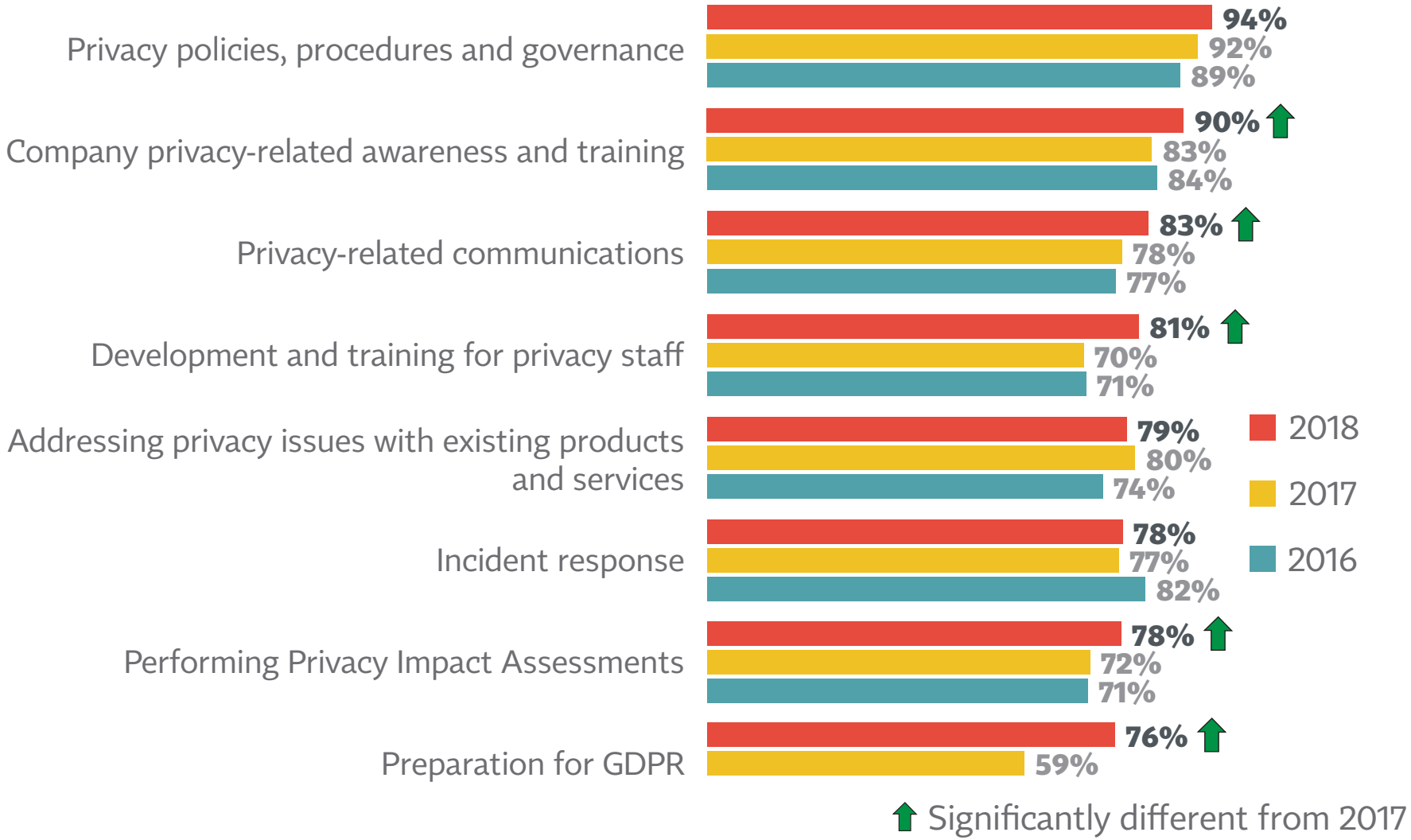
	Under 5K	5–24.9K	25–74.9K	75K+
Early	**29%**	24%	6%	3%
Middle	47%	53%	59%	40%
Mature	24%	24%	35%	**57%**

Significantly higher than total

In addition, we see increases in privacy's involvement across a range of "top" responsibilities

Top Privacy Team Responsibilities

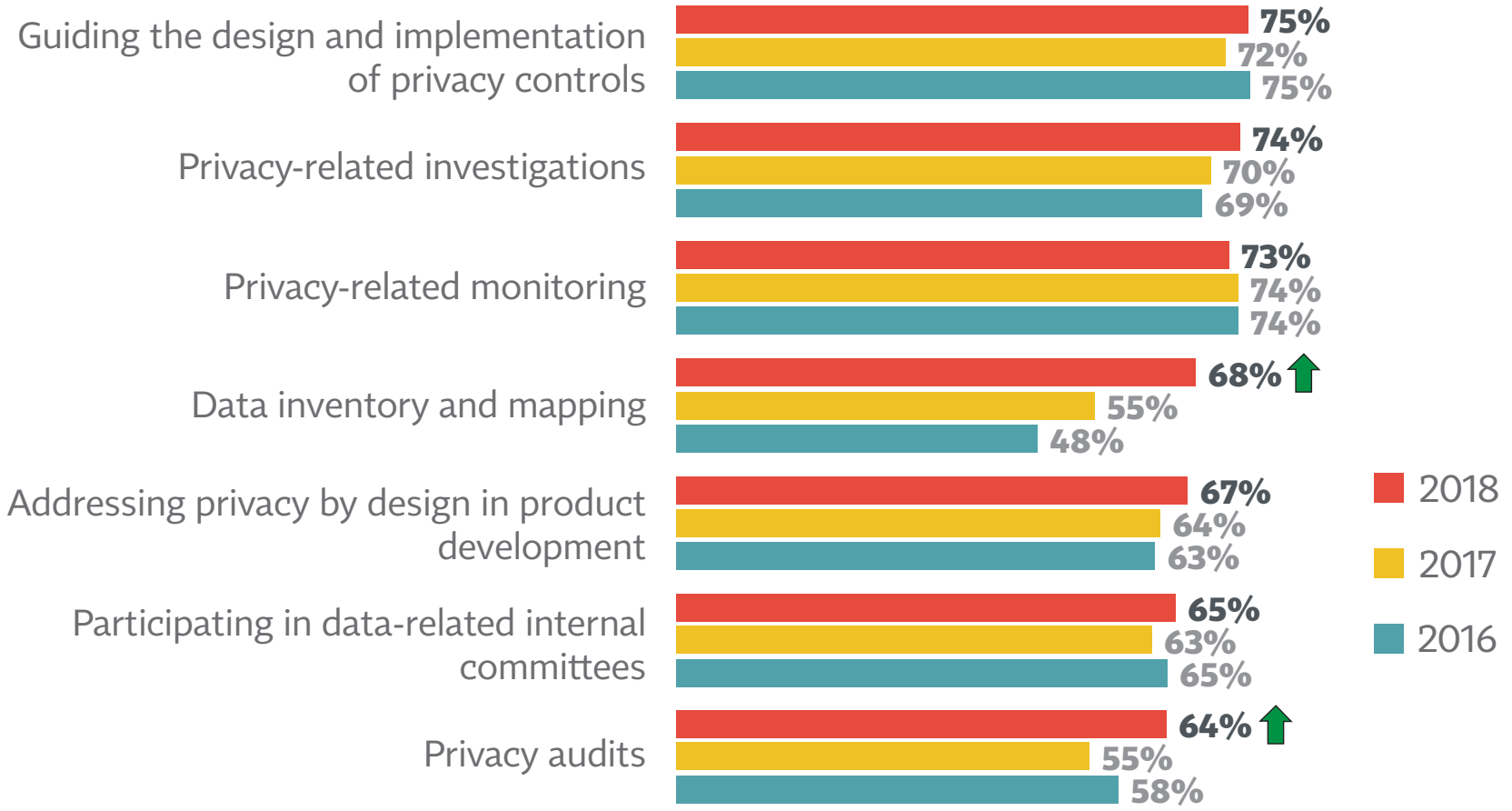
(Respondents could choose as many as they liked)



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

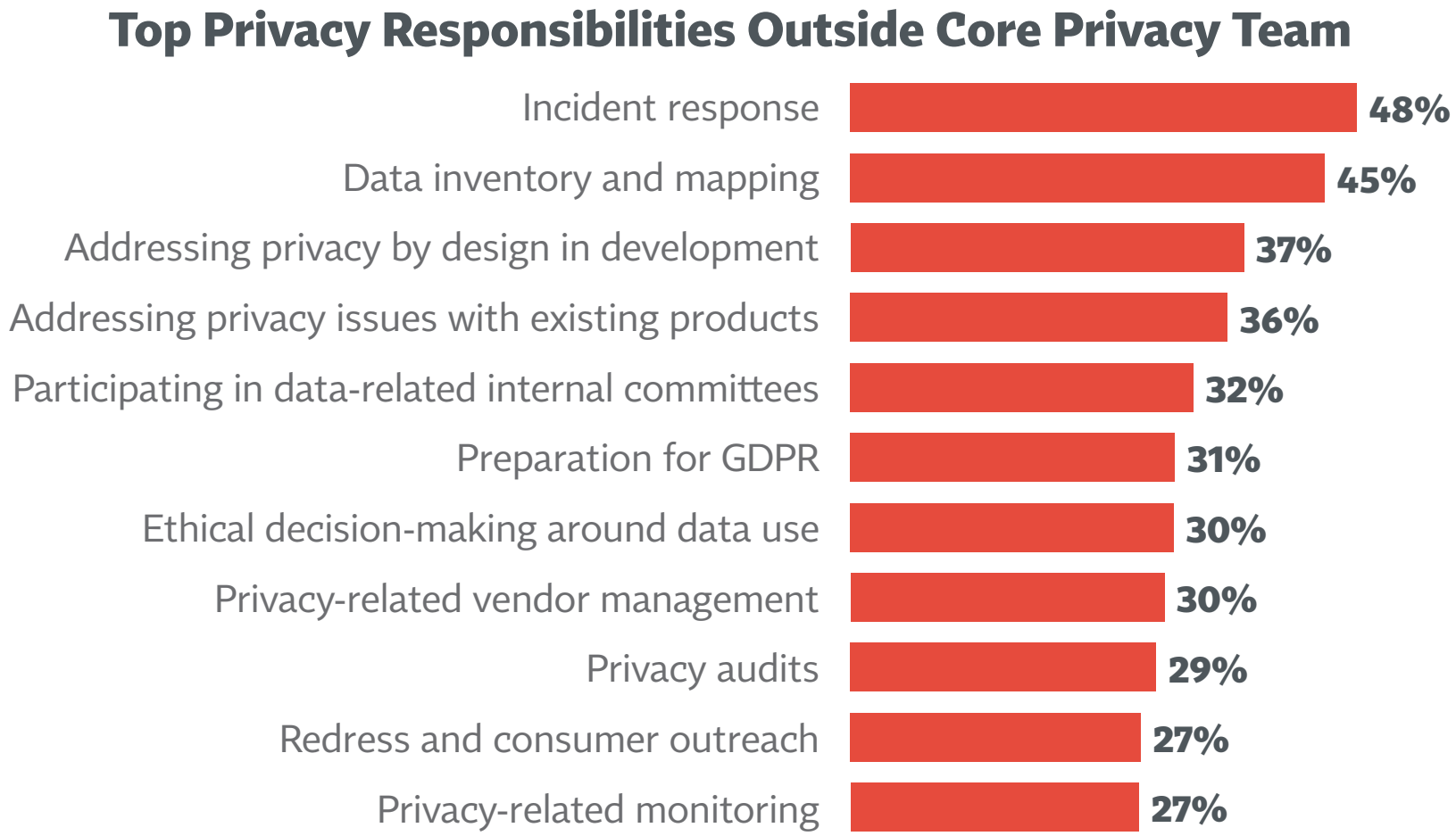
We're also seeing increases in privacy teams doing data mapping and privacy audits

Top Privacy Team Responsibilities
(Respondents could choose as many as they liked)



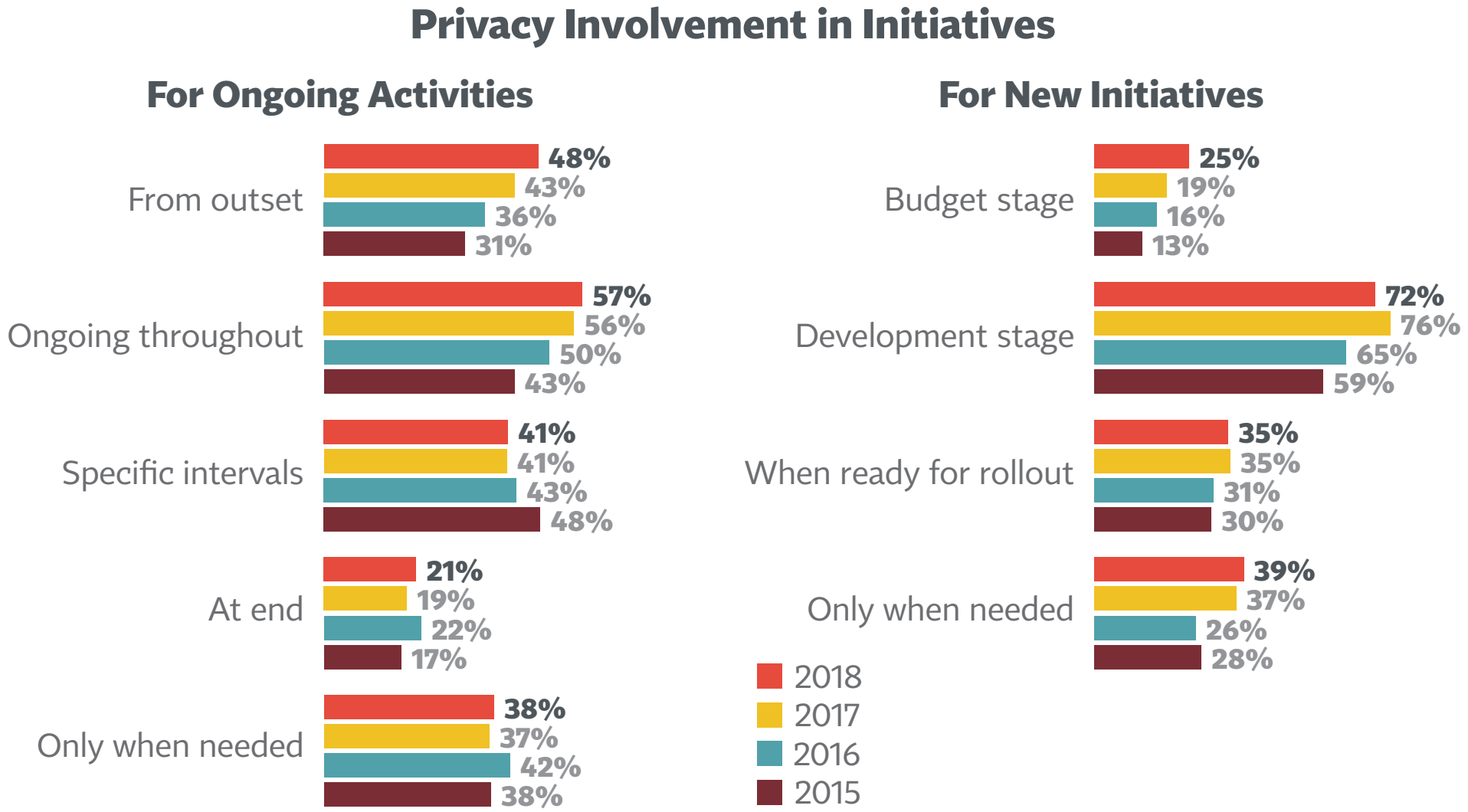
D4: Which of the following is your team responsible for accomplishing on an annual basis?

The top privacy responsibilities for those working outside the privacy team tend to be technical



D4: 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?

