IAPP-EY Annual Privacy Governance Report 2021

iapp

EY

Building a better working world

Introduction

This year's "Privacy Governance Report," produced in collaboration with EY and EY Law, analyzes the state of the privacy profession in 2021. It examines the ongoing effects of the COVID-19 pandemic on the privacy profession, including the evolution of remote/hybrid/office work, as well as expectations about the future of business travel, legal compliance issues related to the EU General Data Protection Regulation and California Consumer Privacy Act, as well as the progress of organizations in adapting to new laws, including the California Privacy Rights Act and other U.S. state laws, as well as Brazil's General Data Protection Law. It also details the organizational architecture of privacy teams, taking an in-depth look at the privacy leadership, reporting structures, and privacy staff and budgets. It covers the privacy team's core responsibilities, shifting priorities and efforts to benchmark their privacy programs. Finally, it examines the workflow around data subjects and processing vendors, answering questions ranging from how long it takes a typical organization to respond to a data subject request to what assurances most organizations require from vendors that handle their data.

The survey targeted privacy professionals around the world. To reach them, an online survey invitation was sent to subscribers of the IAPP's "Daily Dashboard" publication. A total of 473 surveys were completed.

By Müge Fazlioglu, CIPP/E, CIPP/US
IAPP Senior Westin Research Fellow

For privacy pros, this year has been anything but uneventful. In July, the power of the GDPR was on full display when Amazon disclosed that Luxembourg's National Commission for Data Protection imposed an unprecedented 746 million euro fine on it for alleged violations of the GDPR. Described as "arguably the most important GDPR decision issued," it is the biggest GDPR fine to date — eclipsing the French Commission nationale de l'informatique et des libertés' 50million euro fine against Google and more recently the Irish Data Protection Commission's 225 million euro fine against WhatsApp — and is more than the total of all other GDPR fines that have been imposed since the law went into effect.

Although the GDPR may dominate the headlines, other laws around the globe are shaping up to have as great if not more of an impact on privacy practices worldwide. In August, China adopted the Personal Information Protection Law, which is set to go into effect Nov. 1. Both similar and dissimilar to the GDPR, the passage of China's new privacy law comes just months after a major cybersecurity reform went through, promising more frequent enforcement against companies operating in China. Another privacy law impacting global businesses, South Africa's Protection of Personal Information Act came substantively into force July 1. All the developments also come on the heels of Brazil's passage last year of the LGPD, compliance with which we examine for the first time in this year's report.

At the state-level in the U.S., privacy laws continue to advance from passage to implementation and enforcement. As CCPA claims work their way through the courts, legislatures in Virginia and Colorado have added to the growing roster of U.S. state-level privacy legislation. Yet, without baseline federal privacy protections in place, the U.S. approach essentially "leaves it to companies to set the rules for privacy" for many new technologies. We see examples of this with recent privacy-centric initiatives rolled out by technology companies, such as Apple's App Tracking Transparency feature, Google's Privacy Budget and the pledge by tech companies to invest more in cybersecurity, all of which seek to address consumer privacy concerns even absent a federal, omnibus privacy law.

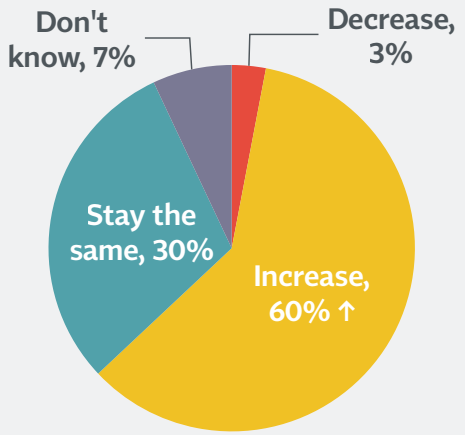
With so much going on and constantly changing in the world of privacy, we hope you find this year's "Privacy Governance Report" to provide a consistent, powerful benchmark for your privacy program operations and a unique source of insight into how the privacy profession is evolving today.

Contents

KEY FINDINGS

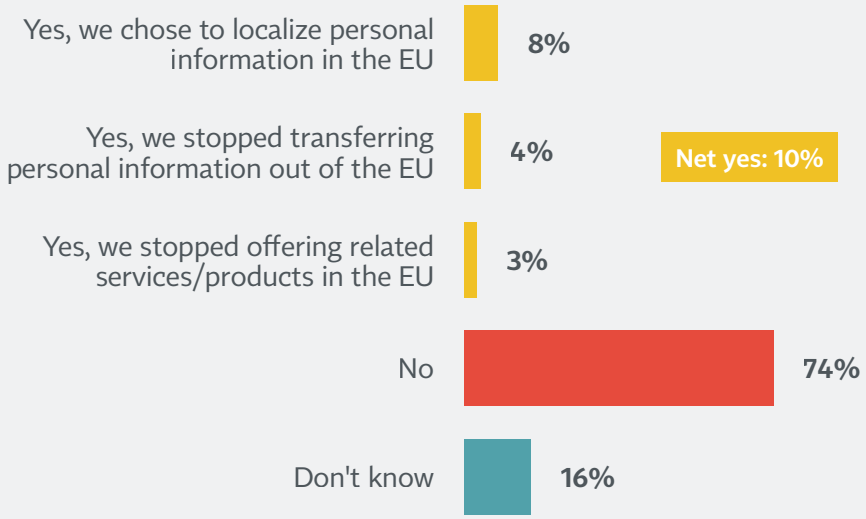
- Privacy budgets have increased significantly since last year, with the average privacy spend among organizations being $873,000 (and the median being $350,000). Six out of 10 privacy pros also expect their budget to increase over the next year, while almost none are anticipating cuts.
- Forty-five percent of respondent organizations are planning to hire at least one or two new privacy pros over the next six months.
- Complying with cross-border data transfer laws is rated by the majority of privacy pros as their most difficult task. Ten percent of respondents said their firms chose to localize data, stop transfers or halt related services as a result of the Court of Justice of the European Union's "Schrems II" decision.
- Regarding CCPA compliance, 26% of firms to which the law is applicable reported being in full compliance, while 41% reported being very compliant. Similarly, 20% of firms to which the GDPR is applicable rated themselves as fully compliant with the law, while 43% said they are very compliant. Meanwhile, nearly half of firms to which LGPD applies said they are either fully compliant (20%) or very compliant (26%) with Brazil's new privacy law.
- As has been true over the past few years, the topic most commonly reported by the privacy team to the board of directors is data breaches, which 76% of privacy teams reported to their boards. The next most reported topics are an organization's level of compliance with privacy and data protection laws (56%) and progress on privacy initiatives (52%).

In next 12 months, privacy budget will…
(Base: Director or higher)

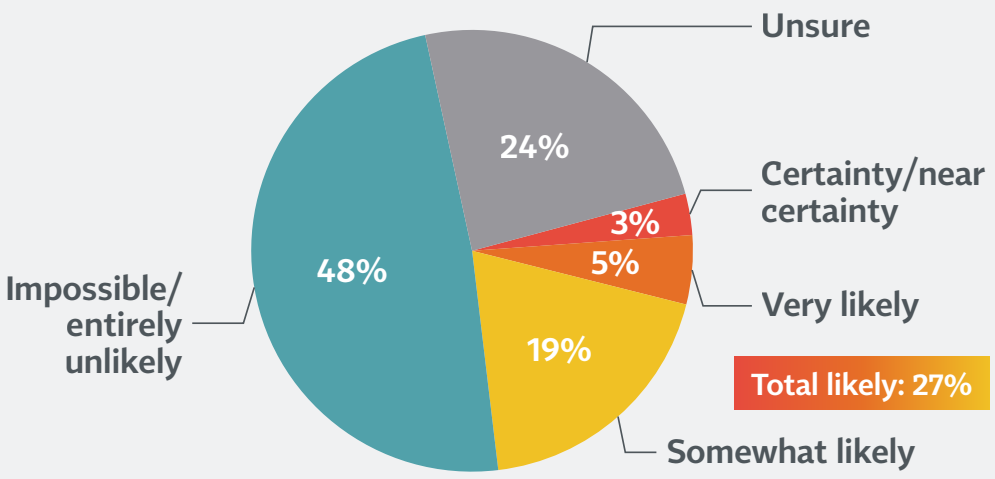


↑ Significantly different from 2020

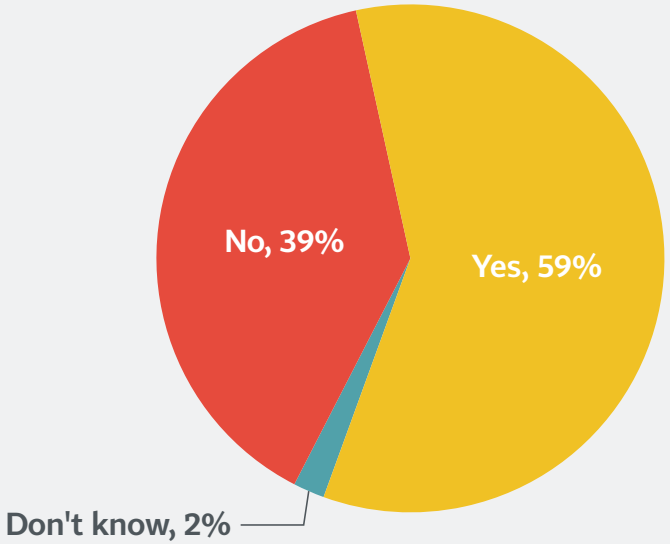
"Schrems II" decision
(Adds to more than 100% because respondents could choose more than one)



Likelihood of a COVID-19 vaccine passport requirement to return to work



Whether team is dedicated to handling DSRs



KEY FINDINGS, *continued*

- Twenty-two percent of employers were collecting employee vaccination records as of mid-2021. About 1 in 4 respondents rated it as at least somewhat likely their employer would adopt a vaccine passport system to bring employees back into the office.
- This year, 81% of privacy pros continue to work exclusively or mostly from home. By the end of the year, the bulk (78%) of privacy pros still expect to remain remote/hybrid workers. In a year's time, 82% of privacy pros expect to be mostly remote or some form of hybrid, dividing their working hours between home and office, suggesting expectations around remote/hybrid work will remain stable into 2022.
- Fewer than half of privacy pros expect to travel for work over the next six months, with most of these planning to do so only once or twice. By mid-2022, however, two-thirds expect they will have taken at least one or two business-related trips.
- Six in 10 organizations have a dedicated team in place for handling DSRs, with access requests and right-to-erasure requests being the two most common.
- Three in 4 privacy teams rely on some sort of automated technologies for tasks such as DSRs, data mapping, cookie consent/website scanning and other privacy-related responsibilities.