Privacy by design is increasingly taking hold; privacy is involved ever earlier in new products and services



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 …

Tech firms tend to get privacy involved earliest and most often

Privacy Involvement in Products and Services

BY INDUSTRY

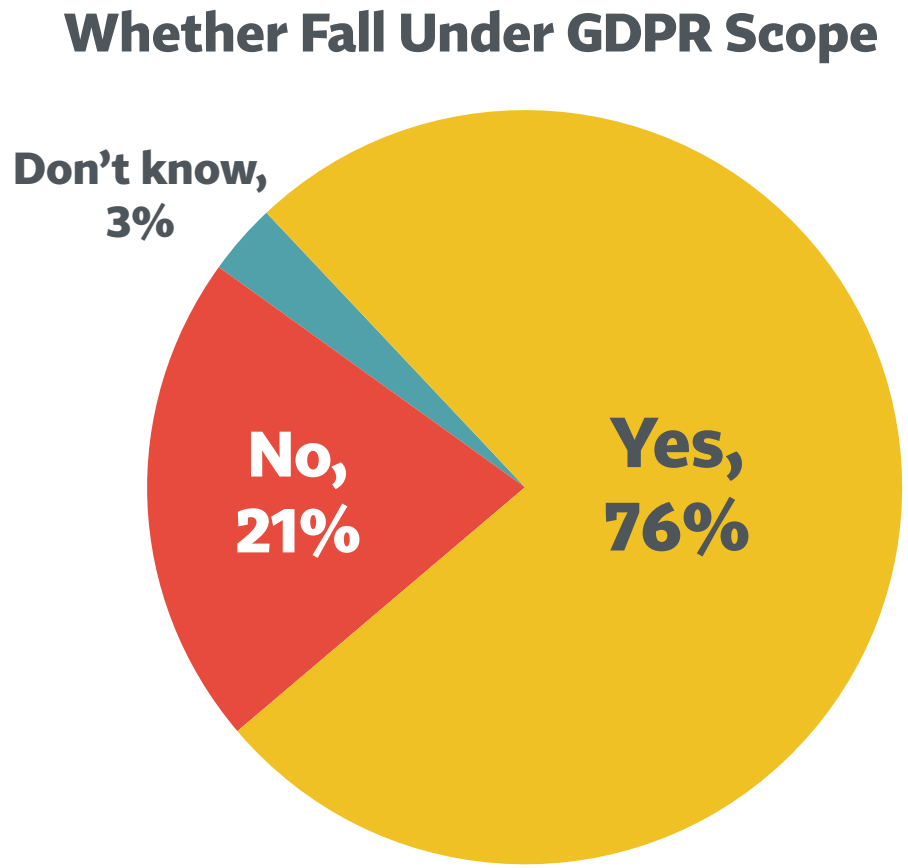
	Average	Finance	Health*	Tech
Ongoing activities: Involved on ongoing basis	57%	52%	64%	**69%**
New initiatives involvement: At budget stage	25%	12%	17%	**33%**
New initiatives involvement: At development stage	72%	**80%**	73%	**80%**
Ongoing activities: Involved only when needed	38%	35%	39%	32%

Significantly higher than total

* Small sample size

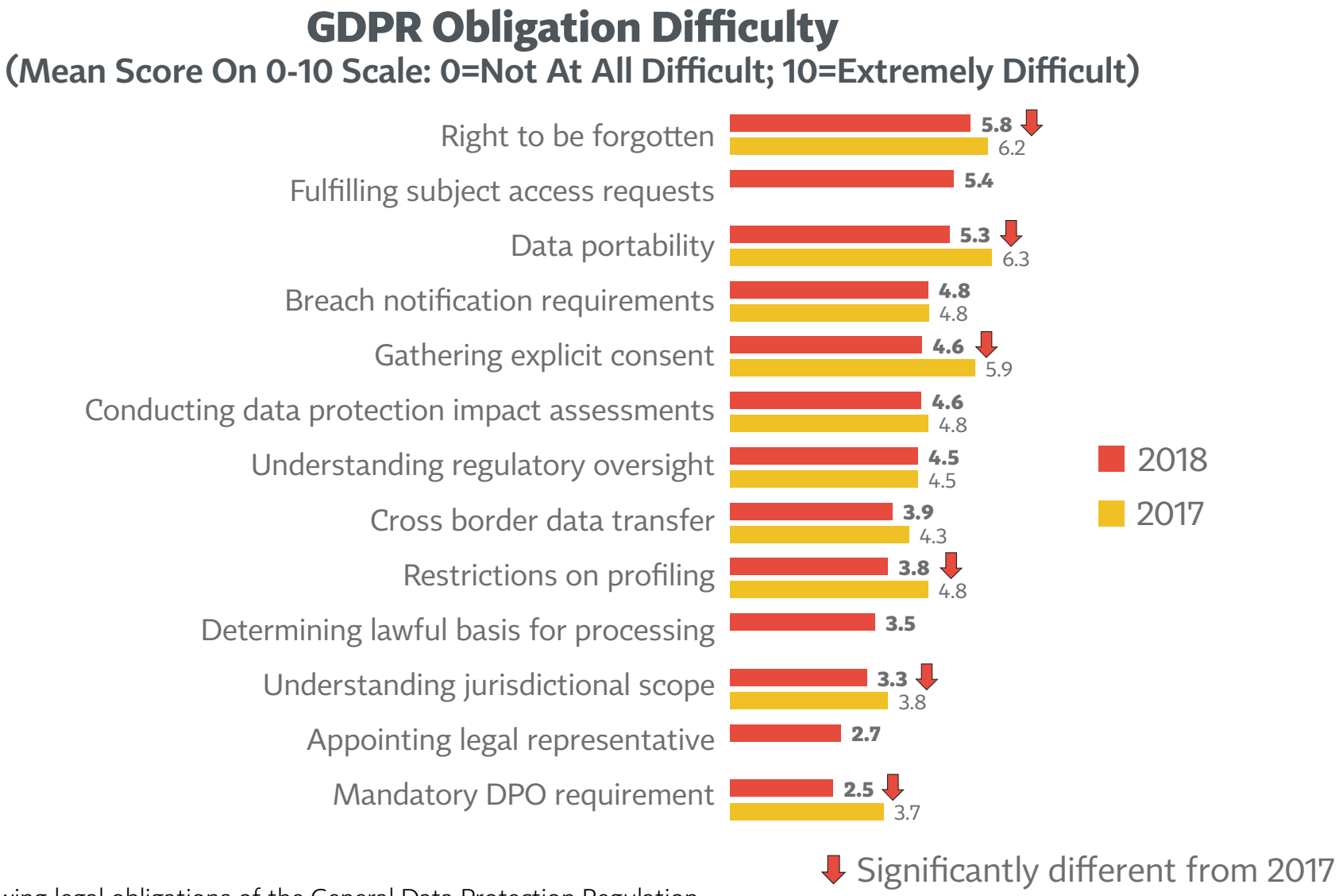
Contents

Just over three quarters of our sample organizations say they fall within the GDPR's scope



J5: Do you feel your company falls under the jurisdiction of the EU's General Data Protection Regulation?

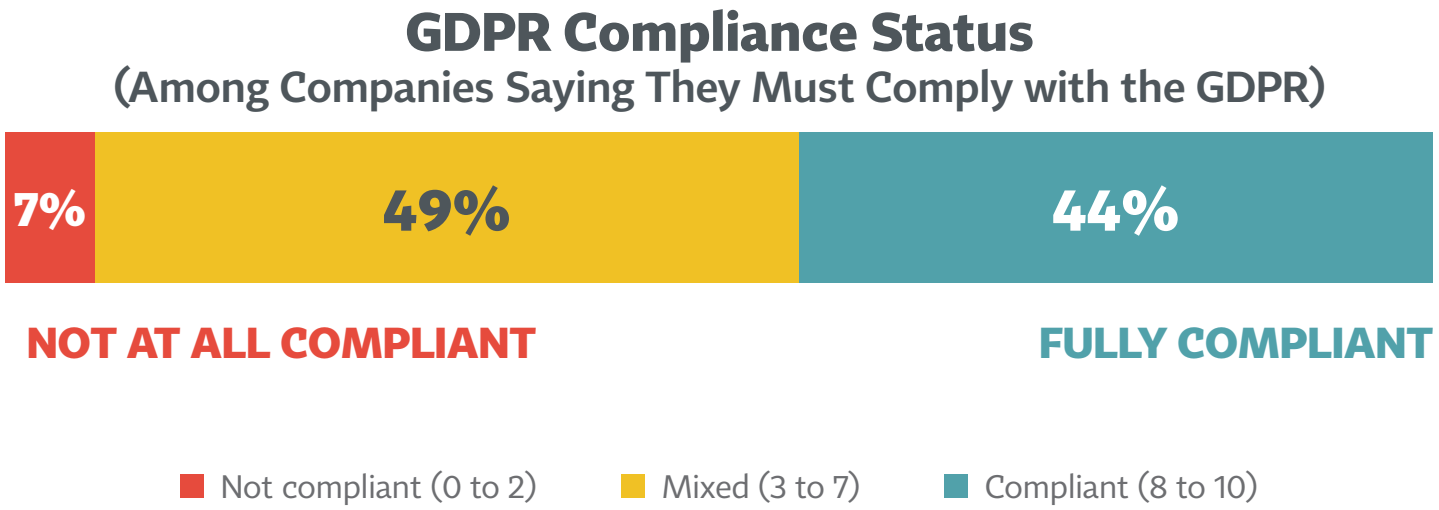
Perceived level of GDPR difficulty has fallen in several areas since last year, including Right to be Forgotten and Data Portability



J8: Rate the following legal obligations of the General Data Protection Regulation in terms of how difficult they are for your company to comply

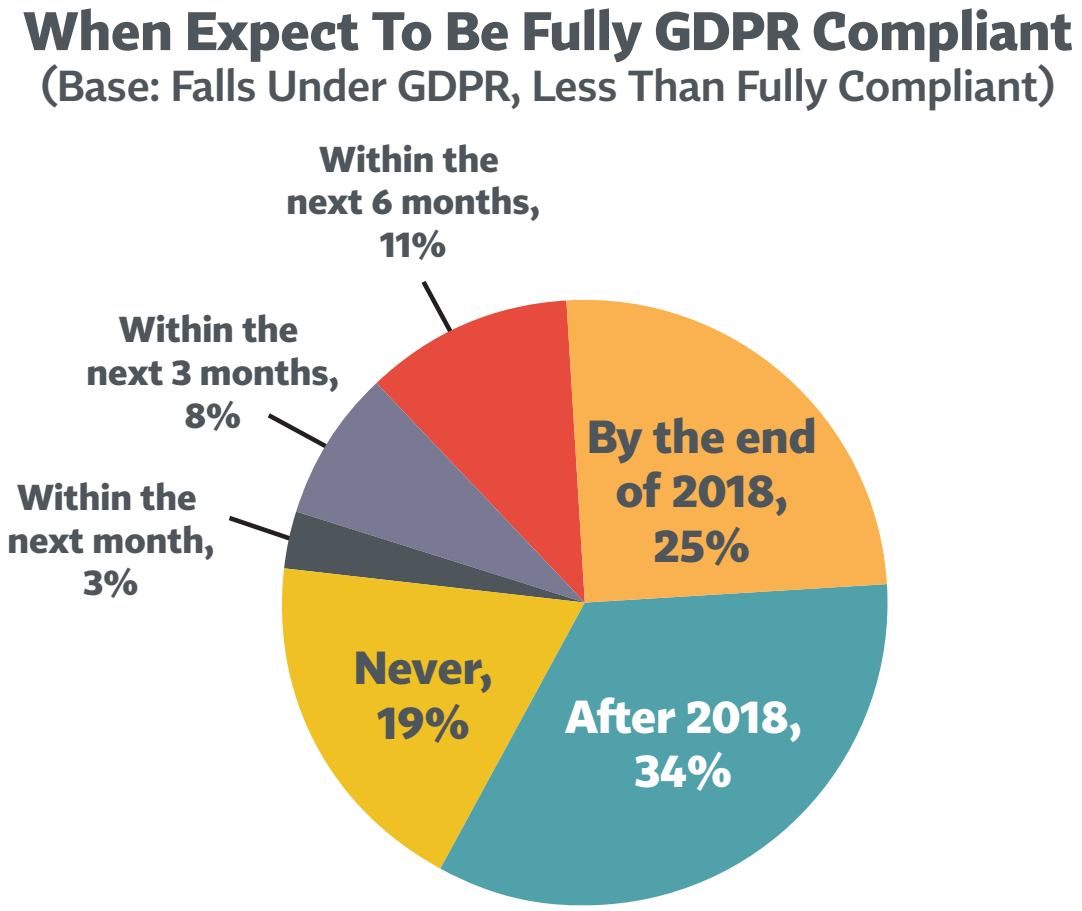
Just 44% of GDPR-affected firms consider themselves fully compliant or close to it

More than half give themselves a lower rating, including 49% giving a "mixed" rating to their current level of compliance



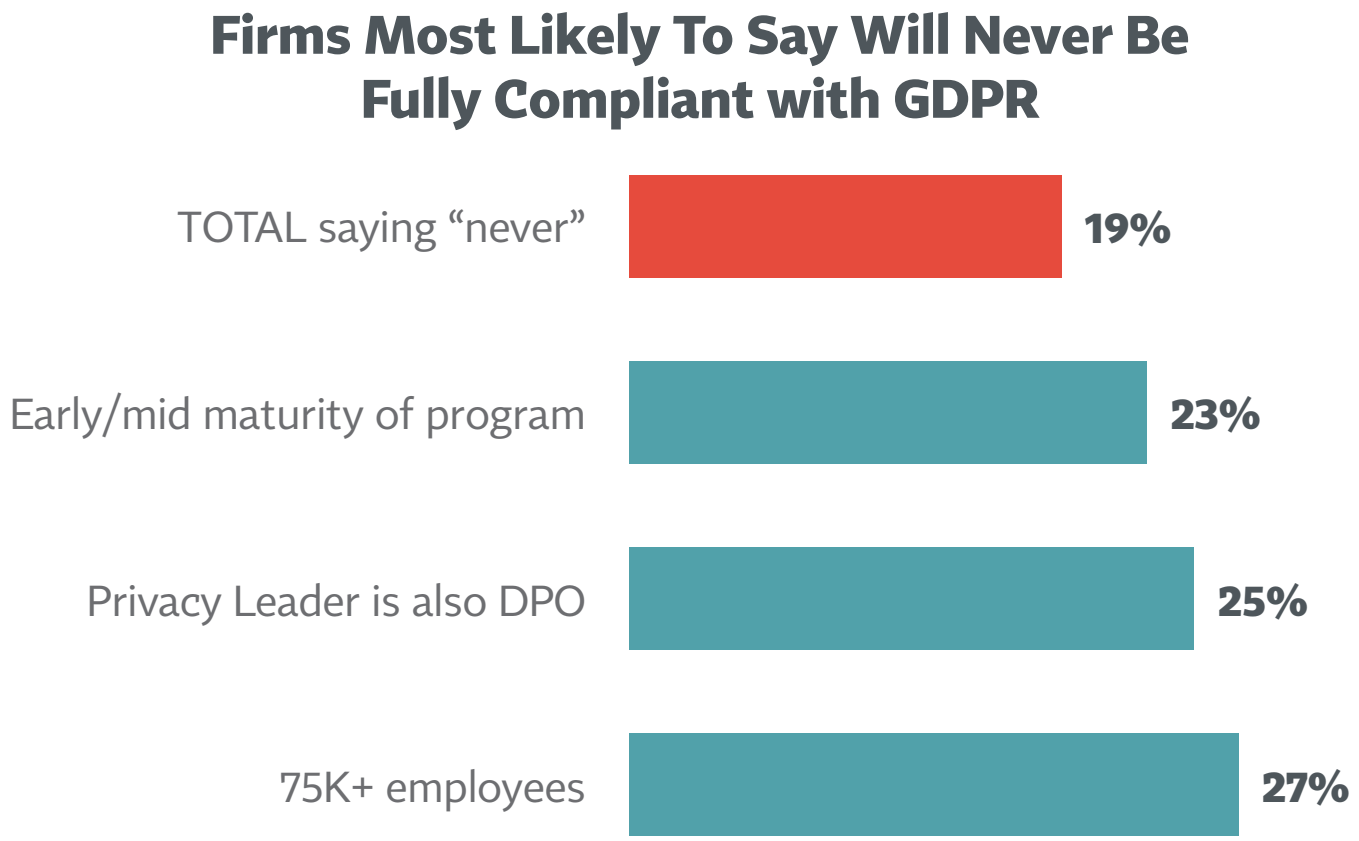
J18: All things considered, how would you rate your current level of GDPR compliance?

For those less than compliant, one-third say they won't reach compliance until after 2018; 19% say "never"



J19: When you do you expect to be completely compliant with the GDPR?

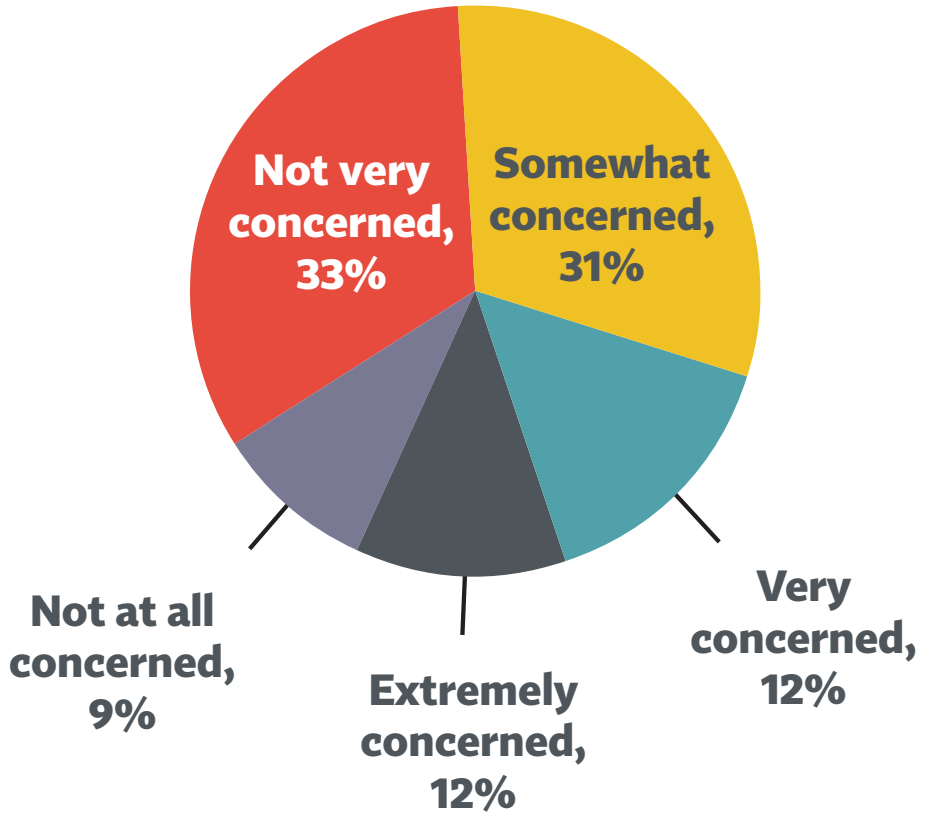
Although differences are directional, less mature & large firms are most likely to say they'll never be compliant



46% of firms falling under GDPR are concerned about how it will conflict with national law

Concerned About GDPR vs. National Conflicts

(For those who say they must comply with GDPR, but have to also comply with national laws)



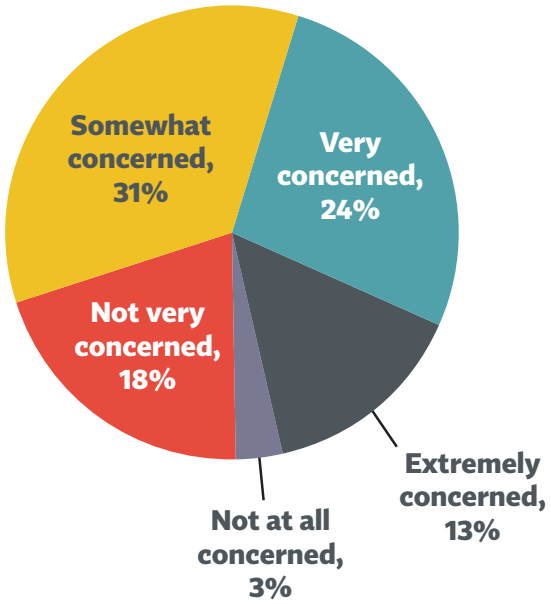
J7: How concerned are you that GDPR requirements could conflict with obligations set by national laws?

Privacy pros in the US are most concerned about conflicts with national laws

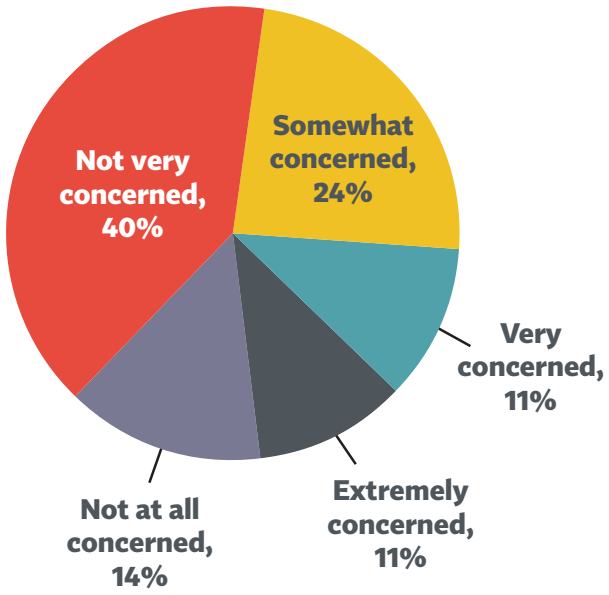
Concerned About GDPR vs. National Conflicts

(For those who say they must comply with GDPR, but have to also comply with national laws)

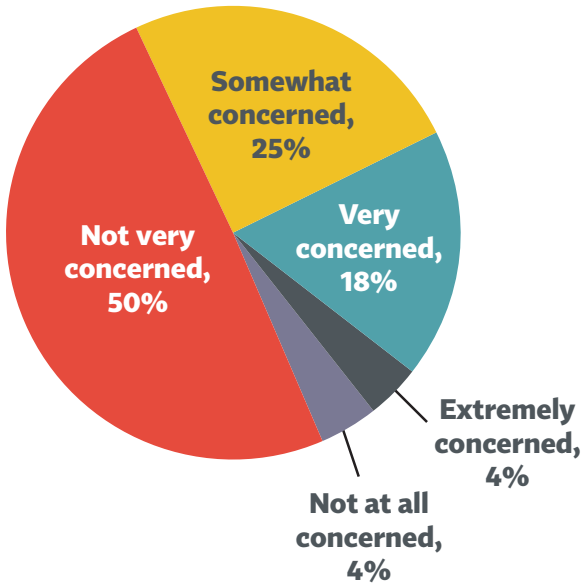
Respondent Based in US



Respondent Based in EU

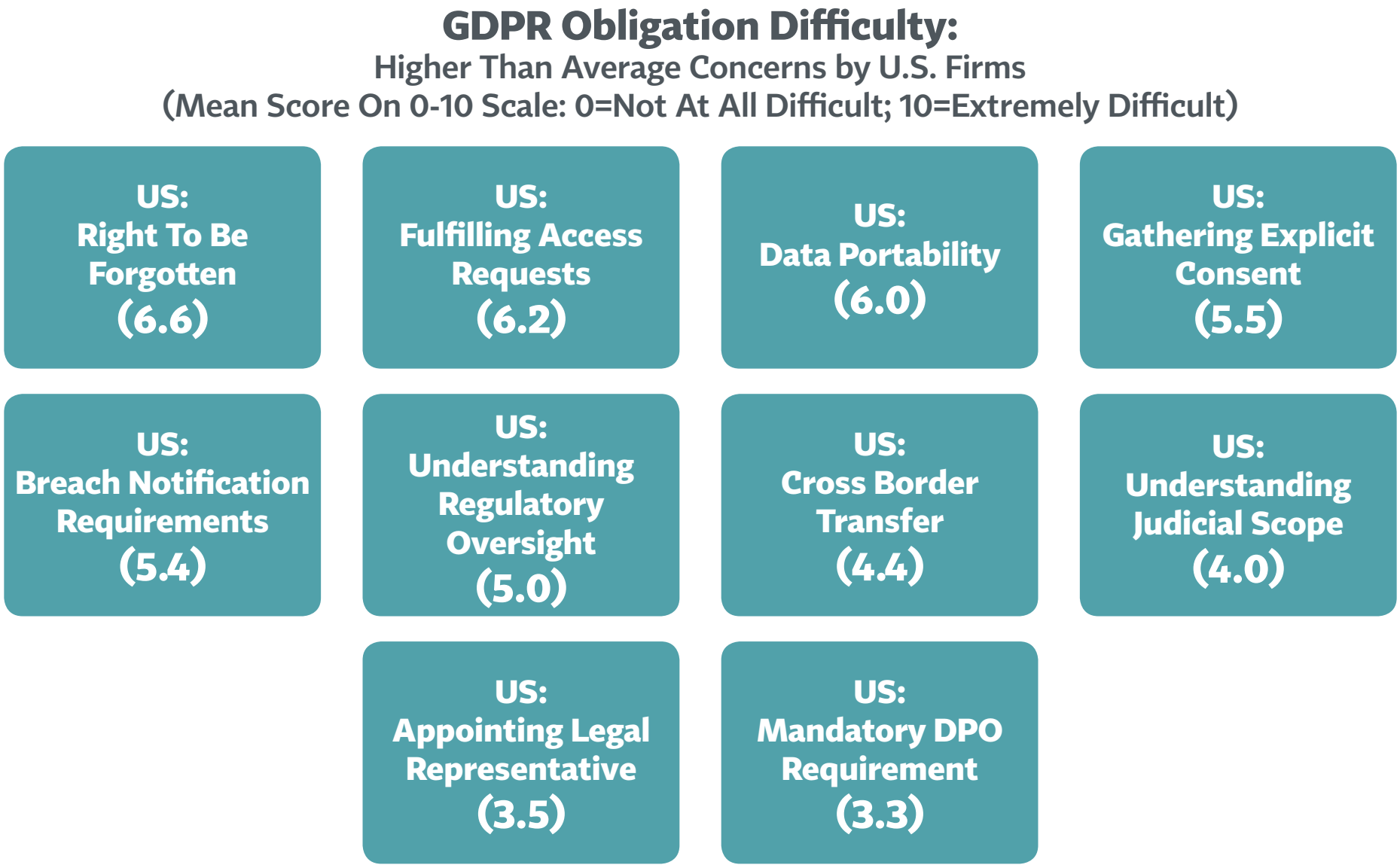


Respondent Based Elsewhere



J7: How concerned are you that GDPR requirements could conflict with obligations set by national laws?

US firms are more likely than EU firms to consider most GDPR obligations "difficult"

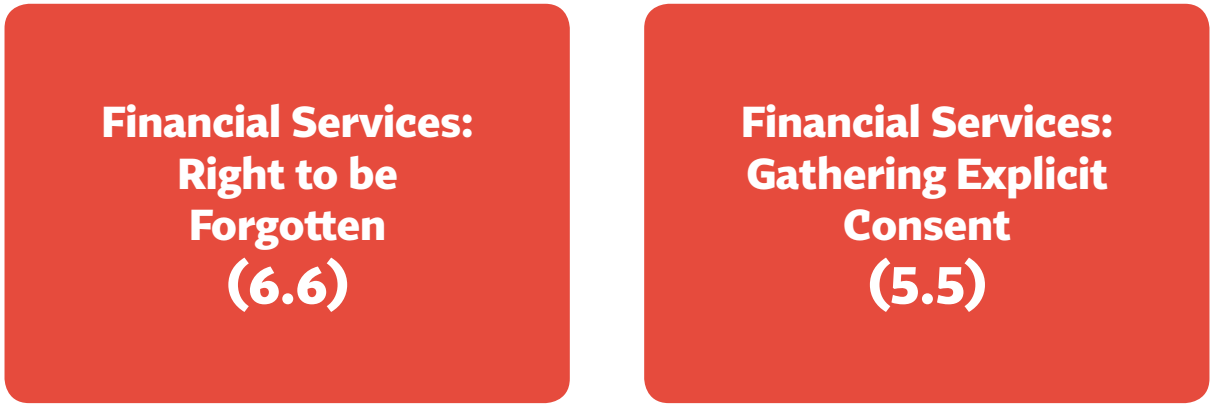


J8: Rate the following legal obligations of the General Data Protection Regulation in terms of how difficult they are for your company to comply.

Two obligations are especially concerning to financial firms: explicit consent and right to be forgotten

GDPR Obligation Difficulty:

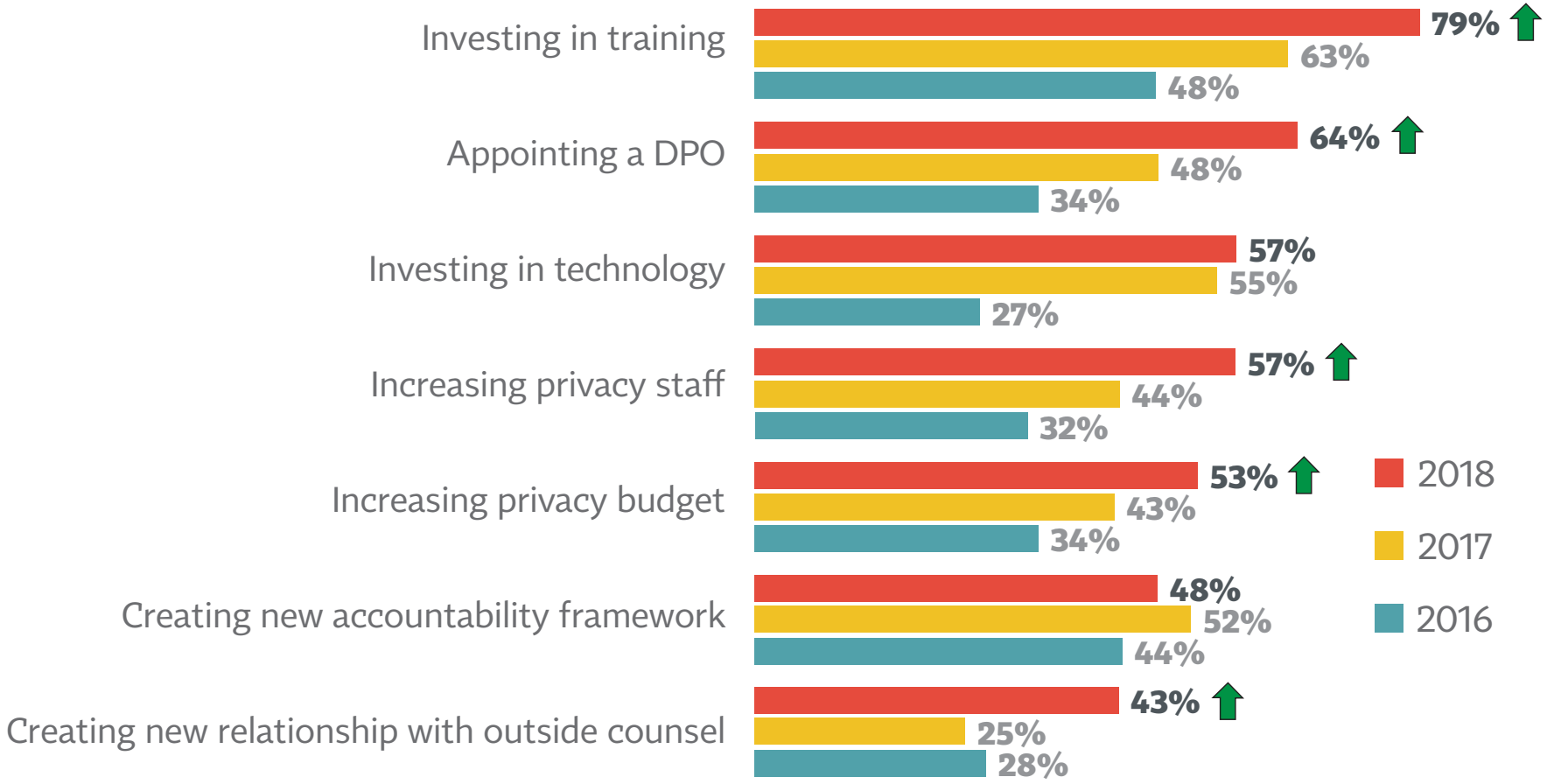
Higher Than Average Concerns by Financial Services Companies
(Mean Score On 0-10 Scale: 0=Not At All Difficult; 10=Extremely Difficult)



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

With 2018 being the GDPR compliance year, we see large increases in preparation steps across the board

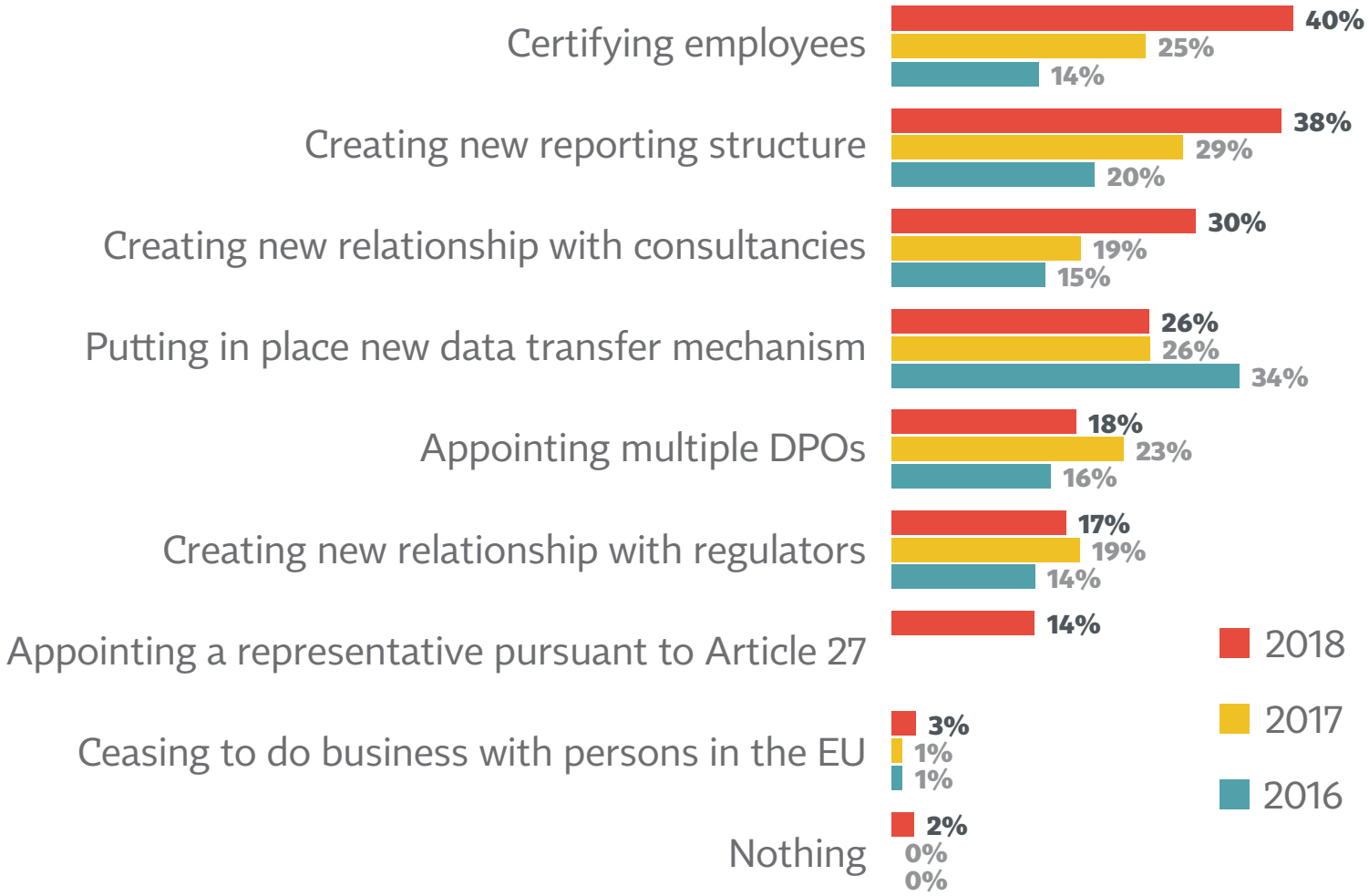
Steps Being Taken To Prep for GDPR
(Among Companies Saying They Must Comply with the GDPR)



J9: What, if anything, is your organization doing to prepare for the GDPR?