Contents

Executive Summary

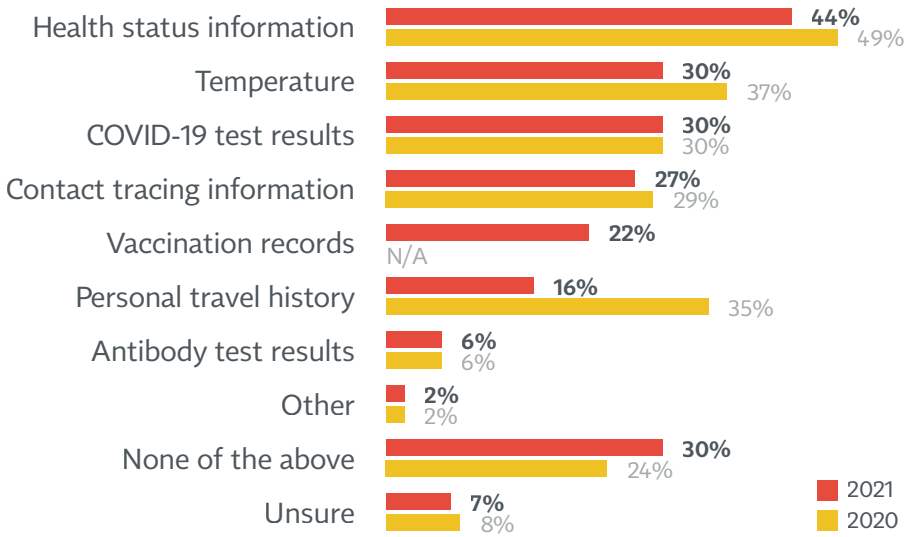
COVID-19: Employee data collection, work arrangements and business travel in the near future

Well into 2021, the COVID-19 situation remains fluid. While many employers had announced plans for their workforces to return to the office this year, many of these plans have been disrupted by the spread of the delta variant of COVID-19 and plateauing of vaccination rates. While much uncertainty remains regarding how COVID-19 will continue to impact the work of privacy pros, there are several things we know for sure.

First, fewer employers are collecting COVID-19-related health data from their employees this year compared to last, though 70% still does. In mid-2021, 44% of employers were still collecting some kind of health status information from their employees, with 30% collecting temperature information or COVID-19 test results and 27% collecting contact tracing information. More than 1 in 5 employers (22%) were also collecting vaccination records by mid-2021, a number that has likely increased into the latter half of 2021. Only 16% of employers were collecting data about their employees' personal travel, however, which is down from 35% in 2020, showing the reduced importance placed on this type of data to mitigate the spread of COVID-19.

Second, some businesses are encouraging or requiring vaccines among their employees as a prerequisite to return to the office. Yet, the adoption and use of COVID-19 vaccine passports is not without controversy and privacy implications. U.S. President Joe Biden's Sept. 9 Executive Order, which requires all federal employees and contractors — subject to exemptions — to be vaccinated against COVID-19, will shift the calculus for many employers. At the time of the survey in mid-2021, most businesses seemed unlikely to unilaterally implement such a formal requirement on their own for a return to the office. Although about 1 in 4 (27%) of privacy pros rated it as at least somewhat likely that their employer would require the adoption of some sort of vaccine passport system to bring employees back to the office, almost half (48%) said such a scenario was either entirely unlikely or implausible at that time. Another 1 in 4 privacy pros said they were uncertain about whether they would need a vaccine passport to return to the office. Nonetheless, given the changing regulatory landscape around COVID-19 vaccine mandates across the federal, state and local level, businesses must be aware of how these various rules apply to them.

Data collected from employees during COVID-19



Third, into mid-2021, the majority of privacy pros (81%) continued to work mostly from home due to the COVID-19 pandemic. While 58% said they were working exclusively from home, another 23% said they were mostly working from home. Yet, the proportion of those exclusively remote is down to 58% from 71% in 2020, suggesting the norm is shifting from fully remote to hybrid work in 2021. Moreover, only 5% of privacy pros reported working exclusively or mostly in an office with other employees, meaning 95% of privacy pros were either fully remote or working in some form of hybrid arrangement.

The bulk of privacy pros expects to remain remote/hybrid workers through 2021. That is, nearly 7 in 10 expect to either work mostly from home (32%) or split their working hours between home and the office (36%), with only about 10% expecting to be exclusively or mostly working in an office by the end of this year.

Expectations about hybrid work in 2022 are similar: 82% of respondents see themselves as having some sort of hybrid work arrangement next year, with 25% expecting to be working mostly from home, 11% expecting to be working mostly in an office, and 46% expecting to be working equally between home and office.

Lastly, business travel expectations only appear to pick up substantially in early to mid-2022. Over the next six months, fewer than half of privacy pros expects to travel for work, with most of these planning to do so only once or twice. The other half (46%) does not expect to engage in any business travel at all this year. Over the next 6 to 12 months, however, the proportion expecting at least one work-related trip increases to two-thirds. More than one-third (35%) of privacy pros expect to travel once or twice for work by mid-2022, with about the same proportion (31%) expecting to travel at least a few times by then.

Compliance: GDPR, CCPA/CPRA and beyond

As privacy and data protection laws proliferate around the world and become ever more complicated, issues of legal compliance remain at the forefront for privacy pros. Yet, we see firms taking divergent strategic approaches to global compliance: While the largest group, nearly half (48%), has a single global privacy strategy, a significant number of firms (32%) categorize their data subjects by jurisdiction and handle their data according to local, applicable laws. The remaining 17% of firms pursue a local strategy toward their data subjects since they all reside primarily in one location.

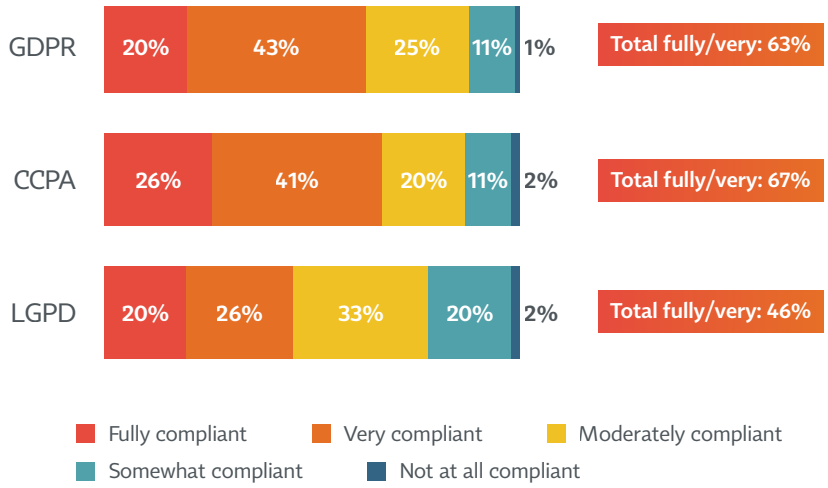
Despite the complexities introduced by COVID-19, perhaps no issue has been more complicated for privacy pros in recent years than the CJEU's ruling in the C-311/18 ("Schrems II") case, which invalidated the EU-U.S. Privacy Shield agreement and drew into question the legality of standard contractual clauses as a means of transferring data outside the European Union. Indeed, nearly 6 in 10 privacy pros said complying with cross-border data transfer laws is their most difficult task.

The ruling impacted most businesses, as more than 7 in 10 privacy pros work at a firm that transfers data from the EU to a third country. Nearly all of them (94%) now use SCCs as the primary legal means for doing so. A notable number of firms also rely on "supplementary measures" or additional safeguards, either technical (38%), contractual (36%) or policy-based (26%), to complement their use of SCCs. Other

widely employed bases for data transfers out of the EU include adequacy decisions (39% of businesses that transfer data out of the EU rely on them) and consent (25%).

SCCs have been the subject of much focus and debate in the aftermath of the CJEU's decision. As our survey confirms, most businesses that transfer data out of the EU have either continued to rely on or switched to using SCCs, which were updated by the European Commission in June. However, 10% of such firms have made a major change, such as localizing data or halting their data transfers, because of the CJEU's "Schrems II" decision. Such changes will undoubtedly impact global trade and growth. One model, developed in a report for DIGITALEUROPE, forecasts that a moderately restrictive policy on data flows — one in which the EU is unable to rely on GDPR data transfer mechanisms — will lead to a 4% reduction in EU exports and 1% reduction in gross domestic product annually. By 2030, losses would amount to 1.3 trillion euros and 1.3 million jobs across small and large enterprises.

Compliance with GDPR, CCPA and LGPD
(Base: Law applies)



We also asked for the first time this year about data and technology controls firms have to restrict the transfer, access or storage of data by jurisdiction, finding that 4 in 10 firms said they have some type in place. Within this subgroup of firms, the most common data control was a data center in a country requiring localization, which 55% said they utilize. The next most commonly used data control were firewalls based on origin and destination IP address, which 52% reported using. Hybrid cloud (45%), geo-restricted access (44%) and data flow blocking (27%) are also used by a significant number of business as data control mechanisms.

In terms of legal compliance more generally, we found variation across the GDPR, CCPA and LGPD. While more than half (51%) of respondents rated themselves very or fully compliant with the GDPR, a smaller number (41%) said the same for CCPA, while the fewest (21%) said so for the LGPD. Yet, part of this disparity comes from differences in the scope of these laws and the number of businesses to which each applies, with the GDPR, which has been in place the longest of the three, having the broadest global reach by comparison to the other two.

When excluding those firms to which each law does not apply, we see a greater proportion of respondents rated themselves as fully or very compliant with the CCPA when compared to the GDPR and LGPD. Of the firms to which CCPA is applicable, 26% reported being in full compliance, while 41% reported being very compliant. This compares to 20% of applicable firms that rated themselves as fully compliant with the GDPR, and 43% that said they are very compliant, a difference of about 4% in the fully/very compliant joint category. Meanwhile, nearly half of firms to which the LGPD applies said they are either fully compliant (20%) or very compliant (26%) with Brazil's new law.

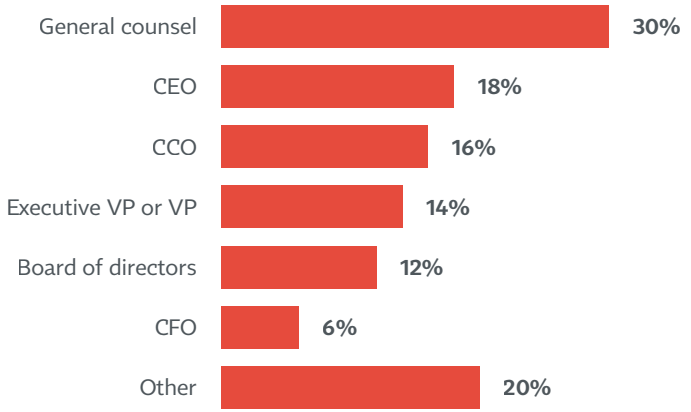
Yet, firms with CCPA compliance programs were dealt a curveball late last year, when the CPRA ballot initiative was approved by California voters. As the law is set to go into effect in January 2023, more than one-third said they are currently fully (8%) or very prepared (29%) for the entry into force of California's newest privacy law. Twenty-two percent feels only somewhat prepared, while 6% feels barely or not at all prepared, indicating a large gap in CPRA preparedness across organizations.

Privacy leadership

Due to businesses' increased reliance on customer data to power their programs, services and insights, organizations must incorporate privacy into their overall data strategy. Privacy leaders thus serve a critical role in helping organizations fulfill their mission and work within and across multiple organizational teams. Within the majority (57%) of organizations, the privacy function sits with the legal team. For most other organizations, the work of privacy sits within the information security, information technology, regulatory compliance or corporate ethics department, or within a separate privacy and data protection department.

Who leads these privacy teams? The most common job title for an organization's privacy leader is chief privacy officer, who is the leader in 32% of organizations. A data protection officer is the lead privacy position in 21% of organizations, although in the EU, the privacy leader is much more likely to be the DPO than in the U.S., where fewer organizations have a DPO. The director of privacy is the head of privacy in another 12% of organizations. Other common job titles for an organization's privacy leader are privacy officer (5%), lead privacy counsel (3%) and chief information security officer (2%).

To whom privacy leader reports



Looking at the position of various roles relative to the privacy leader within an organization, we see privacy leaders are frequently the same as or in an equivalent position to the CPO (in 54% of organizations), DPO (in 51% of organizations) or CISO (in 48% of organizations). Privacy leaders, however, tend to be junior to chief technology officers (54% of CTOs are senior to the privacy leader), chief information officer (47% of CIOs are senior to the privacy leader, while only 4% of PLs are senior to the CIO) and chief compliance officers (41% of CCOs are senior to the privacy leader, while only 3% of PLs are senior to the CCO).

Nearly half of privacy leaders report to either the general counsel (30%) or CEO (18%). Notable percentages also report to the CCO (16%), an executive or vice president (14%), the board of directors (12%), or the chief financial officer (6%). There are some differences in reporting across firms based on their size or location: Privacy leaders working at smaller organizations are more likely than those at larger ones to report directly to the CEO. In addition, while EU privacy leaders are more likely to report to the CEO or board, those in the U.S. are more likely to report to the general counsel.

This year's survey found 74% of firms have a DPO, with 41% having only one DPO, 18% having more than one and 15% outsourcing the role. Moreover, 6 in 10 organizations with an in-house DPO said the role handles matters across all countries, while 4 in 10 of them have country-specific DPOs. The countries DPOs are most likely to work specific to are Germany (59%), the U.K. (34%) and Brazil (25%), although significant numbers are also assigned to France (21%), the U.S. (17%) and Italy (17%). Given the impact of major geopolitical developments, such as Brexit, as well as the introduction of new privacy and data protection laws around the globe, including in countries such as Brazil, many organizations are finding the need for their DPOs to specialize in the legal compliance issues within a specific country.

Privacy staff and budget

Demonstrating the increasing importance organizations are placing on the privacy function, overall privacy spending has increased significantly since last year, with the typical (median) organization's privacy budget being $350,000. This follows the upward trend seen over the past few years, with the median privacy budget in 2020 being $300,000 and the median firm's privacy spend in 2019 totaling $200,000. Average privacy spend has also been growing dramatically year-over-year, rising 29% from 2020 to 2021 after having increased by about 9% from 2019 to 2020. Unsurprisingly, the largest firms, as measured by either employee size or total revenue, spend significantly more on privacy than their smaller peers.

Estimated privacy spend
(Base: Director or higher)

TOTAL PRIVACY SPEND
2021 MEAN: $873,000
2020 MEAN: $676,000
2019 MEAN: $622,000
2021 MEDIAN: $350,000
2020 MEDIAN: $300,000
2019 MEDIAN: $200,000

Regarding how privacy budgets are allocated, the majority (57%) goes toward salaries and travel. Moreover, the share of the privacy budget going to salaries/travel has increased 6 percentage points since last year. Other significant portions of the total privacy spend go to outside counsel (11%), technology and tools (11%), internal training (6%), consulting services (6%), and professional development (5%). The privacy budgeting decisions are most likely to be made by general counsels (38%), CPOs (31%), DPOs (12%) or CISOs (9%).

When asked whether they believe their privacy budget is sufficient to meet their needs, the bulk of respondents (63%) said it is less than sufficient (45%: somewhat less than sufficient, 18%: much less than sufficient). Meanwhile, 35% said their privacy budget is sufficient, and 4% said it is more than what they need. Overall, then, about 6 in 10 privacy pros said their privacy budget is less than sufficient to meet their team's needs, indicating there is room for better alignment before organizations face even greater regulatory and compliance costs down the road.

Yet, looking ahead, 6 in 10 privacy pros expect their budget to increase over the next 12 months, while relatively few expect it to decrease over that time. On average, those expecting their budget to increase think it will increase somewhere

between 20% and 32%, while those expecting a decrease expect to see it drop somewhere between 20% and 22%. Among those expecting a budget increase, most think the extra funds will go to salaries, while the few who do expect a decrease foresee cuts to their consulting expenses.

The picture is also relatively bright from a staffing perspective. Despite the disruption to business-as-usual brought about by the COVID-19 pandemic (e.g., supply-chain chokepoints, shifts to hybrid/remote work, less business-related travel), most companies seem poised to expand their privacy workforces. When asked about future hiring trends, 45% of privacy pros at the director level or higher said they expect their organizations to hire more privacy staff over the next six months. Of these, most (74%) plan to hire for one or two positions, while 18% expects to hire between three to five people, and 6% expect to hire six or more privacy pros.

As of mid-2021, companies have an average of 18 full- or part-time staff working on privacy, with more in the EU (average: 9 full time, 12 part time) than in the U.S. (average: 6 full time, 11 part time). Naturally, privacy staff sizes differ significantly by firm size, with the largest firms relying much more on part-time staff than smaller firms. Privacy staff numbers are also largest in regulated firms and those serving both consumers and other businesses.

Responsibilities of the privacy team

While we know the work of privacy pros is dynamic and evolving in response to global developments, this report distills the core set of responsibilities that lie within the privacy team. Respondents were provided with a list of 30 different tasks and asked to choose all for which they personally or someone else on the privacy team is responsible. These tasks concern things from employee privacy awareness training to legal compliance, redress and consumer outreach. Each responsibility varies in terms of its centrality to the typical privacy team's overall mission.

Ninety percent or more of privacy teams are responsible for:

- Privacy policies, procedures and governance (99%)
- Companywide privacy-related awareness and training (97%)
- Incident response (96%)
- Legislative development tracking around privacy and data protection (96%)
- Privacy issues with existing products and services (96%)
- Privacy impact or data protection assessments (95%)
- Privacy-related communications (95%)
- Design and implementation of privacy controls (95%)
- DSAR processing (93%)
- Privacy-related investigations (92%)
- Participation in data-related internal committees (92%)
- Privacy-related monitoring (92%)
- Privacy-related vendor management (90%)
- Data inventory and mapping (90%)

continued on xiv

However, not all privacy teams are the same, and many factors — from the industry they work in to the size of the organization and where it is located — can shape the responsibilities its privacy team must fulfill. For example, U.S.-based firms are more likely than EU firms to work with vendors, undertake compliance for the CCPA and LGPD, and measure consumer sentiment. Meanwhile, EU-based organizations are significantly more likely to carry out GDPR compliance tasks (98%) than are U.S.-based firms (83%).

Overall, the smallest firms by revenue and employee size reported having fewer privacy responsibilities than the largest firms. For instance, while about 92% to 94% of companies with revenues over $1 billion utilize privacy program metrics, only 77% to 85% of companies with revenues under $1 billion do so.

The survey results indicate that privacy programs are maturing, and privacy work is an increasing share of the total work that respondents do. This year, respondents said on average that privacy work accounts for 76% of the time they spend on their jobs, compared to 71% in 2018. As has been true in the past several years, about 4 in 10 study respondents said they have no other job responsibilities than privacy. Yet, privacy pros at the smallest firms spend less of their time on privacy than privacy pros working at larger firms. Also, 6 in 10 firms have had a privacy program for 3-9 years, up from just half in 2020.

Privacy priorities, reporting and benchmarking

Amid the barrage of legal, political and social developments affecting privacy, most privacy team priorities continue to center around legal compliance. We have seen that since at least 2018, compliance with the GDPR has been the top priority for the greatest number of organizations, with 32% of privacy teams reporting it as their biggest responsibility. In addition, 12% said the privacy team's top job is to comply with the CCPA/CPRA or other U.S. state privacy laws.

Yet, with the further development of privacy laws around the world, privacy priorities are increasingly globally oriented: 18% said regulatory compliance outside of EU/U.S. privacy laws is their top priority. Another 15% reported

At least two-thirds of privacy teams are responsible for:

- Privacy by design in product development (89%)
- Proper cross-border data transfer (89%)
- Development and training specifically of privacy staff (89%)
- Privacy program metrics (collection, analysis and/or reporting) (86%)
- Privacy-related legal counsel (internal) (85%)
- Compliance with the GDPR (84%)
- Ethical decision-making around data use (84%)
- Privacy audits (82%)
- Privacy-related subscriptions and publications (81%)
- Privacy-enhancing software (77%)
- Compliance with the CCPA (71%)
- Redress and consumer outreach (70%)

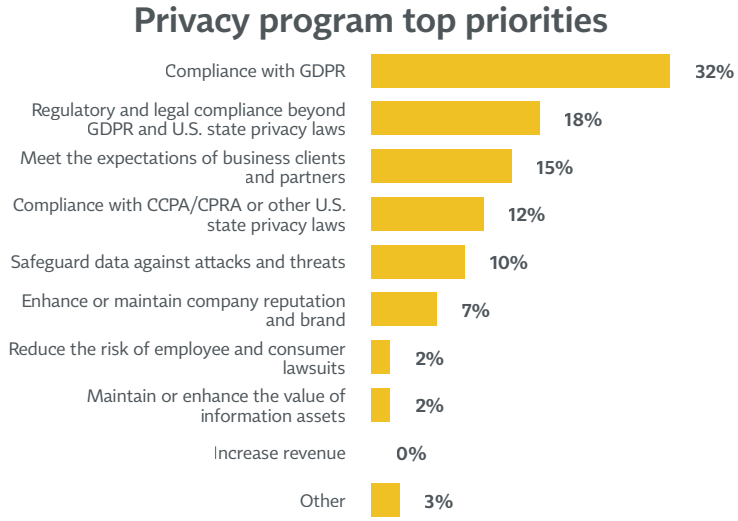
continued on xv

meeting the expectations of business clients and partners is their top priority, while 10% said safeguarding the business against threats and attacks is their top concern.