Two more secondary steps also saw large increases this year: employee certification and reporting changes

Steps Being Taken To Prep for GDPR (*continued*)
(Among Companies Saying They Must Comply with the GDPR)

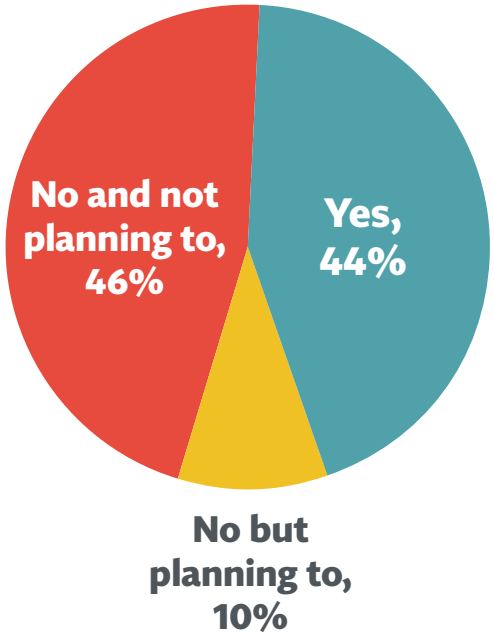


J9: What, if anything, is your organization doing to prepare for the GDPR?

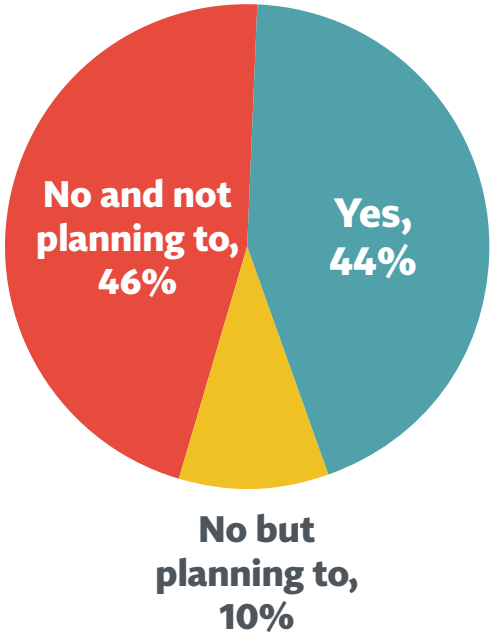
GDPR has fundamentally changed the structure of many organizations, and that will continue

As Part of GDPR Compliance Efforts, Has…
(Among Companies Saying They Must Comply with the GDPR)

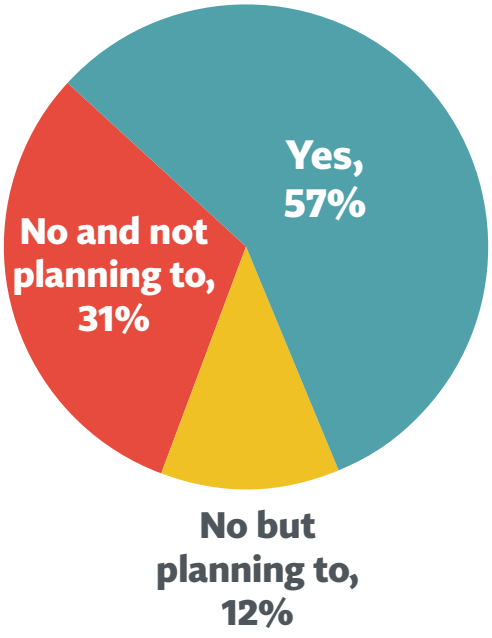
Reporting Structure Changed?



Position of Privacy Leader Elevated?



Reporting to Board Changed?



J10: Has your privacy team's reporting structure changed in the last year as part of GDPR compliance efforts?
J11: Have you elevated the position of privacy leader in the last year due to GDPR compliance efforts?
J11a: Has reporting of privacy matters to the board of directors changed in the last year as part of GDPR compliance efforts?

The average GDPR-affected firm has added 2.8 full-time and 2.5 part-time employees to help comply

Among the largest firms, the number of additional hires averages 13

Additional Employees Hired Because of GDPR
(Among Companies Saying They Must Comply with the GDPR)

BY EMPLOYEE SIZE

Mean Employees Hired	TOTAL	Under 5K	5–24.9K	25–74.9K	75K+*
Full time	2.8	1.0	2.4	3.0	**6.7**
Part time	2.5	0.4	2.4	3.2	**6.3**

Significantly higher than total * Small sample size

J12: How many additional employees has your company hired to assist with GDPR-related activities, if any?

Health and tech firms have hired the most additional staff because of the GDPR

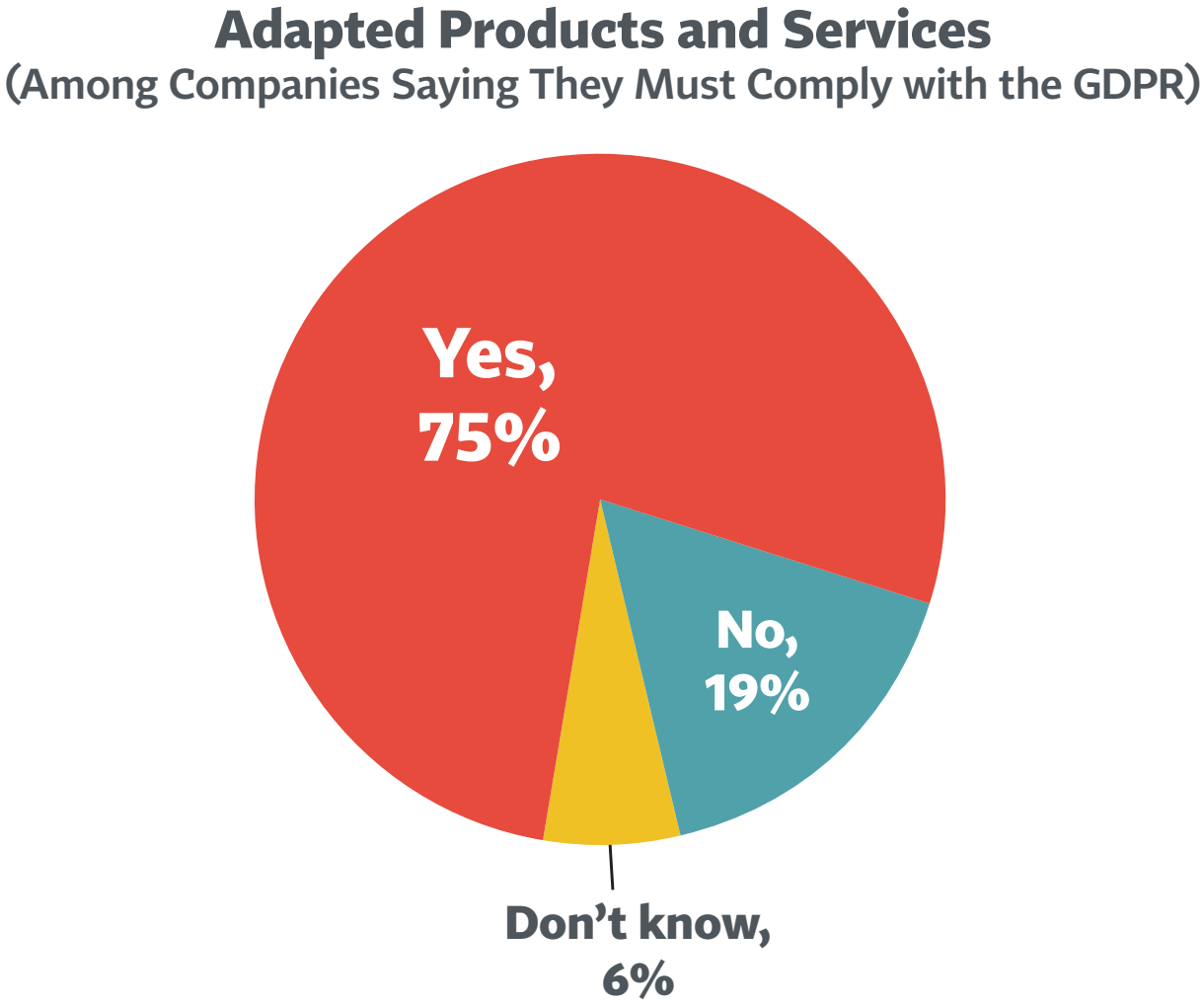
Additional Employees Hired Because of GDPR
(Among Companies Saying They Must Comply with the GDPR)

BY INDUSTRY

Mean Employees Hired	Average	Financial	Health	Tech
Full time	2.8	1.9	3.6	5.5
Part time	2.5	3.4	4.7	3.3

J12: How many additional employees has your company hired to assist with GDPR-related activities, if any?

3 in 4 firms say they've adapted products and services to be GDPR compliant



J13: Has your company adapted current products and services to be GDPR compliant?

The average firm says they'll spend a total of $3 million as a result of GDPR

Additional Spending Resulting from GDPR
(Among Companies Saying They Must Comply with the GDPR)

BY HQ LOCATION

Mean Spending (000)	TOTAL	US	EU
Already spent to adapt products and services	$1,276	$1,175	$1,535
Additional expected to spend to adapt	$822	$730	$981
Added $ to adapt to GDPR other than adapting products and services	$989	$758	$1,361

J14. How much have you spent (including salaries and benefits) to adapt these current products and services to be GDPR compliant?
J15. How much do you expect to further spend (including salaries and benefits) to adapt products and services to be GDPR compliant?
J16. In addition to spending to adapt products and services, about how much do you think you will spend (including salaries and benefits) in your budget to comply with GDPR, not including spending to adapt specific products and services? We're just looking for your best estimate.

Financial and tech firms have been the biggest spenders on GDPR compliance

Additional Spending Resulting from GDPR
(Among Companies Saying They Must Comply with the GDPR)

BY INDUSTRY

Mean Spending (000)	Average	Financial	Health*	Tech
Already spent to adapt products and services	$1,276	$2,666	$381	$1,861
Additional expected to spend to adapt	$822	$1,161	$279	$781
Added $ to adapt to GDPR other than adapting products and services	$989	$2,320	$344	$466

* Small sample size

J14. How much have you spent (including salaries and benefits) to adapt these current products and services to be GDPR compliant?
J15. How much do you expect to further spend (including salaries and benefits) to adapt products and services to be GDPR compliant?
J16. In addition to spending to adapt products and services, about how much do you think you will spend (including salaries and benefits) in your budget to comply with GDPR, not including spending to adapt specific products and services? We're just looking for your best estimate.

GDPR spending has also been highest among the largest firms by number of employees

Additional Spending Resulting from GDPR
(Among Companies Saying They Must Comply with the GDPR)

BY EMPLOYEE SIZE

Mean Spending (000)	TOTAL	Under 5K	5–24.9K	25–74.9K	75K+*
Already spent to adapt products and services	$1,276	$478	$848	$1,207	$2,935
Additional expected to spend to adapt	$822	$271	$886	$1,673	$1,144
Added $ to adapt to GDPR other than adapting products and services	$989	$168	$1,376	$1,843	$1,510

* Small sample size

J14. How much have you spent (including salaries and benefits) to adapt these current products and services to be GDPR compliant?
J15. How much do you expect to further spend (including salaries and benefits) to adapt products and services to be GDPR compliant?
J16. In addition to spending to adapt products and services, about how much do you think you will spend (including salaries and benefits) in your budget to comply with GDPR, not including spending to adapt specific products and services? We're just looking for your best estimate.

Staff and external help will make up the lion's share of any additional spending firms expect to make

Distribution of Additional GDPR Compliance Budget
(Among Companies Saying They Must Comply with the GDPR)

J17: About what percentage of that additional budget for GDPR compliance falls into each of these categories?

A larger share of additional GDPR spending in the EU will go to tech solutions vs. in the US

Distribution of Additional GDPR Compliance Budget
(Among Companies Saying They Must Comply with the GDPR)

BY HQ LOCATION

% Of Budget To:	TOTAL	US	EU
Outside counsel	18%	21%	12%
Consultants	15%	13%	16%
Technology solutions	22%	19%	27%
Training	12%	11%	13%
Staff	33%	34%	33%

J17: About what percentage of that additional budget for GDPR compliance falls into each of these categories?

Financial firms are also especially likely to allocate a significant proportion of new GDPR spending to tech

Distribution of Additional GDPR Compliance Budget
(Among Companies Saying They Must Comply with the GDPR)

BY INDUSTRY

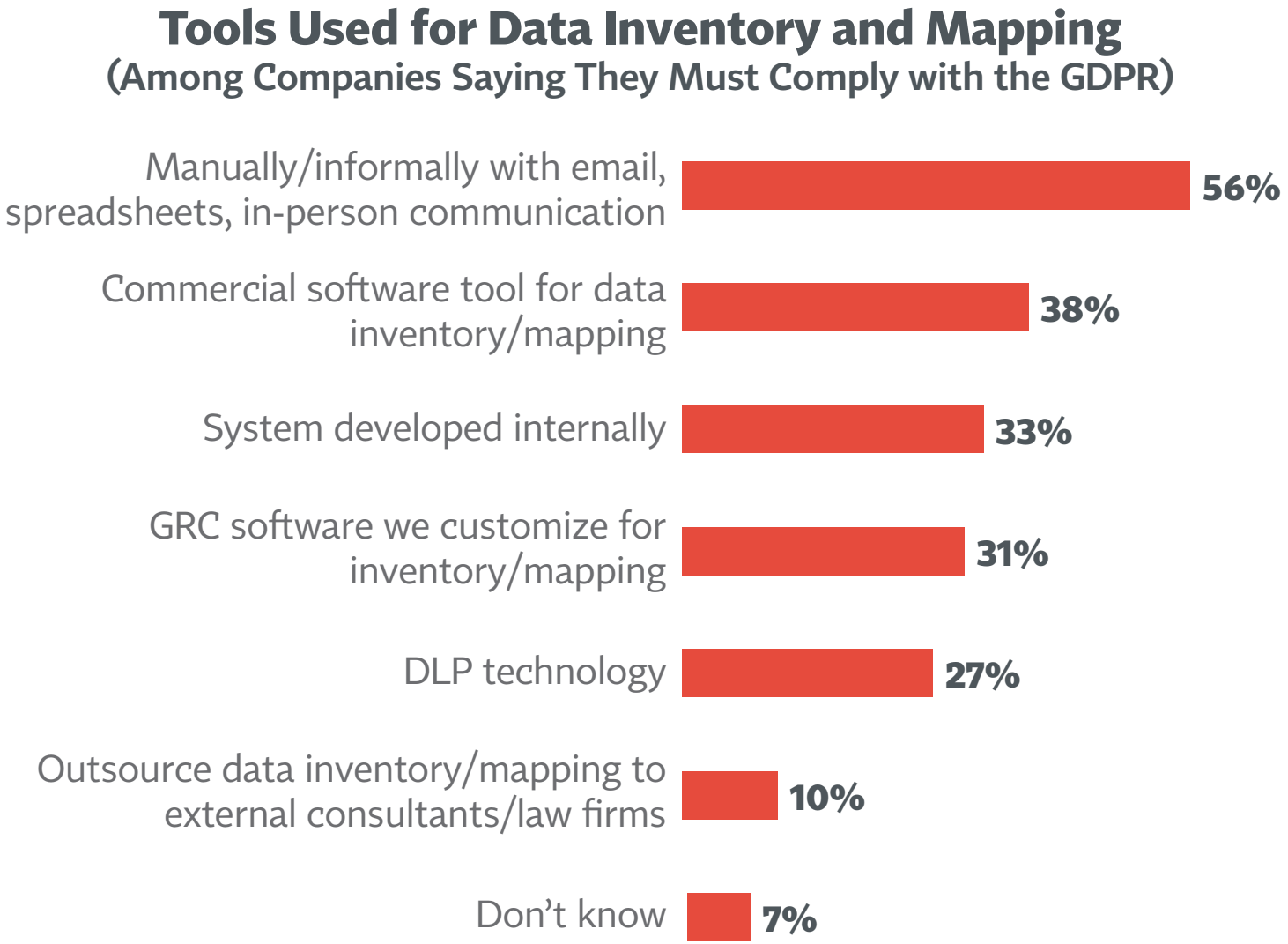
% Of Budget To:	Average	Financial	Health*	Tech
Outside counsel	18%	12%	14%	20%
Consultants	15%	16%	15%	10%
Technology solutions	22%	**38%**	33%	17%
Training	12%	9%	12%	14%
Staff	33%	26%	26%	37%

Significantly higher than total

* Small sample size

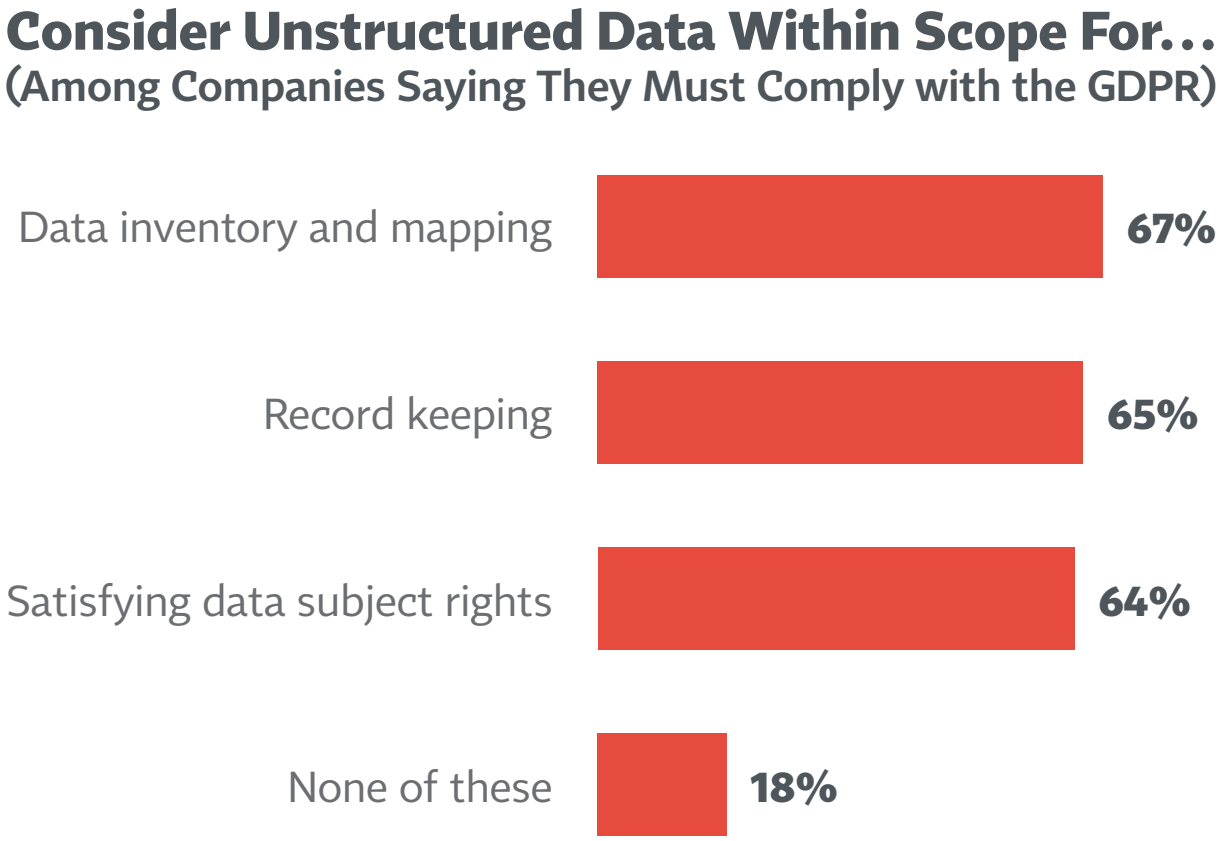
J17: About what percentage of that additional budget for GDPR compliance falls into each of these categories?

Manual methods are most often cited as tools for data inventory and mapping



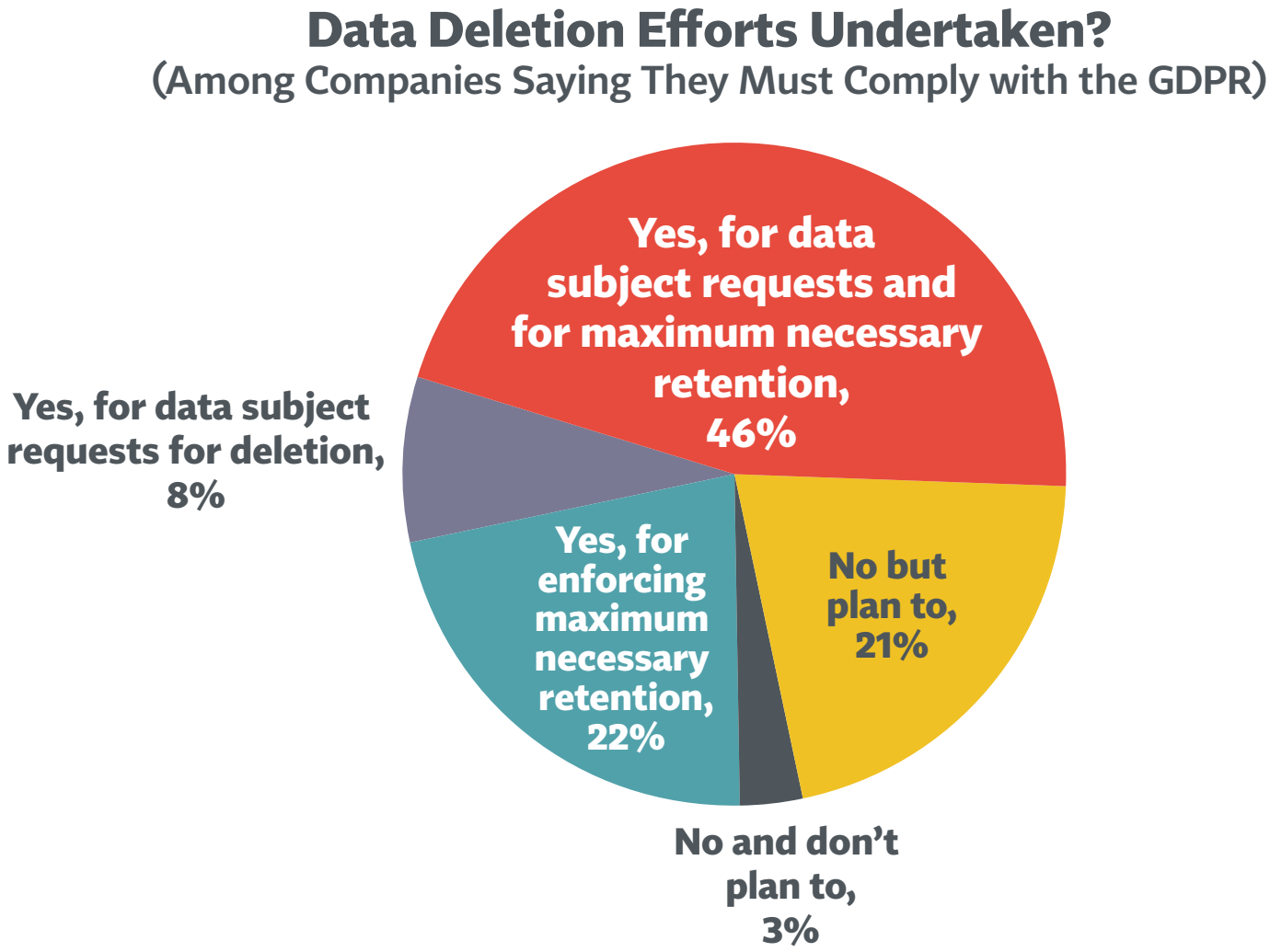
J20: Which of the following tools will you use to perform data inventory and mapping requirements of article 30 of GDPR? ?

2 in 3 consider unstructured data to be within scope for data inventory, record keeping, and data subject rights



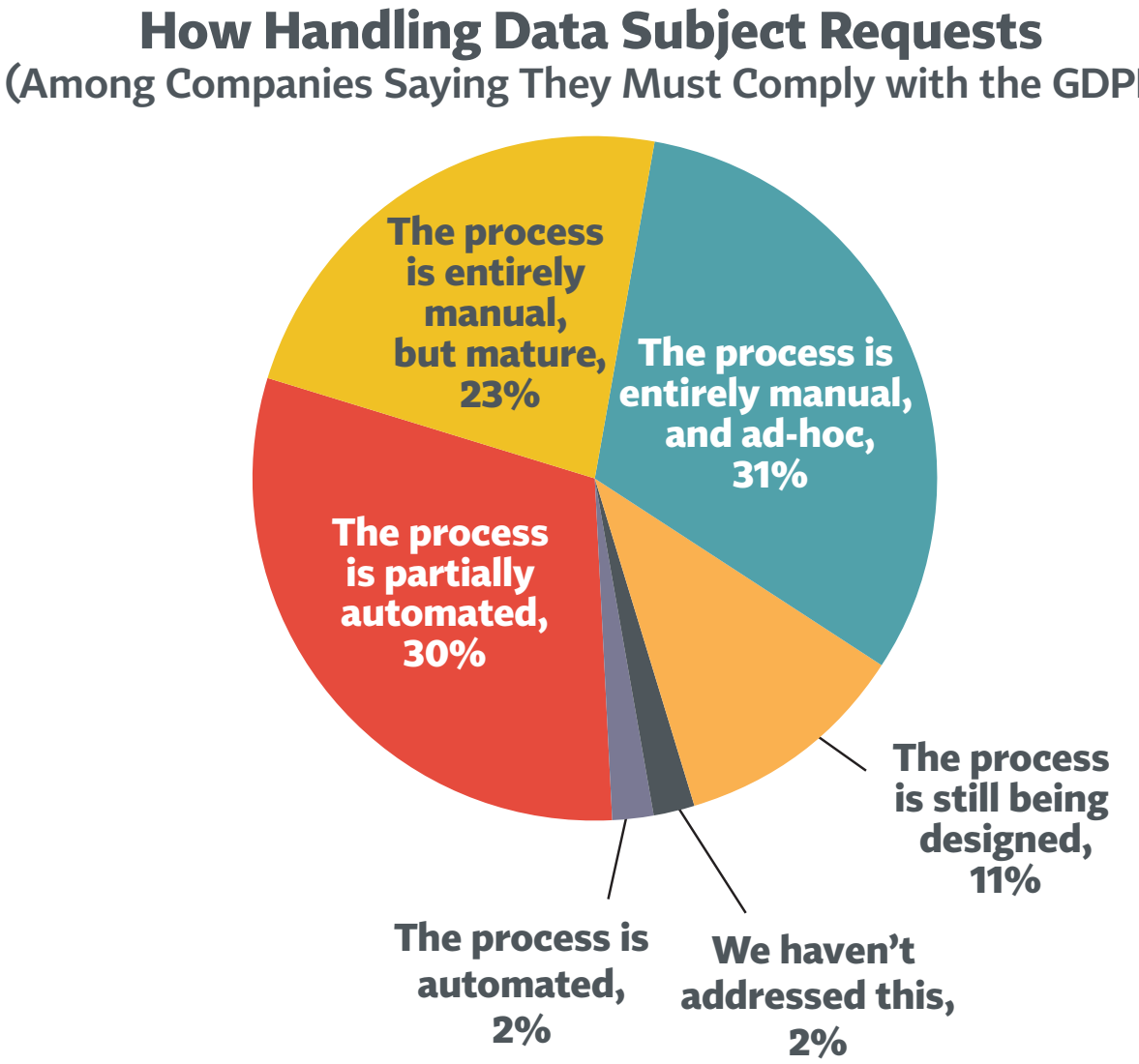
J21: When it comes to GDPR compliance, does your company consider unstructured data to be within scope for any of the following?

3 in 4 firms have taken data deletion efforts; about half have done it for requests and maximum retention



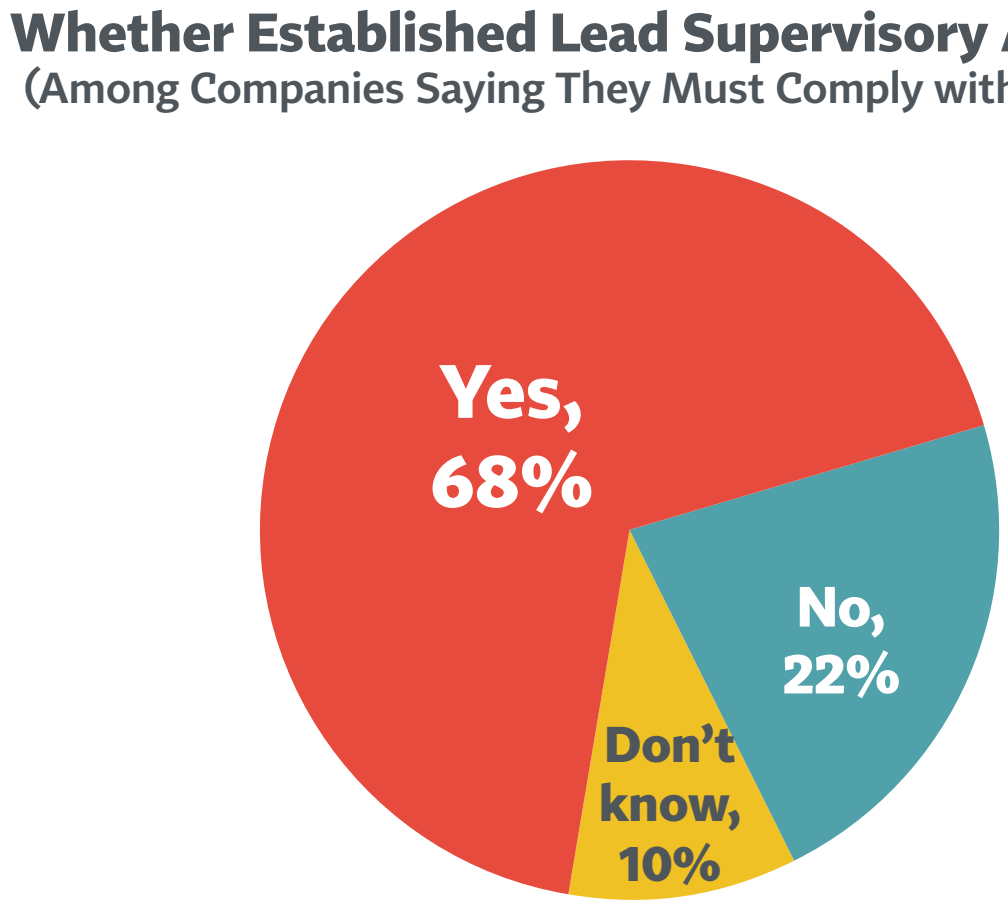
J22: Has your company undertaken efforts specifically aimed at data deletion?

As for data subject requests, more than half of organizations use an entirely manual process



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

Two thirds of GDPR affected firms have established a lead supervisory authority; 1 in 5 say they haven't



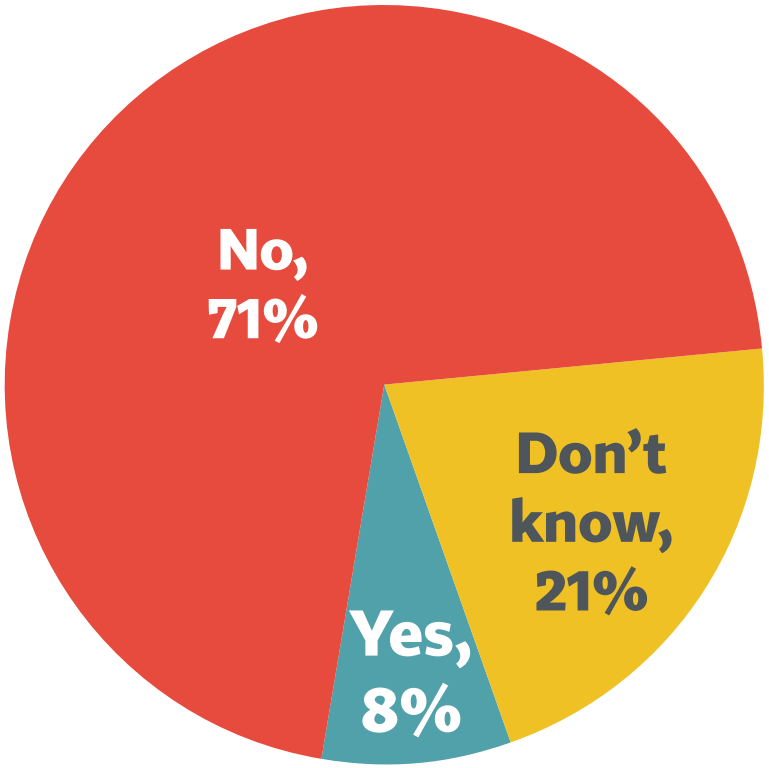
J24: Per GDPR regulations, has your company identified a supervisory authority you consider to your "lead supervisory authority"?

When organizations have a choice of lead authority, they gravitate toward known quantities

J26: What are the main reasons your company took steps to identify a specific lead supervisory authority?

1 in 10 falling under GDPR say they've notified a supervisory authority of high risk processing

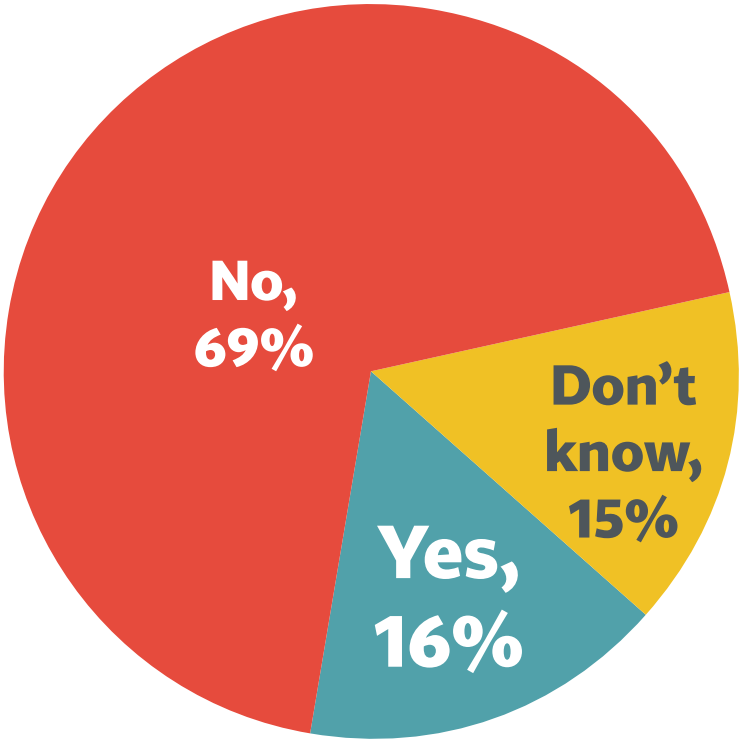
Whether Notified Supervisory Authority of High-Risk Processing
(Among Companies Saying They Must Comply with the GDPR)



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

In addition, 16% have notified an authority of a data breach

Whether Notified Supervisory Authority of Data Security Breach
(Among Companies Saying They Must Comply with the GDPR)



J27: Pursuant to GDPR, has your company already notified any supervisory authorities of a data security breach?