Different priorities are visible across the jurisdictions in which businesses operate. For example, whereas nearly 7 in 10 EU firms rated GDPR compliance as their top priority, only 2 in 10 U.S.-based firms did so. Unsurprisingly, 19% of U.S.-based organizations considered compliance with U.S. state laws, such as the CCPA/CPRA, to be their top priority, while no EU-based organizations did. Regulatory compliance beyond the GDPR and U.S. state privacy laws, meeting the expectations of business clients and partners, and safeguarding data against attacks and threats were all more likely to be the top priority for U.S.-based organizations than EU-based ones.

To measure the effectiveness of their programs and ability to reach their goals, privacy teams rely on a variety of benchmarks. More than 1 in 4 organizations use NIST's Privacy Framework (28%) or ISO 27701 (26%) as benchmarks. In addition, 17% reported using another framework developed by a third party, while 1 in 10 said they use IAPP's "Privacy Governance Report."

Some of the most common metrics for benchmarking, used by more than half of privacy teams, include incident response metrics (58%), privacy or data protection impact



assessments (56%), training and awareness metrics (56%), and DSAR metrics (55%). Substantial numbers of privacy teams also use data subject deletion request metrics (42%), third-party risk assessments (37%) and data subject do-not-sell request metrics (19%). Lastly, about 1 in 10 use automation and scalability or customer or brand impact assessments, while 23% reported using no formal metric at all to measure their privacy program's performance.

As in previous years, the topic most commonly reported by the privacy team to the organization's board of directors is data breaches, which 76% of privacy teams said they report at the board level. More than half also report to the board on the status of compliance with data

Lastly, at least half of privacy teams are responsible for:

- ➔ Accelerating digital transformation and digital capabilities (63%)
- ➔ Monitoring customer sentiment about the organization's privacy approach (63%)
- ➔ Overseeing privacy-related web certification and seals (61%)
- ➔ Guiding compliance with Brazil's LGPD (55%)

protection or privacy laws (56%), progress on privacy initiatives (52%) or privacy program key performance indicators (51%). Developments in privacy compliance (41%), privacy litigation (40%), and future trends or threats (38%) are also topics commonly reported to the board.

The question of what topics are reported and to which stakeholders is an important one, with ramifications for both a company's reputation and bottom line, especially for public companies. Just over 4 in 10 firms in the sample are publicly traded companies, essentially unchanged since last year. Importantly, about half of these firms include privacy issues in disclosures and reports; most said both compliance and data breach risks are reported.

Data subject requests

With the massive amounts of personal data held by companies and the expansion of their legal obligations, requests from consumers to access, correct or delete their data are taking up a greater share of privacy operations. Indeed, 6 in 10 organizations said they now have a dedicated team in place for handling DSRs.

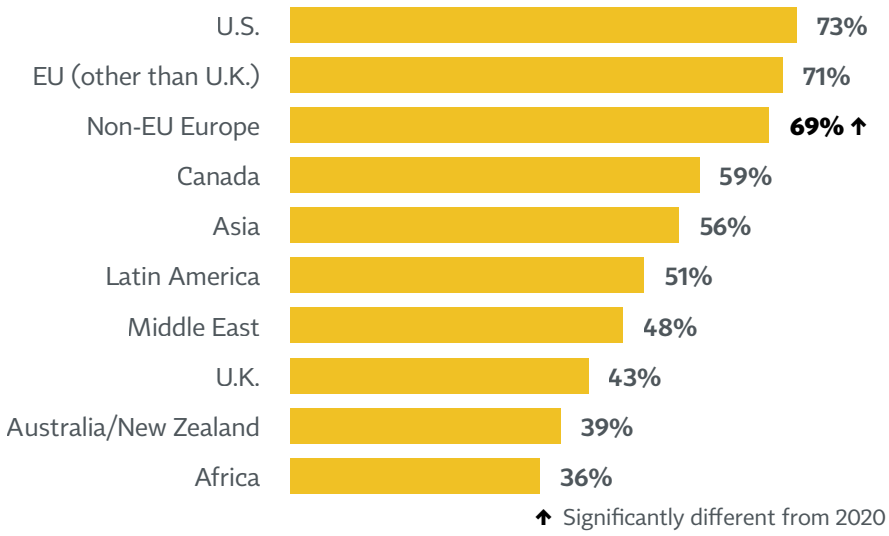
To make matters more complicated, this data is coming from consumers located all around the world, creating a patchwork of national legal standards that businesses must comply with to operate globally. About 3 in 4 firms collect information from data subjects in the U.S., 7 in 10 collect information from data subjects in Europe (EU or non-EU), and about half of businesses collect personal information from data subjects in Asia (56%) or the Middle East (46%). Another 39% collects information from data subjects in Australia or New Zealand and 36% from data subjects in Africa.

Access requests and right-to-erasure requests are the most common DSRs across firms, with at least two-thirds receiving them. Correction/rectification requests (28%), do-not-sell requests (28%), processing restrictions and objections (24%), and data portability requests (14%) are other common DSRs that many businesses receive. Moreover, 11% reported receiving no DSRs over the past year.

Most firms (58%) said they usually take at least a few days to respond to DSRs, with nearly 4 in 10 saying they take at least a week. Meanwhile, about 1 in 5 (22%) organizations are able to process DSRs in less than a day or two. More than half of organizations handle DSRs manually, while about 1 in 3 have either partially (32%) or fully (3%) automated the process.

When asked about the most challenging issue related to the DSR response process, nearly half (47%) said locating an individual's data within the organization was the most

Where company's data subjects reside

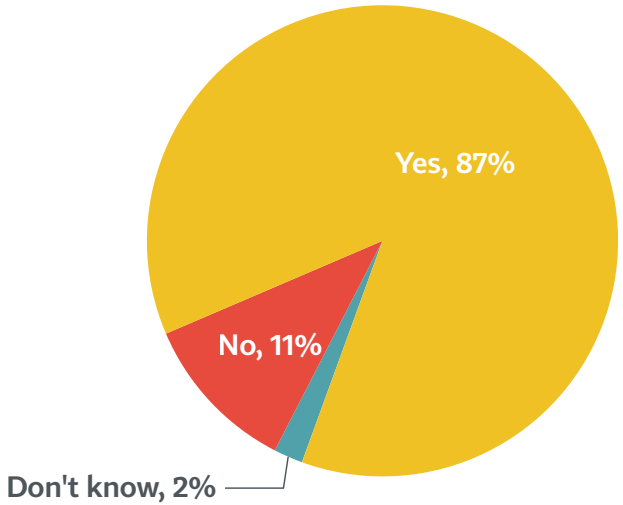


difficult thing to deal with. One-third said the biggest DSR-related hurdle was monitoring the practices of third parties with which their organization shares data. And about 1 in 5 identified the top challenge as either ensuring data minimization (21%), minimizing the impact of data deletion on the business (20%), anonymizing data (19%), developing an easy-to-use, centralized opt-out tool (18%), or verifying the data subject's identity (17%).

Data-processing vendors

As the growth of IAPP's "Privacy Tech Vendor Report" over the past several years has shown, vendors are becoming increasingly central to privacy operations. Given that the vast majority of firms (87%) use outside firms to process personal data, the network of vendors that firms deal with on a regular basis has become critical. To ensure vendors are meeting their commitments, most organizations rely on contractual assurances (90%), the completion of a questionnaire (67%) or documentation from a third-party audit (48%) to keep them accountable.

Use of other companies to process data



Some of the most common audits or certifications that organizations require from entities that process their data include ISO 27001 (28%), SOC2 Privacy (22%) or some internally developed assessment (17%). A notable number of organizations also require their vendors to adhere to PCI (13%), ISO 27002 (8%) or the NIST Privacy Framework (5%). U.S. firms are more likely than EU firms to require a variety of certifications, including SOC2 Privacy and NIST's Privacy Framework, from their data processors.

Across all privacy functions, about 3 in 4 firms have some sort of automated privacy technologies in place, with most (41%) having purchased them. Organizations most frequently use privacy technologies for DSRs (40%), data mapping (39%), cookie consent/website scanning (39%), privacy and data protection impact assessments (37%), consent management (35%), and third-party risk management (32%). In addition, organizations reported using third-party service providers most often for cookie consent/website scanning (36%), data mapping/inventory (23%), privacy and data protection impact assessments (20%), third-party risk management (19%), consent management (18%), and DSRs (17%).

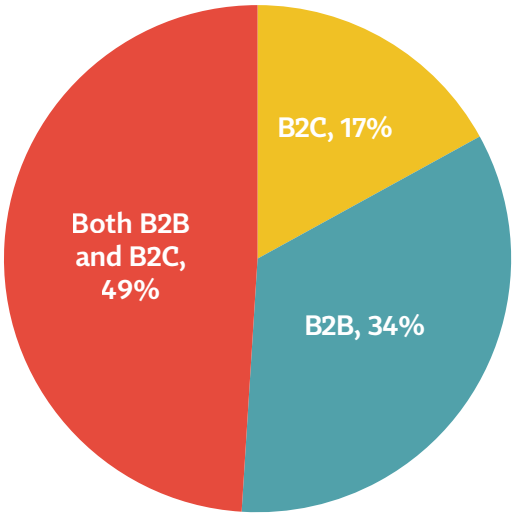
Demographics and firmographics

An analysis of the demographic and firmographic characteristics of the respondents provides a look at a cross-section of the privacy profession in terms of geography, industry, organization size and type, job titles, credentials, authority levels, and gender.

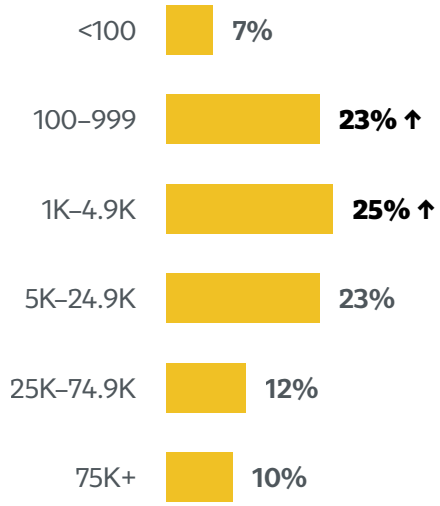
In terms of the location of the organizations at which they work, the vast majority, or about 8 in 10 respondents, work for a firm headquartered in either the U.S. (54%), EU (16%) or U.K. (10%). The rest work for organizations based in Canada (8%), Australia/New

Company profiles

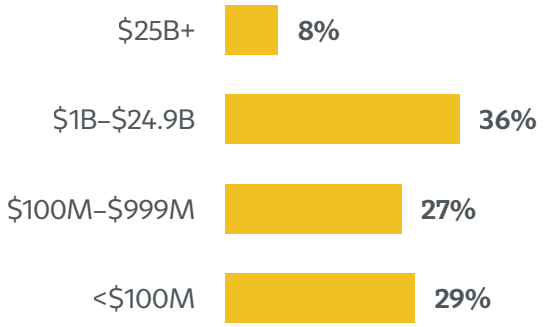
Business type



Industry sector



Employees



↑ Significantly different from 2020

Zealand (3%), another non-EU country in Europe (2%) or some other country (8%). In addition, about half (47%) of respondents are also personally based in the U.S., 19% in the EU and 14% in the U.K.

As in prior years, privacy pros working in technology, telecommunications and software make up the largest industry group (23%). The next largest sector respondents came from was finance/insurance (18%), followed by health care/pharma (11%) and government (7%). Other industries that make up notable portions of the respondent pool include energy/mining/utilities (4%), education and academia (4%), retail (3%), transportation (3%), and media and entertainment (3%).

Regarding the size of organizations they work for, respondents are distributed fairly evenly across small, medium and large firms. Overall, 30% of respondents work at organizations with fewer than 1,000 employees, 25% with between 1,000 and 5,000 employees, and 45% with 5,000 employees or more. Respondents also come from organizations of varying revenues: 29% at firms with under $100 million in annual revenue, 27% at firms with between $100 million and $999 million, 36% at firms earning between $1 billion and $24.9 billion, and 8% at firms earning $25 billion or more in annual revenue.

Half of respondents held one of three job titles: data protection officer (25%), privacy manager (13%) or chief privacy officer (12%). Other common job titles for respondents included privacy officer (12%), director of privacy (11%), privacy analyst (7%), privacy counsel (7%) and data privacy manager (6%). One-third of privacy pros are at the manager/supervisor level, while another one-fourth are directors. Sizeable numbers also work at the solutions architect/coordinator/analyst level (10%), associate/assistant counsel level (10%), C-suite level (10%) and general/lead counsel level (6%).

Two-thirds (67%) of survey respondents this year have a CIPP credential, up from an average of about 59% over the past three years. The most commonly held credential is CIPP/E, which is held by 44% of respondents, followed by CIPM, held by 38% of respondents. CIPP/US was the third most common, held by 30% of respondents. Sizeable groups of respondents also held CIPT (10%), CIPP/C (8%), CISSP (6%) and CISM (6%). Regarding gender, survey participants this year were roughly split evenly between males and females, with 2% identifying as nonbinary.

Conclusion

This year's "Privacy Governance Report" continued its benchmarking of the privacy profession, examining the core functions and responsibilities of the privacy team, the roles and composition of the privacy leadership, privacy staff and budgeting, and issues such as handling DSRs and maintaining relationships with data-processing vendors. Moreover, it considered the impact of the changing legal landscape and ongoing effects of the COVID-19 pandemic on the privacy world writ large.

Into its second year, the COVID-19 pandemic continues to impact the work of businesses, in general, and privacy pros, in particular. As they have since the onset of the pandemic, the majority of privacy pros continue to work exclusively or mostly from home this year. Moreover, at the end of the year, the bulk of privacy pros expect to remain hybrid workers. Projecting into 2022, expectations for hybrid work persist. Business travel expectations appear muted throughout the rest of 2021 but poised to tick up by early to mid-2022. Yet, given this data was collected in June/July and individual sentiment regarding various COVID-19 issues is fast-changing, expectations may have shifted significantly since then.

Demonstrating the increasing importance organizations are placing on the privacy function, overall privacy spending has increased significantly since last year, with the typical (median) organization's privacy budget being $350,000. And, looking ahead, most privacy pros expect their budget to increase over the next 12 months, while almost none expect it to decrease over that time.

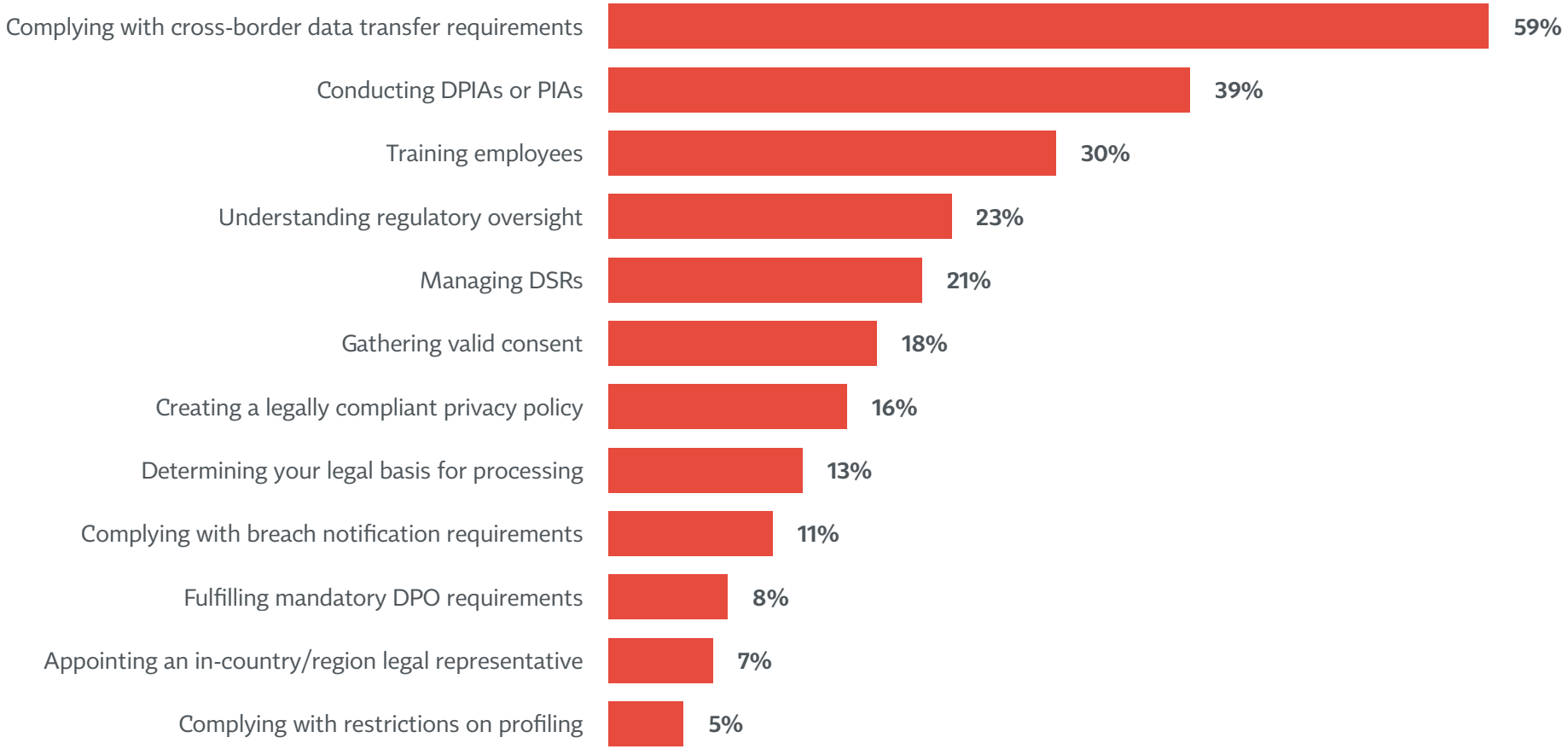
Compliance with the GDPR, CCPA/CPRA and other U.S. state privacy laws, as well as other global laws, has been a top priority for most privacy teams over the past year. Furthermore, the majority of privacy pros said complying with cross-border data transfer laws is their most difficult task, especially in light of last year's ruling by the CJEU in "Schrems II."

These findings demonstrate the privacy function within organizations and the privacy profession, in general, continues to grow, not only in terms of privacy staff numbers and budgets, but also in the amount and complexity of their daily responsibilities. An increasing number of privacy laws — both at the state level in the U.S., as well as at the national level around the world — make privacy operations increasingly central to what an organization does. Despite the uncertainties, volatility and disruptions over the past year and a half, privacy is more critical than ever to consumers, regulators and businesses alike.

Contents

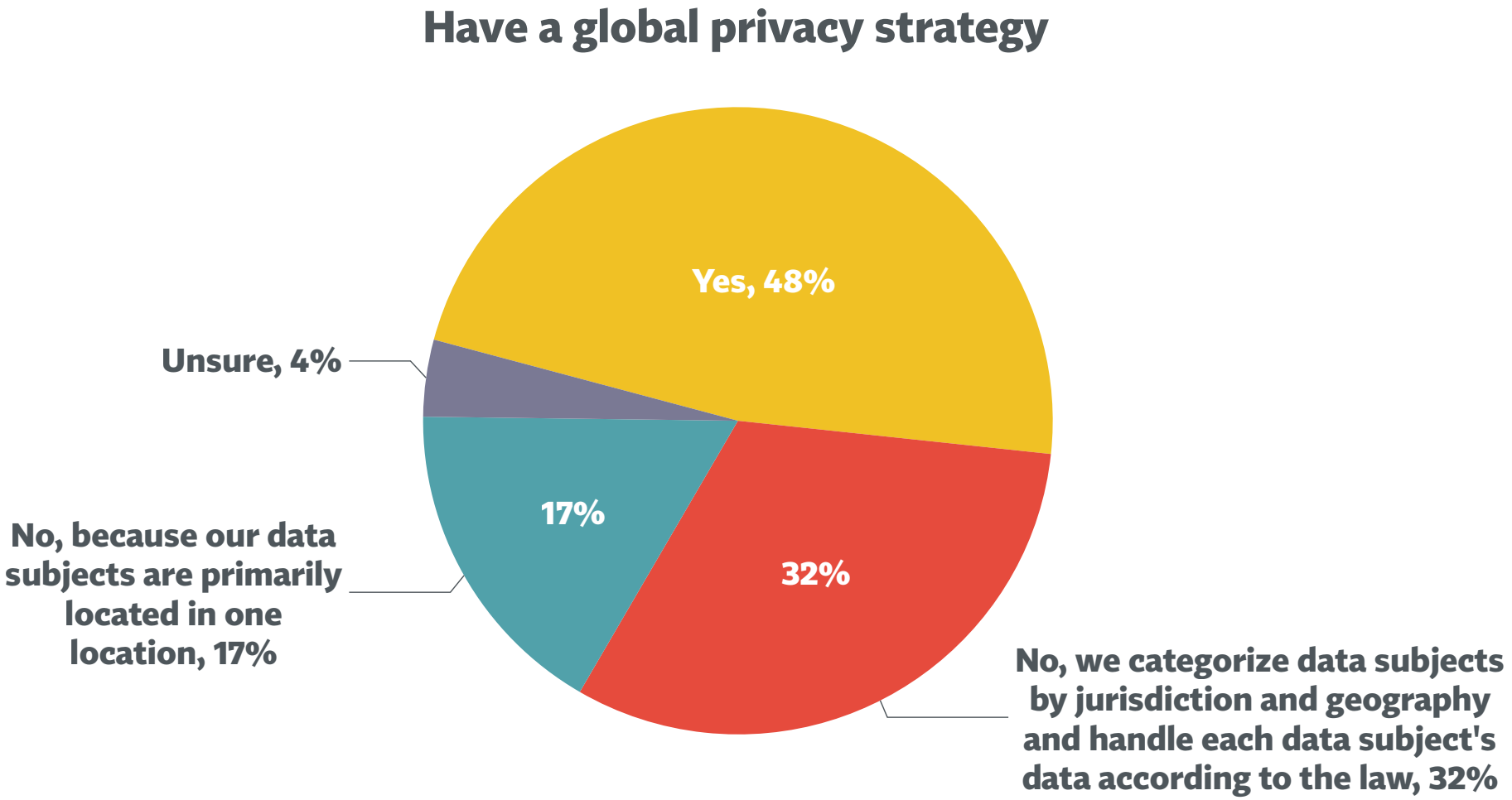
Nearly 6 in 10 privacy pros said that complying with cross-border data transfer laws is their most difficult task

Most difficult tasks to comply with
(Adds to more than 100% because respondents could choose up to three)



L3: Considering privacy and data protection laws around the world, which of the following tasks is most difficult to comply with?