EU firms are more likely than US firms to have taken a range of actions related to GDPR compliance

But U.S. organizations have adapted more products and services and are more likely to report they are fully compliant

BY LOCATION

	TOTAL	US	EU
Have appointed DPO	64%	61%	70%
Have invested in technology	57%	61%	59%
Have certified employees	40%	32%	**51%**
Have created relationship with outside counsel	43%	**56%**	37%
Have created relationship with consultancies	30%	25%	**35%**
Have increased privacy budget	53%	51%	59%
Have increased privacy staff	57%	54%	**65%**
Have created new reporting structures	38%	28%	**48%**
Reporting structure has changed	44%	34%	**57%**
Elevated position of privacy lead	44%	32%	**59%**
Reporting to board has changed	57%	47%	**70%**
Adapted products and services	75%	**83%**	75%
8-10 rating on being fully compliant	44%	53%	38%
Has identified supervisory authority	67%	62%	**77%**

Significantly higher than total

Similarly, larger firms are more likely to be mature firms that have responded more clearly to the GDPR

BY EMPLOYEE SIZE

	TOTAL	Under 5K	5–24.9K	25–74.9K*	75K+*
Have invested in technology	57%	48%	51%	61%	**78%**
Have certified employees	40%	37%	30%	37%	**57%**
Have created relationship with outside counsel	43%	32%	47%	**54%**	51%
Have created relationship with consultancies	30%	25%	**41%**	35%	25%
Have increased privacy budget	53%	43%	54%	59%	**65%**
Have increased privacy staff	57%	44%	63%	63%	**70%**
Have created new reporting structures	38%	34%	39%	**54%**	33%
Have created new accountability framework	41%	42%	**59%**	**58%**	46%
Adapted products and services	75%	77%	65%	65%	**88%**
8-10 rating on being fully compliant	44%	45%	33%	37%	**61%**

Significantly higher than total

And large, mature programs are most confident in their compliance

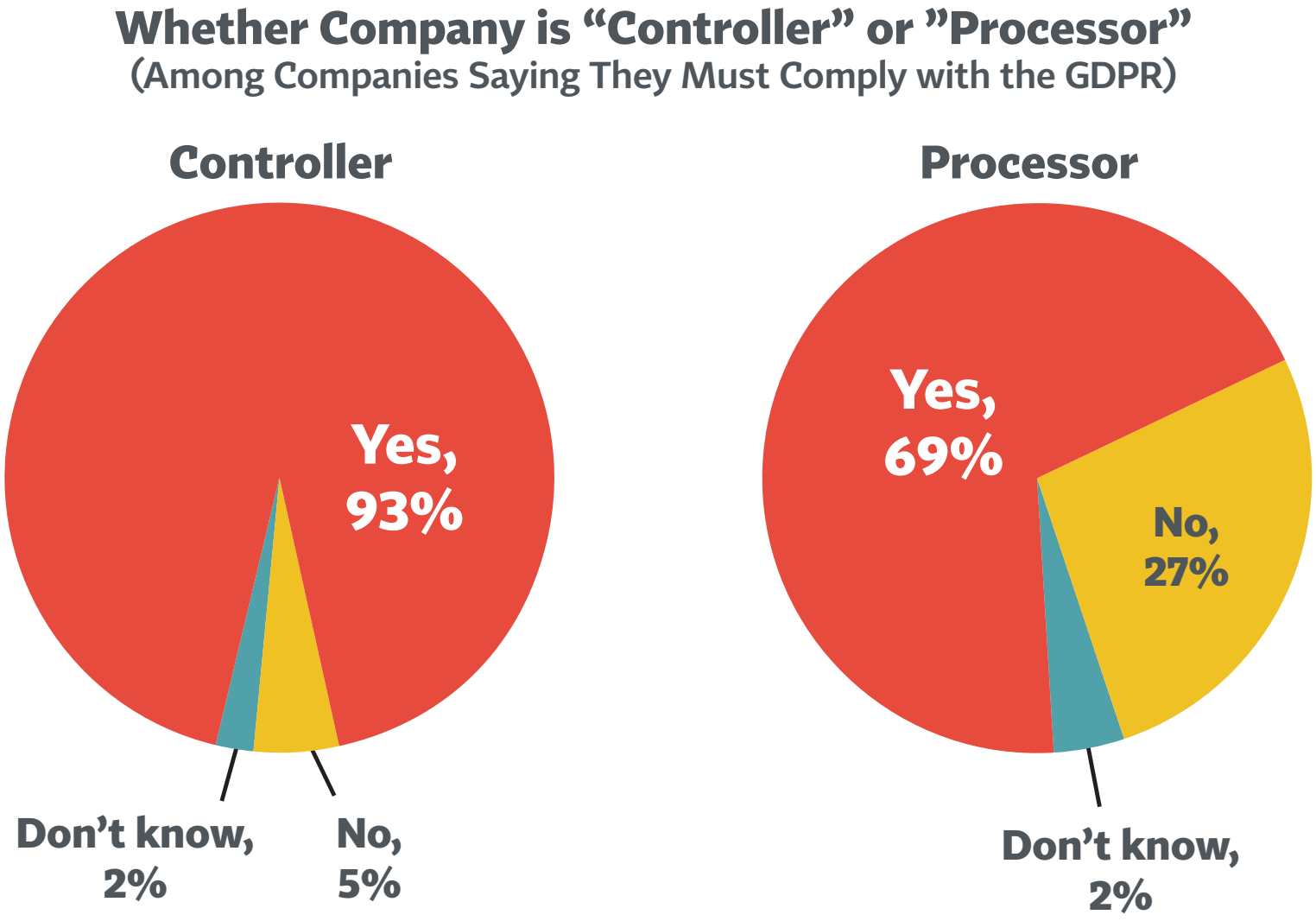
BY PROGRAM MATURITY

	TOTAL	Early/Mid	Mature
Have invested in technology	57%	63%	**75%**
Have certified employees	40%	42%	54%
Have created relationship with outside counsel	43%	**53%**	31%
Have created relationship with consultancies	30%	**41%**	24%
Have increased privacy budget	53%	**61%**	54%
Have increased privacy staff	57%	60%	47%
Have created new reporting structures	38%	44%	32%
Have created new accountability framework	41%	46%	43%
Adapted products and services	75%	81%	79%
8-10 rating on being fully compliant	44%	35%	**78%**

Significantly higher than total

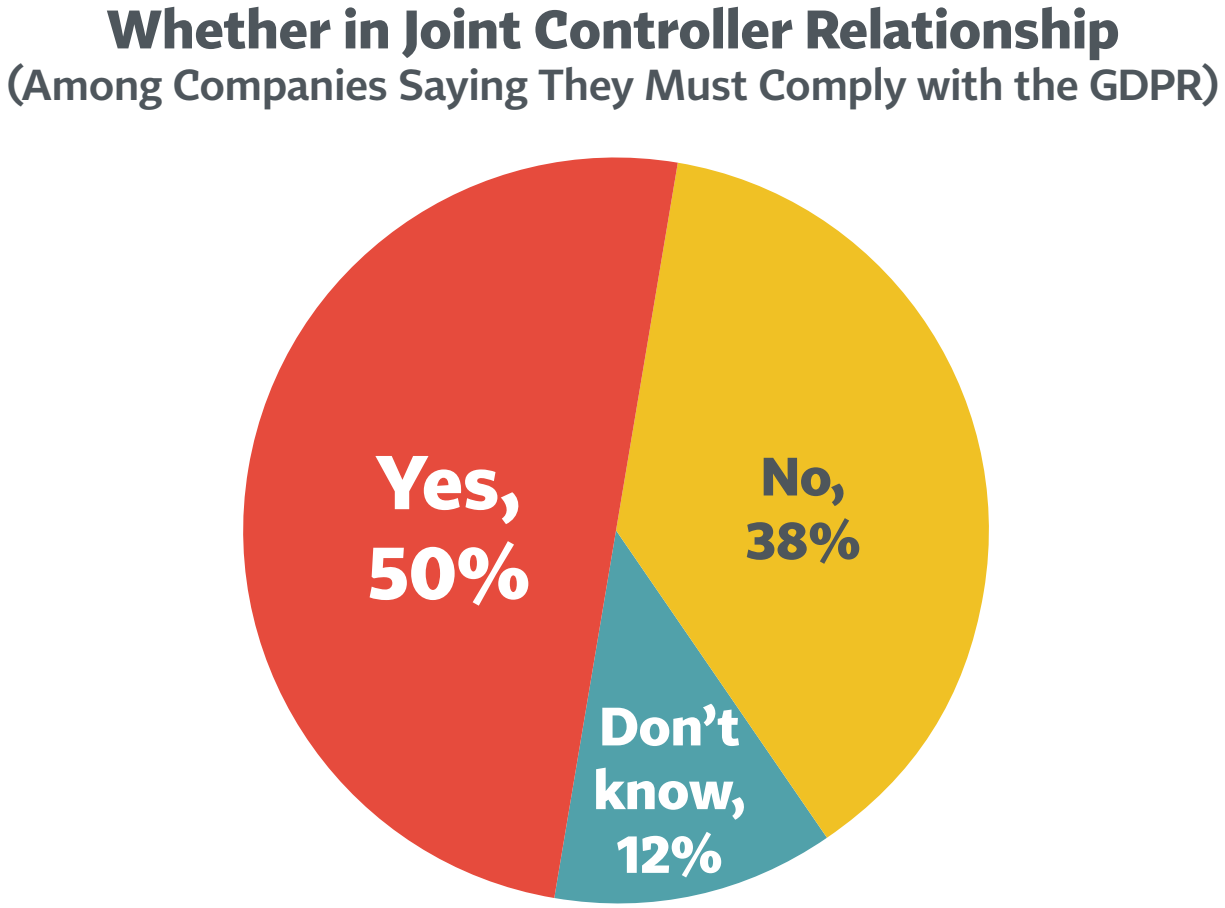
Contents

Virtually all the organizations in the survey are controllers, 7 in 10 act as processors



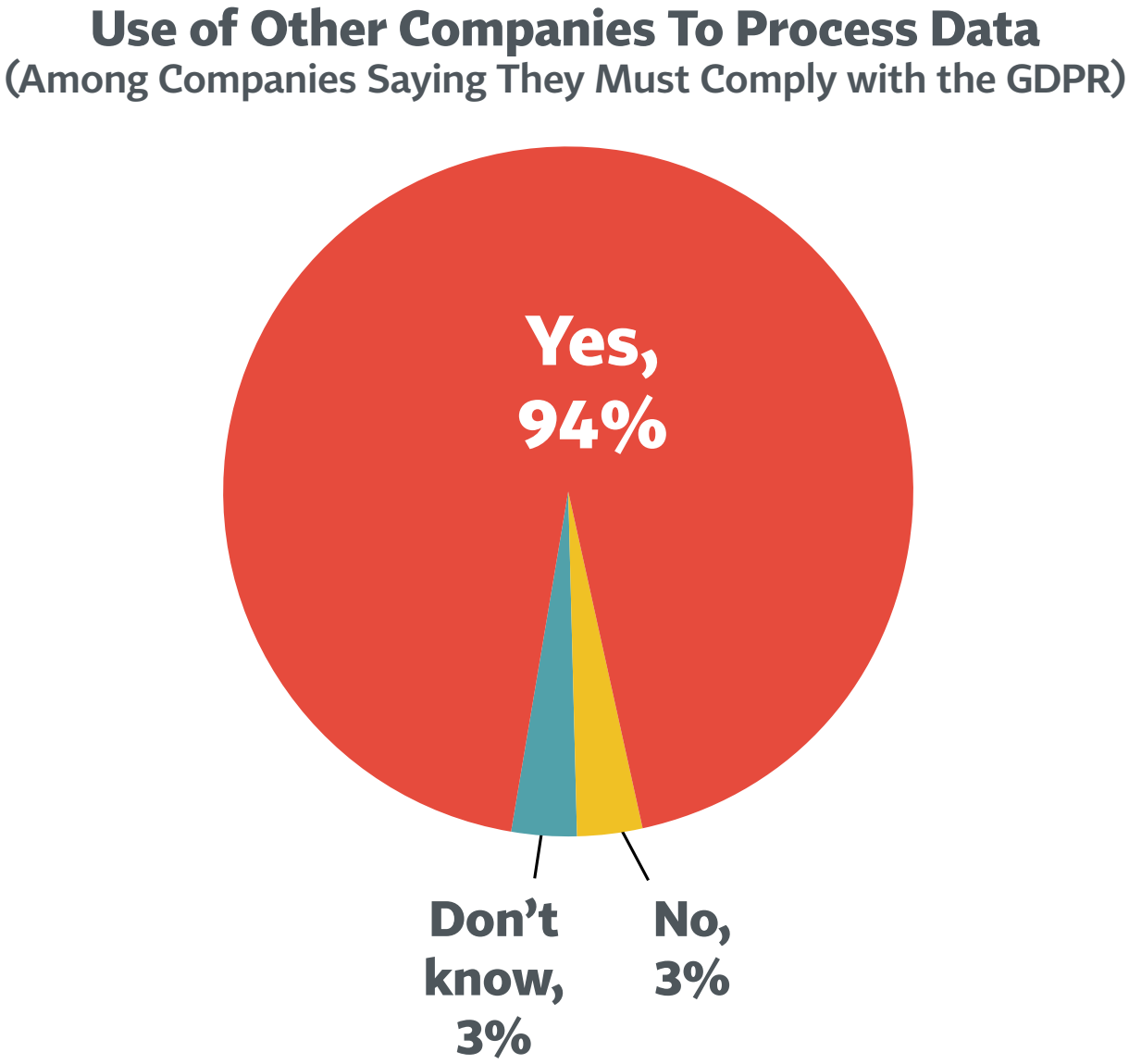
H1: Does your company determine the purposes and means of processing personal data (ie., you are a controller)?
H2: Does your company process personal data on behalf of other companies (ie, you are a processor)?

Half of firms say they're in a "joint controller" relationship



H9: Are you in a business relationship where you consider yourself a "joint controller"?

The vast majority of firms use third-party companies to process data

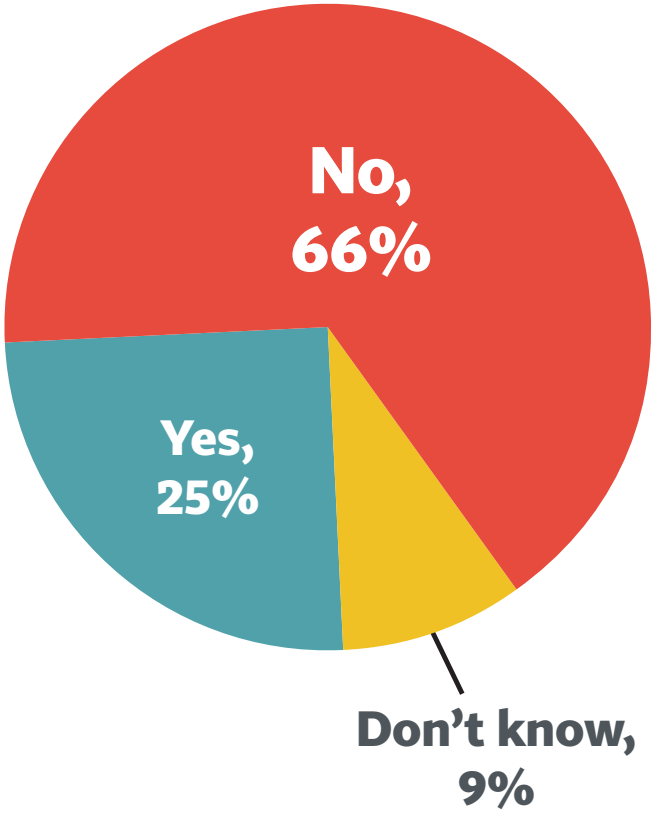


H3: Does your company have other companies process personal data on your behalf (ie., you use "processors")?