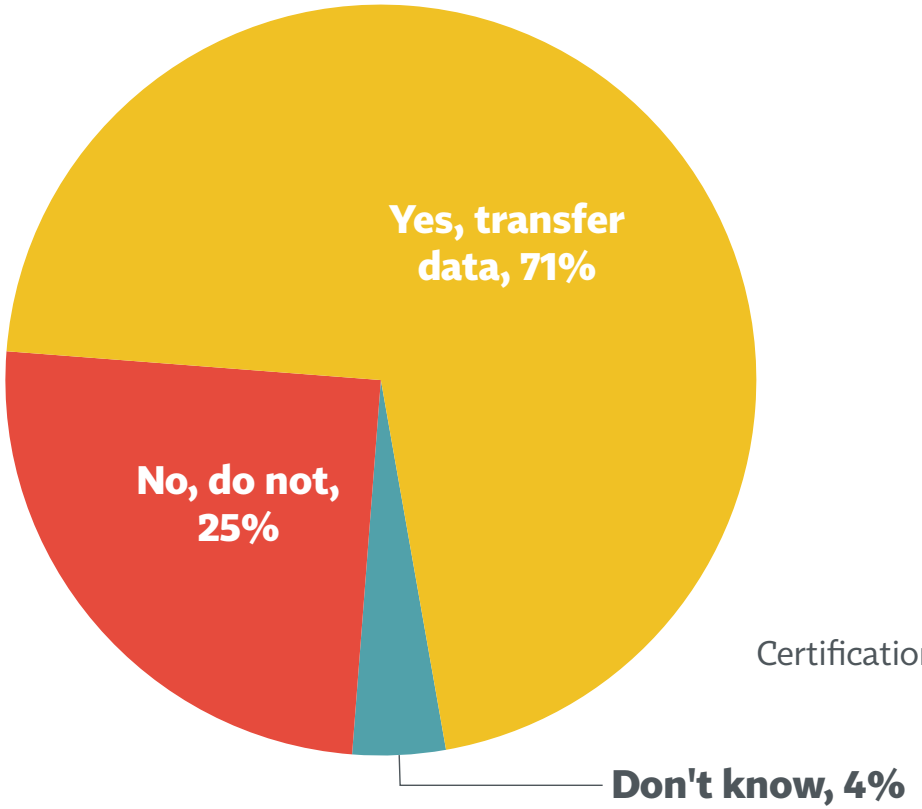
Nearly half (48%) of firms have a single global privacy strategy



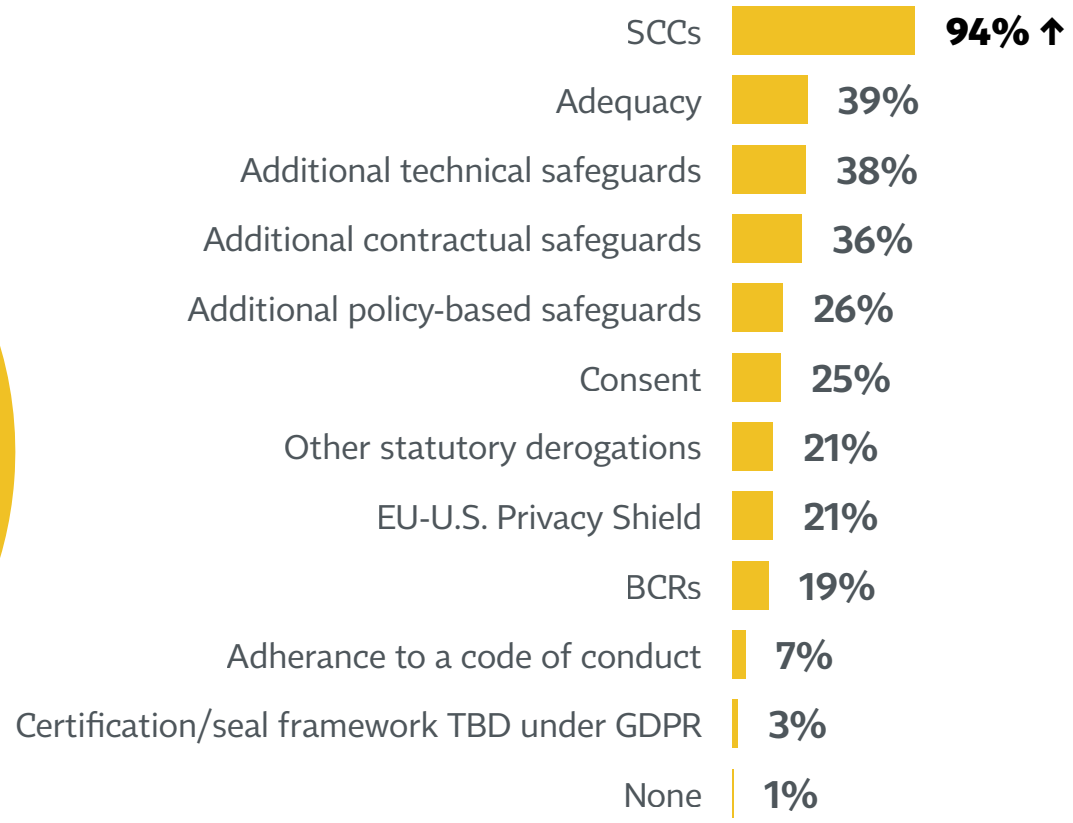
D5: Does your organization have a single global data protection/privacy strategy for data subjects' rights?

More than 7 in 10 firms transfer data from the EU to a third country; SCCs are used by nearly all (94%) of them

Data transfer with EU



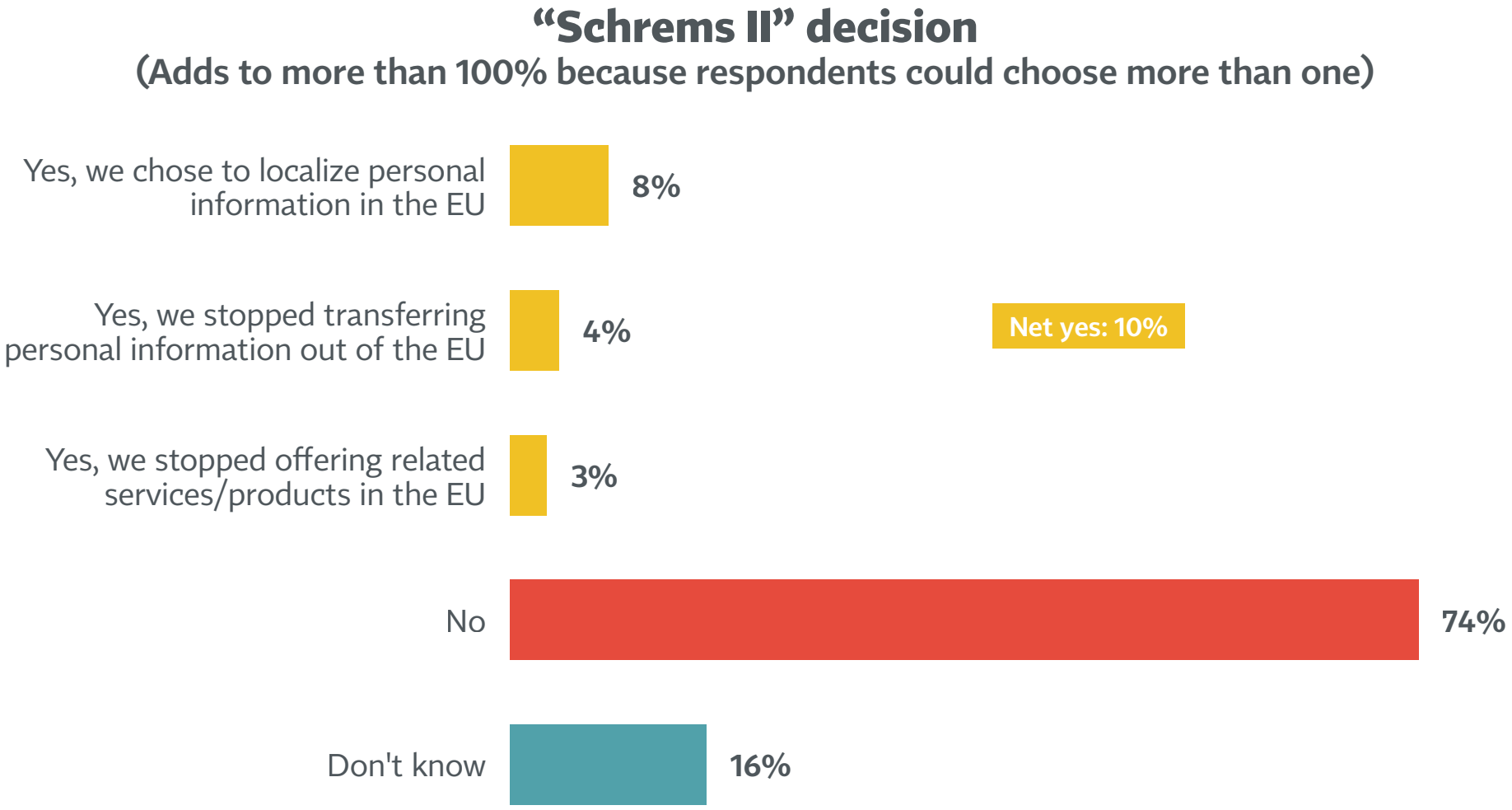
Data transfer mechanisms
(Base: Transfer data with EU)



↑ Significantly different from 2020

J41: Does your company transfer personal information from the European Union and/or those countries in the European Economic Area to another country outside of the EU (or receive personal information from the EU)?
J42: What mechanisms does your company currently use to transmit data outside the EU (or receive personal information from the EU)?

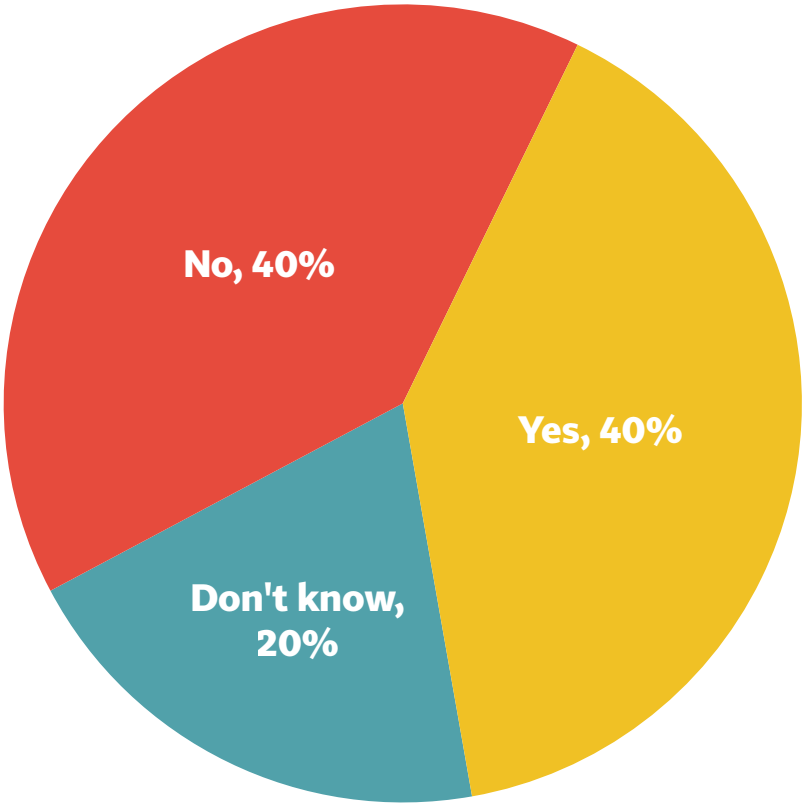
10% of firms chose to localize data, stop transfers or halt related services as a result of the CJEU's 'Schrems II' decision



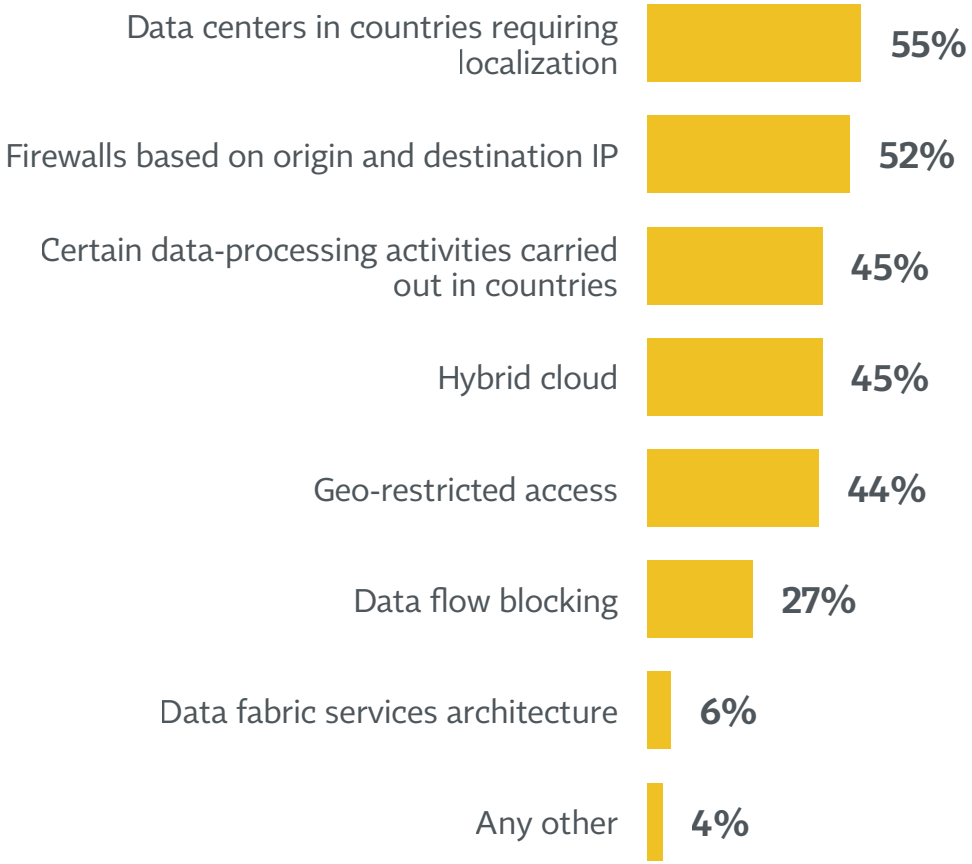
J42a: Did your organization stop transferring any personal information out of the EU, localize any data in the EU and/or stop offering any related services/products in the EU as a result of the Court of Justice of the European Union's "Schrems II" decision?

4 in 10 firms said they have data and technology controls in place to restrict data transfers based on jurisdiction

Have data controls in place

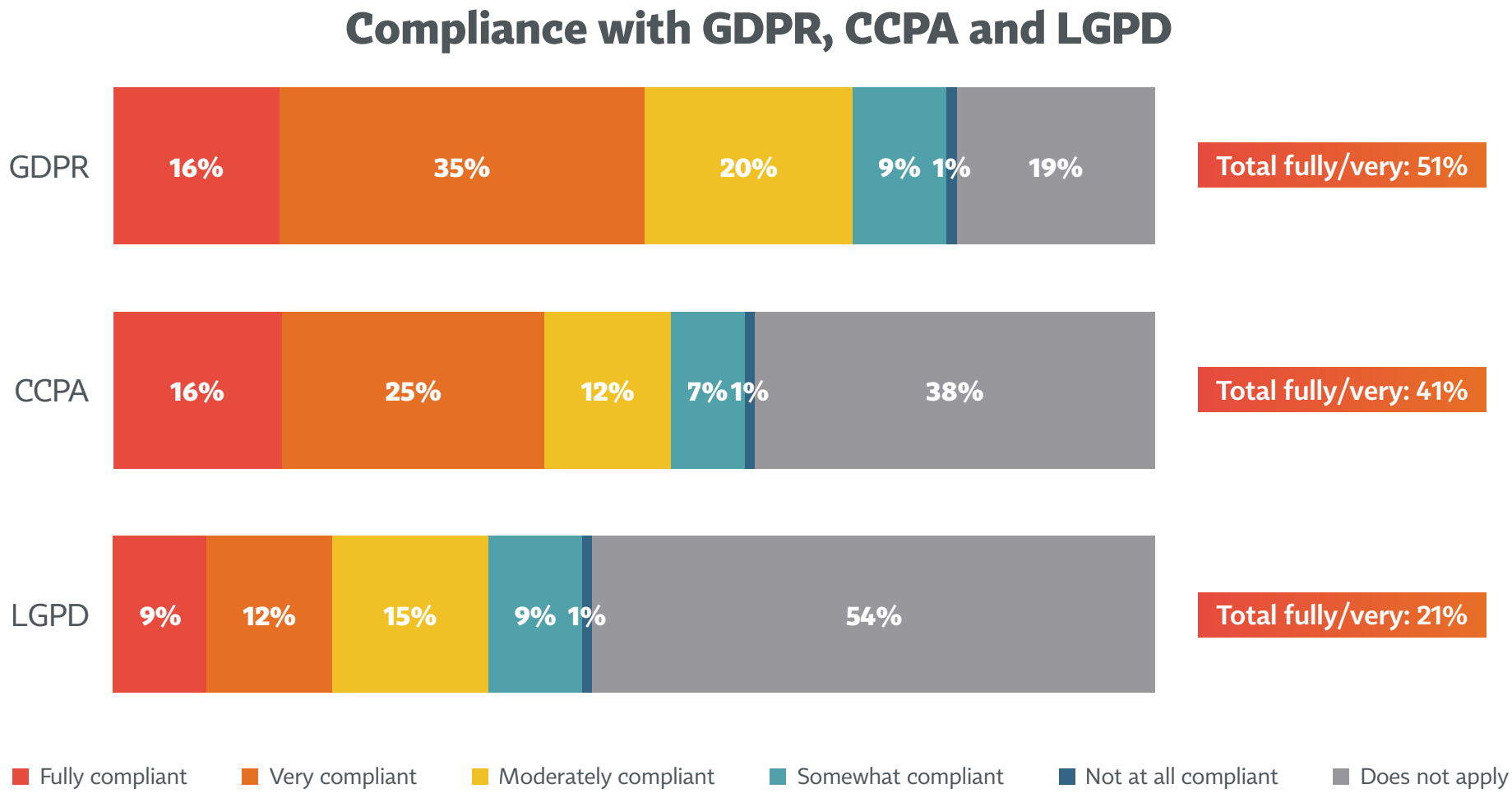


Control mechanisms
(Base: Have data controls in place)