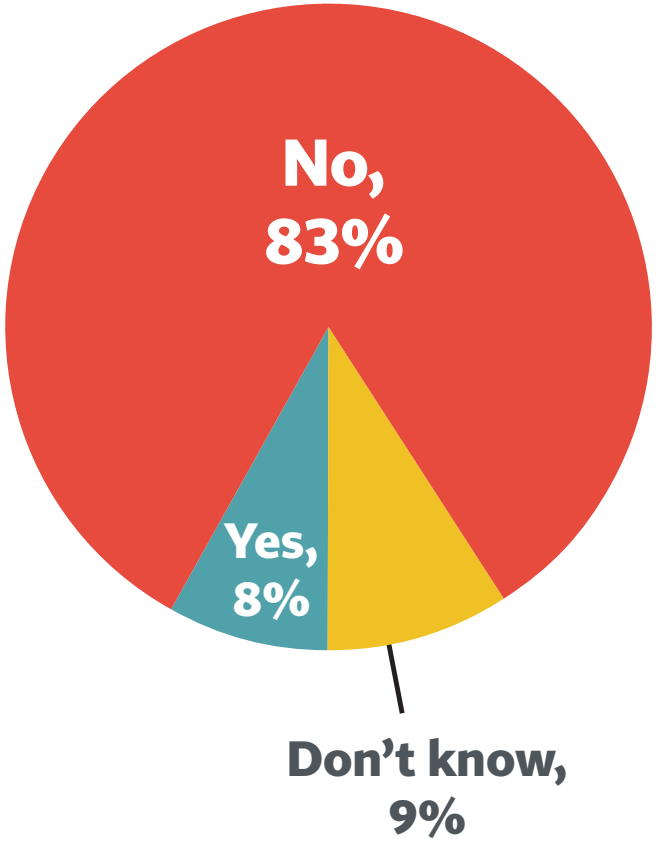
A quarter of respondents have changed processors, with almost 1 in 10 bringing it in house

Data Processing Changes Caused by GDPR
(Among Companies Saying They Must Comply with the GDPR)

Changed Processors



Brought Processing In House

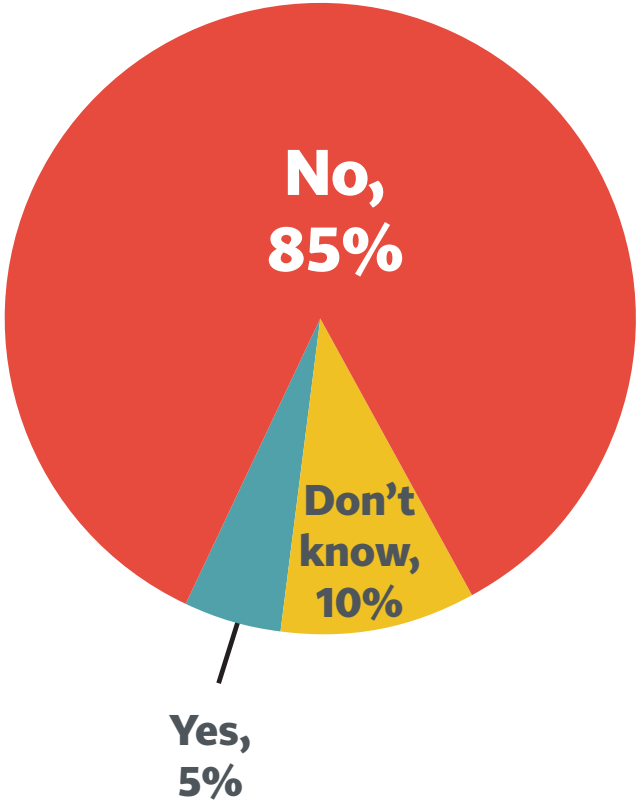


H4: Have you changed your processors to any extent because of the GDPR?
H5: Have you brought processing in-house because of the GDPR?
H5a: Have you outsourced processing previously done in house because of the GDPR?
H7: Have you lost business as a processor because of the GDPR?

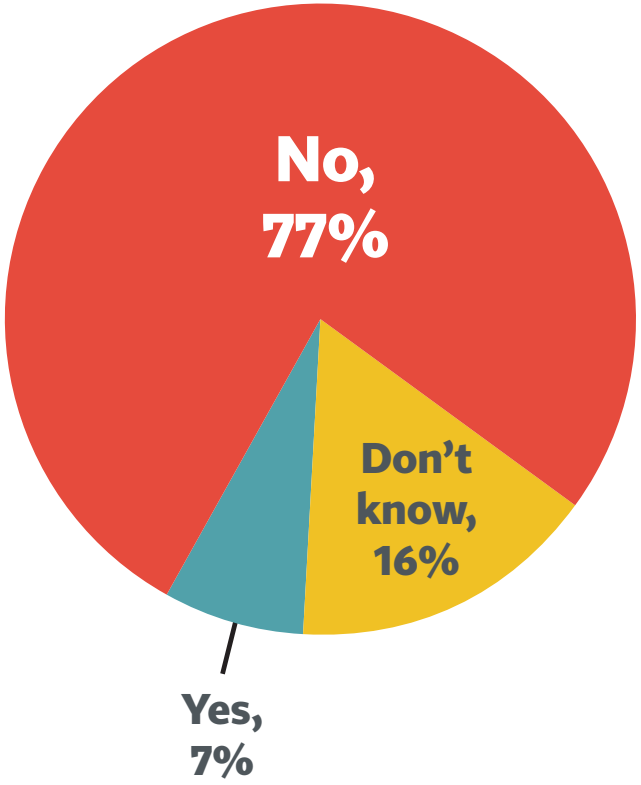
Similarly, the GDPR has led a small percentage to outsource processing, and some processors report losing business

Data Processing Changes Caused by GDPR
(Base: Falls Under GDPR)

Outsource Processing



Lost Processing Business



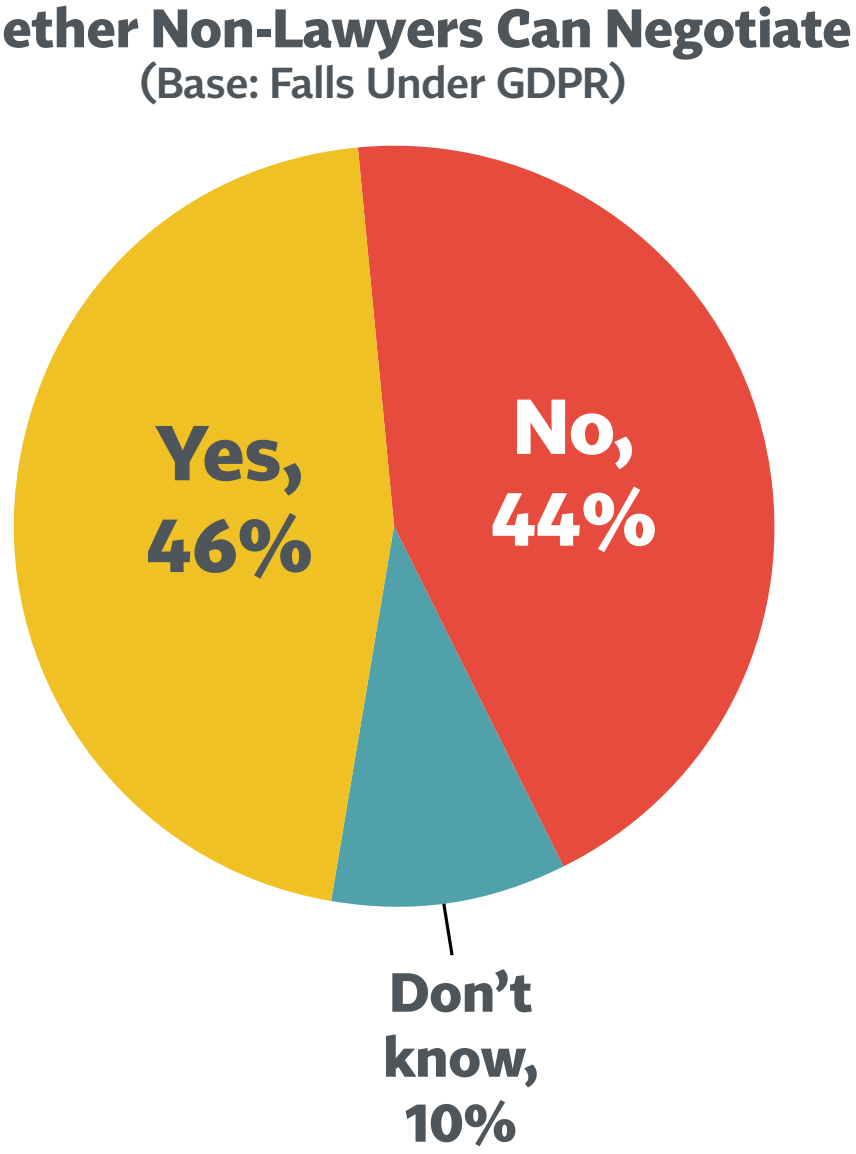
H4: Have you changed your processors to any extent because of the GDPR?
H5: Have you brought processing in-house because of the GDPR?
H5a: Have you outsourced processing previously done in house because of the GDPR?
H7: Have you lost business as a processor because of the GDPR?

For firms using others for processing, the contract is the primary way of assuring processor compliance

Steps Taken To Ensure Processor Responsibilities
(Base: Use Other Companies for Processing)

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

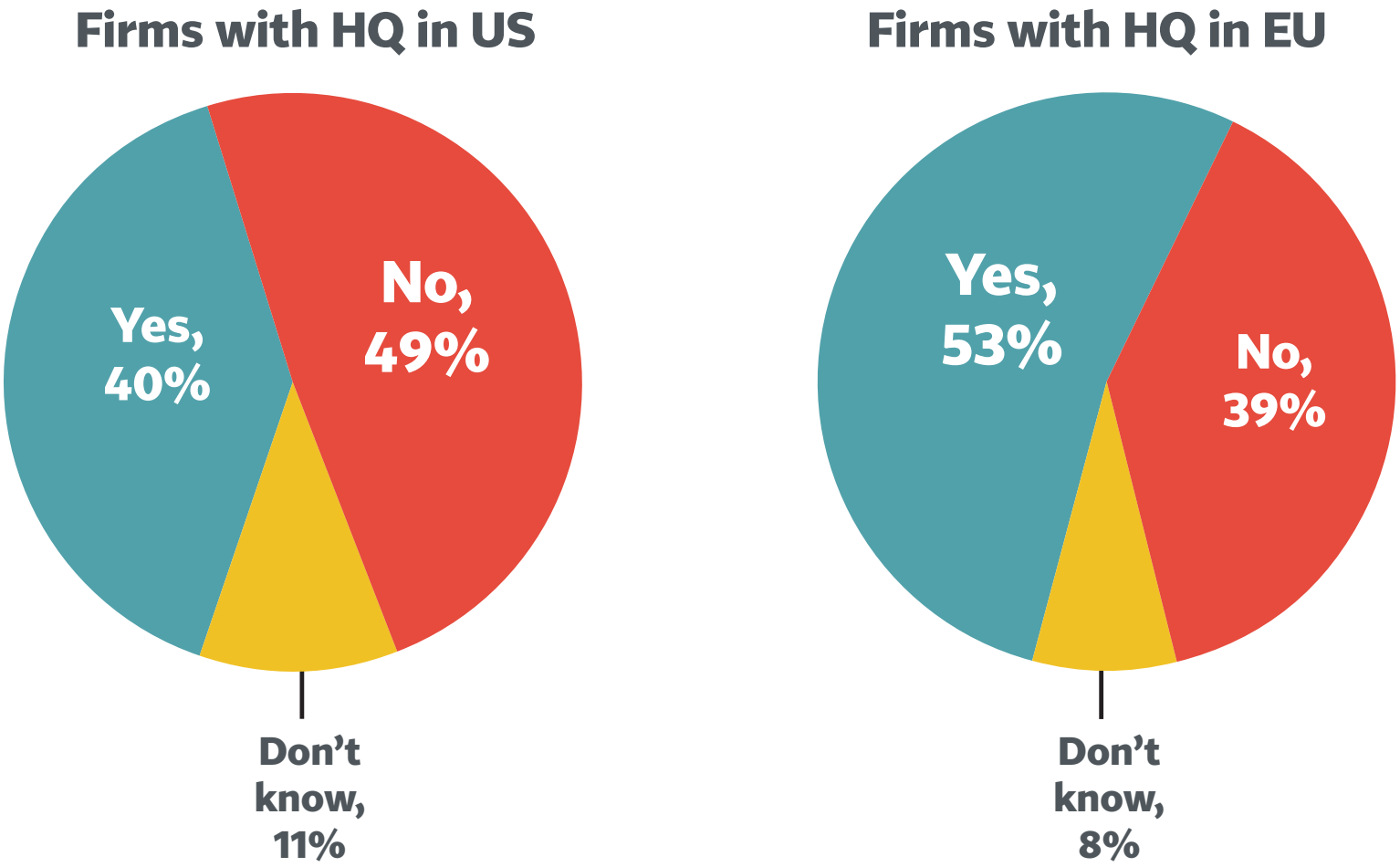
Half also say that in their firm, non-lawyers can negotiate data processing/ joint controller agreements



H10: In your company, can non-lawyers, including potentially the DPO, negotiate data processing and joint controller agreements?

EU-based firms are more likely to say that non-lawyers can negotiate agreements than US-based firms

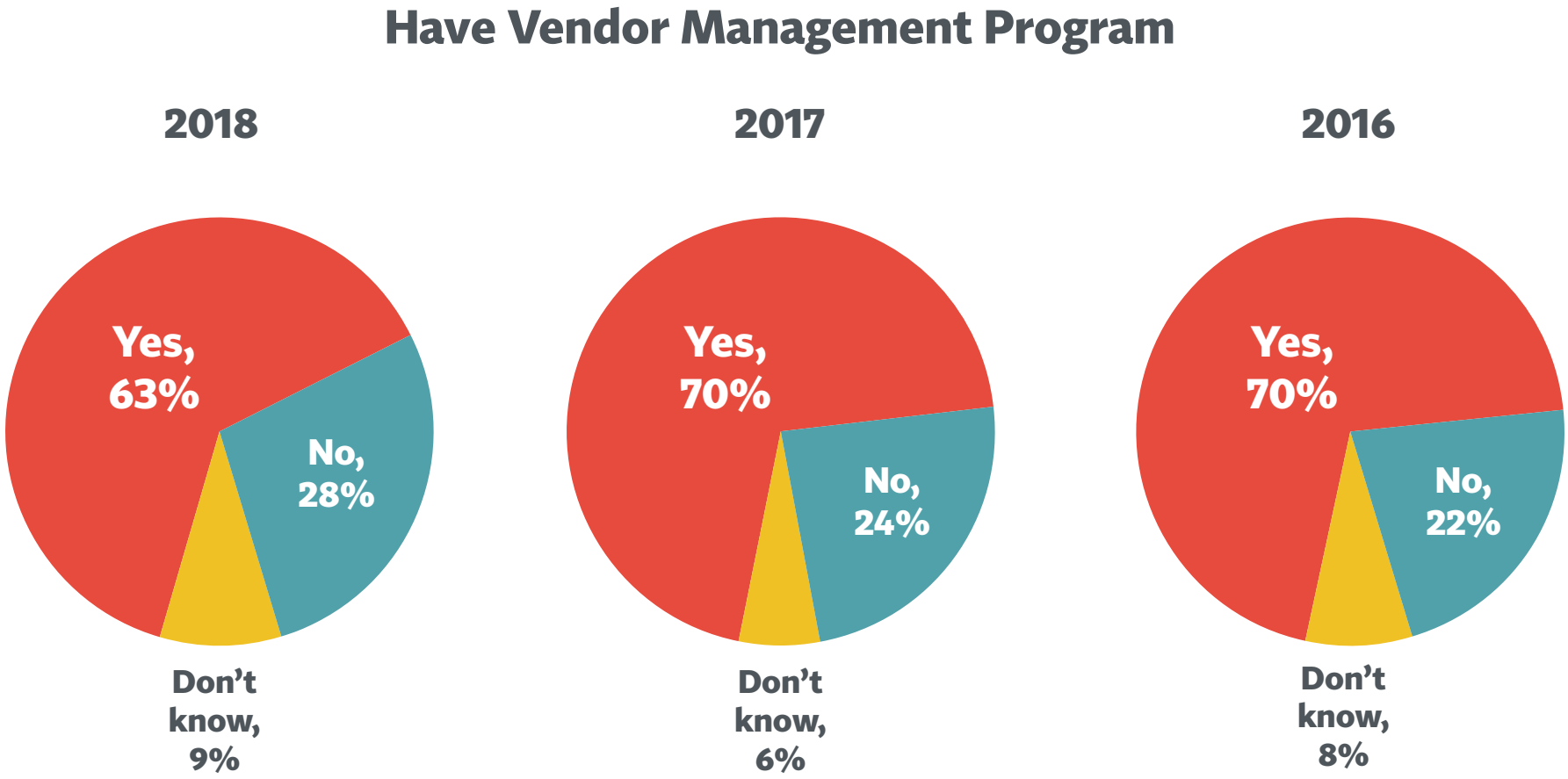
Whether Non-Lawyers Can Negotiate
(Base: Falls Under GDPR)



H10: In your company, can non-lawyers, including potentially the DPO, negotiate data processing and joint controller agreements?

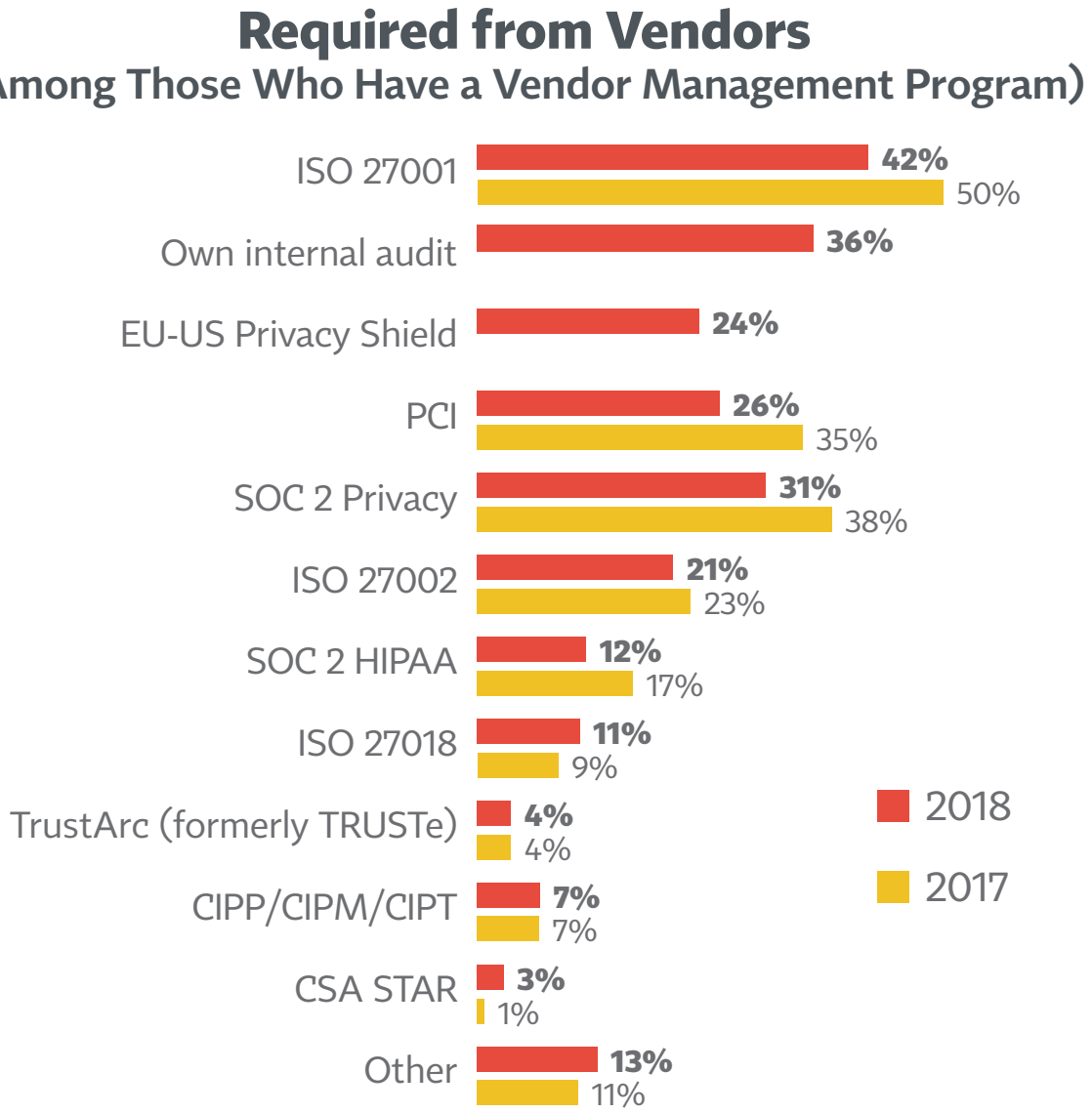
The proportion of firms with a vendor management program has dropped directionally since 2017

This corresponds with the overall drop in privacy program maturity level



K2: Does your company have a vendor management program designed to ensure the privacy and/or security practices of vendors will not threaten the integrity of your company's privacy standards?

For those with vendor management, ISO 27001 is still the most common certification required of vendors



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

US, Finance, and Tech firms are the most likely to have vendor management programs in place

BY GEOGRAPHY

	US	EU
Have vendor management program	**72%**	60%
Third party audits required		
SOC 2 Privacy	**42%**	18%
SOC 2 HIPAA	**17%**	7%

BY INDUSTRY

	Average	Finance	Health*	Tech
Have vendor management program	63%	**73%**	71%	**74%**
Third party audits required				
ISO 27001	42%	45%	28%	**54%**
Internal audit	36%	33%	**51%**	38%
EU-US Privacy Shield	24%	11%	14%	**36%**

Significantly higher than total

* Small sample size

Vendor management is also more common in the largest firms, and those with mature privacy programs

BY EMPLOYEE SIZE

	Under 5K	5–24.9K	25–74.9K*	75K+*
Have vendor management program	58%	56%	68%	**78%**

BY PROGRAM MATURITY

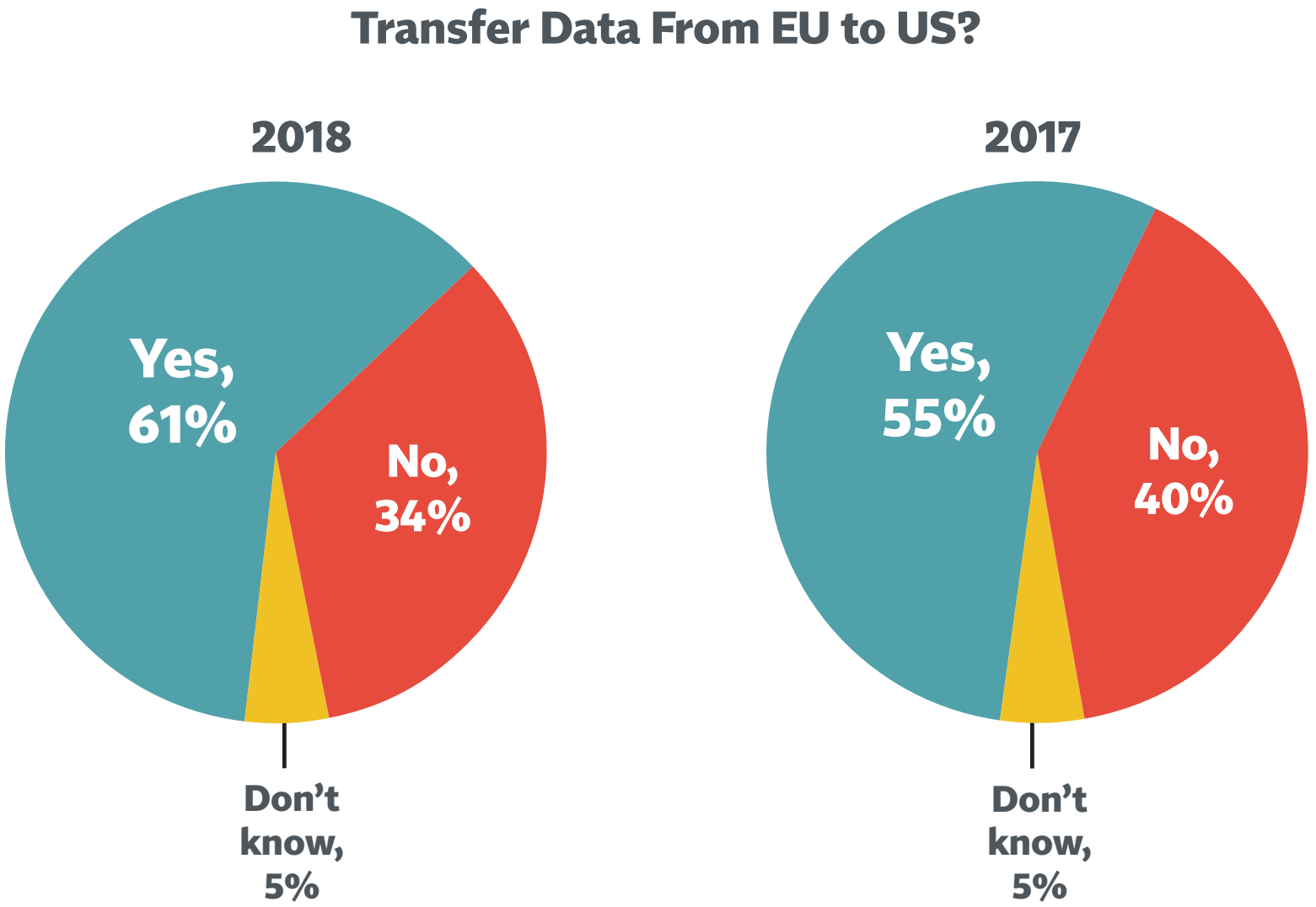
	Early/ Middle	Mature
Have vendor management program	61%	**87%**

Significantly higher than total

* Small sample size

Contents

6 in 10 organizations say they transfer data between the EU and US, slightly higher than in 2017

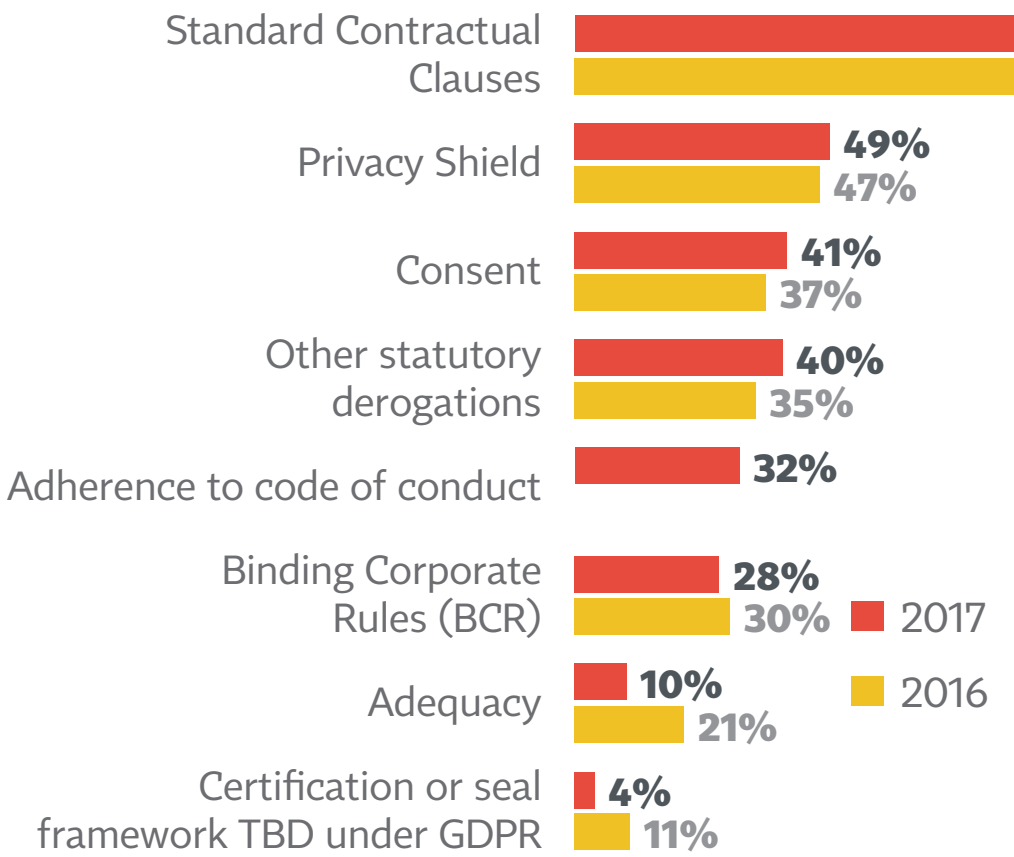


J1: Does your organization transfer personal information from the European Union to the United States?

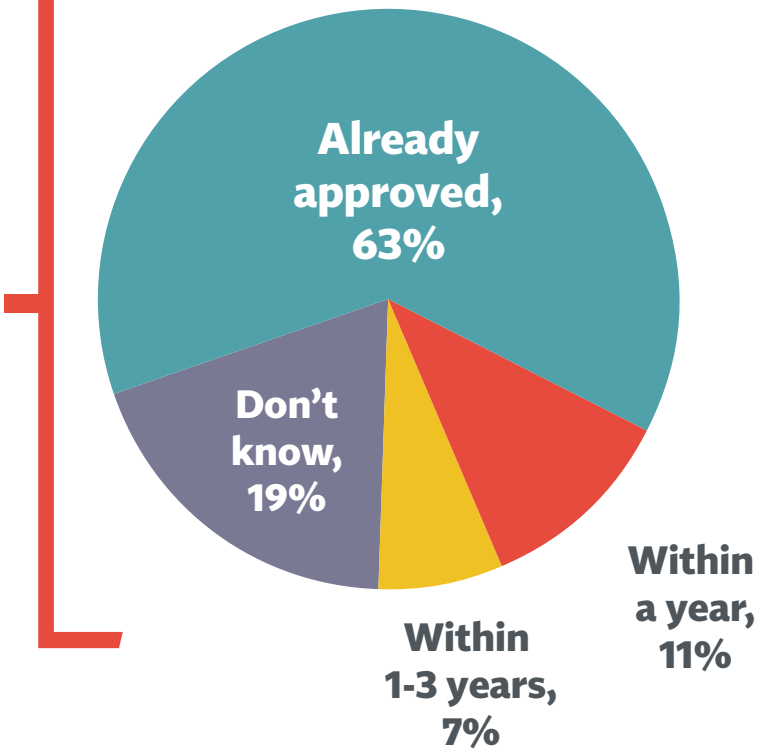
Standard contractual clauses remain by far the most popular data transmission mechanism

For those who cite BCR, two-in-three say their BCR application has already been approved

Data Transmission Mechanisms



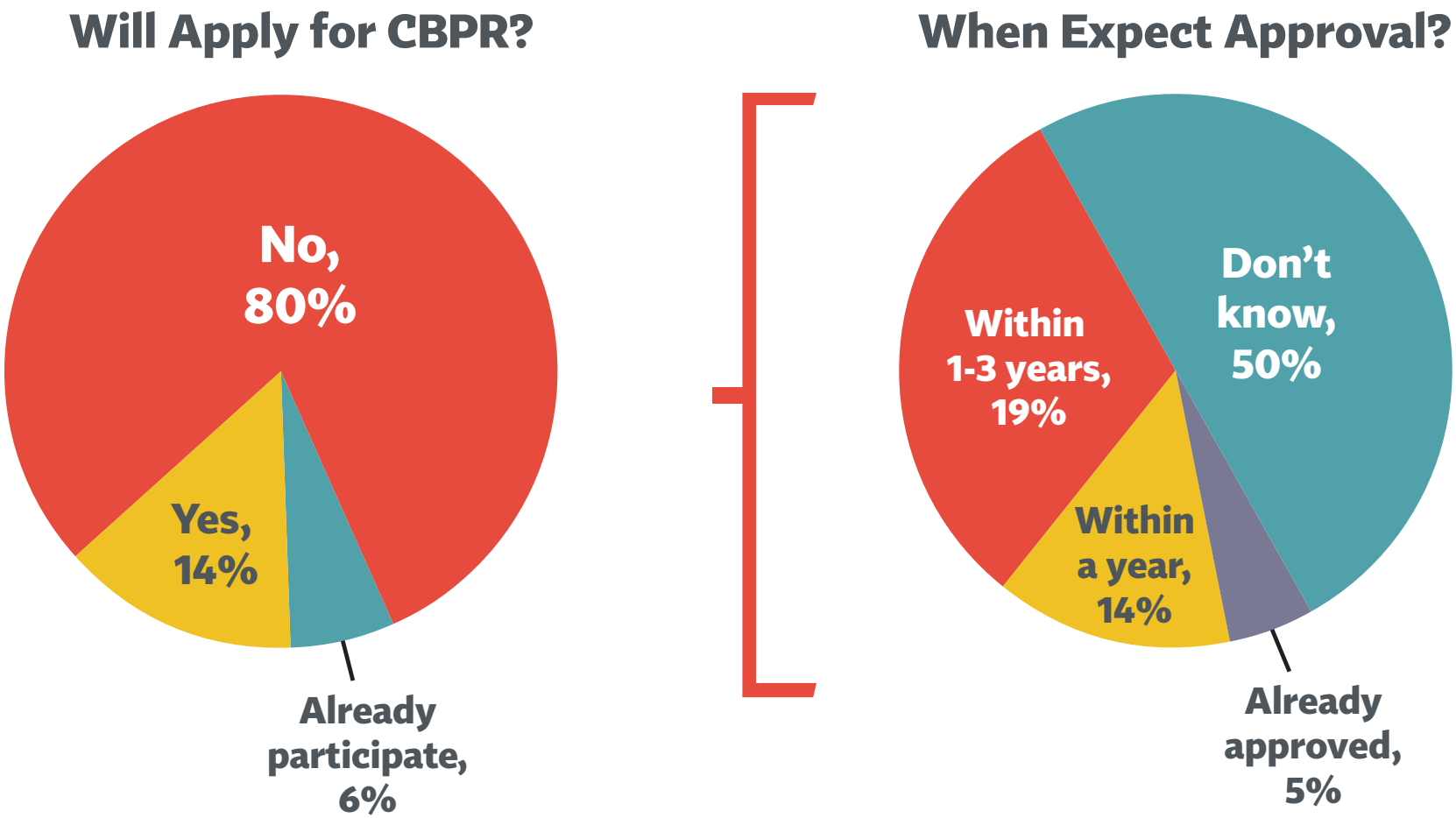
Expected BCR Approval



J2: What mechanism(s) does your company intend to use to transmit data to the U.S.?
J3: When do you expect your BCR application to be approved?

Similar to 2017, a small proportion of firms say they'll apply for CBPR

Half of those who will apply don't know when their application will be approved



K4: Will your organization apply for Cross Border Privacy Rules (CBPR) to transfer data in the APEC region?
K5: When do you expect your CBPR application to be approved?