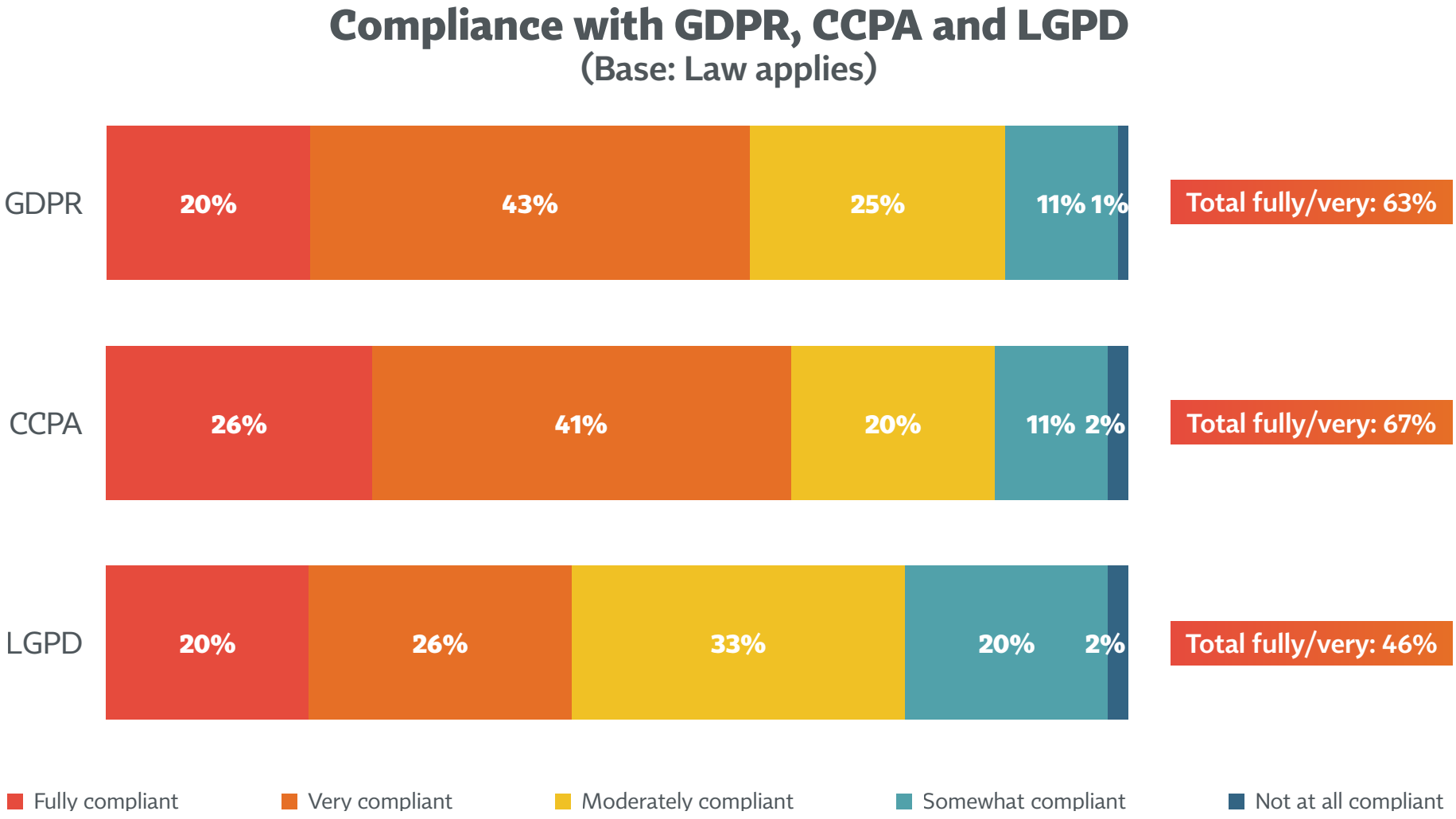
J45: Does your organization have data and technology controls in place to control or restrict the transfer, access and/or storage of data based on jurisdiction?
J45a: Please indicate which types of data and technology controls your organization has in place to restrict the transfer, access and/or storage of data based on jurisdiction.

More than half (51%) of respondents rate themselves very or fully compliant with GDPR, versus 41% for CCPA and 21% for LGPD



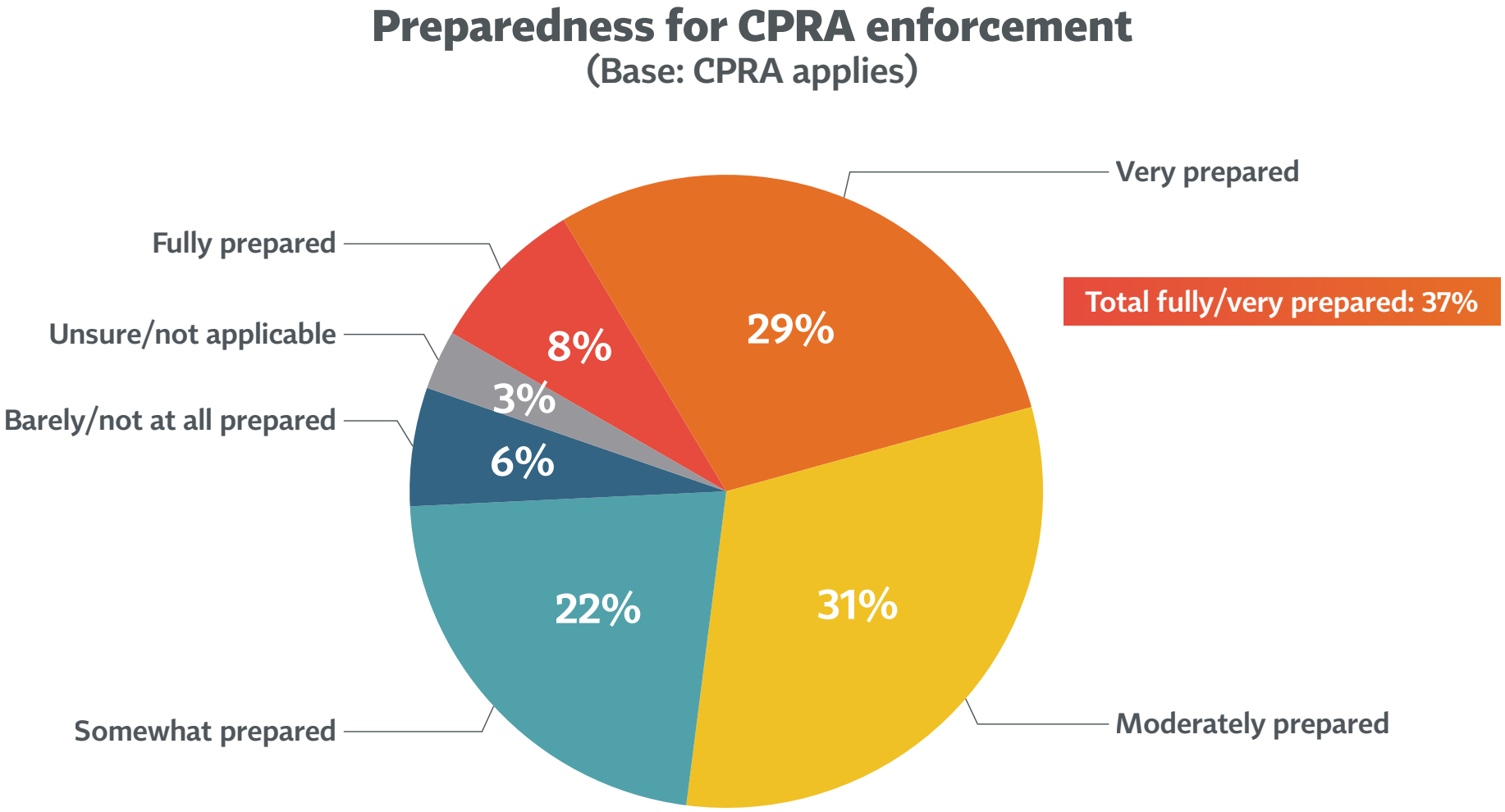
L1: Please indicate your organization's current level of compliance with the California Consumer Privacy Act, EU General Data Protection Regulation and Brazil's General Data Protection Law, as applicable?

Considering only those firms to whom each law applies, compliance is highest for CCPA, with 67% saying they are very/fully compliant



L1: Please indicate your organization's current level of compliance with the California Consumer Privacy Act, EU General Data Protection Regulation and Brazil's General Data Protection Law, as applicable?

Among those saying the CPRA applies to them, more than one-third is fully or very prepared

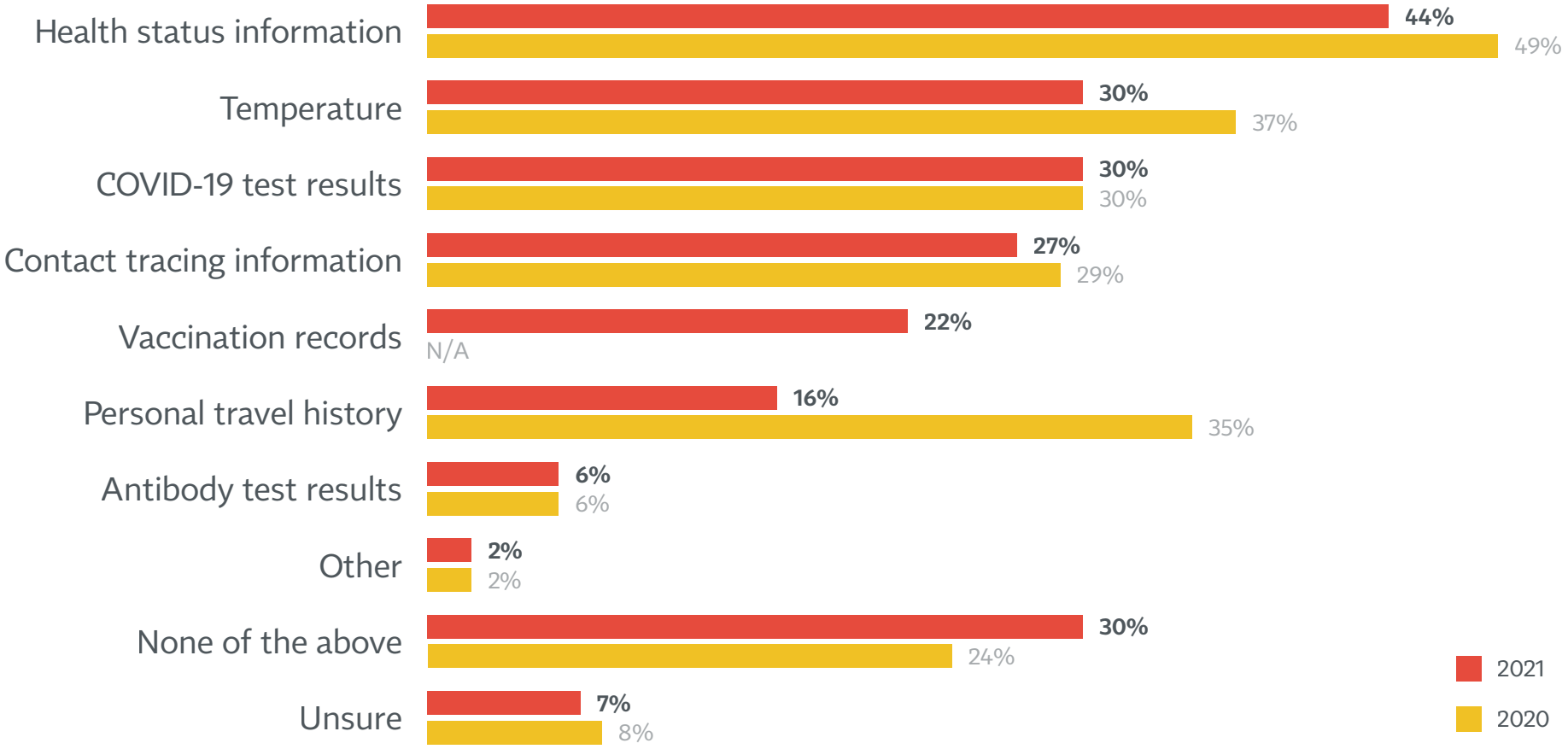


L2: As of today, how prepared is your organization for the future entry into force of the California Privacy Rights Act?

Contents

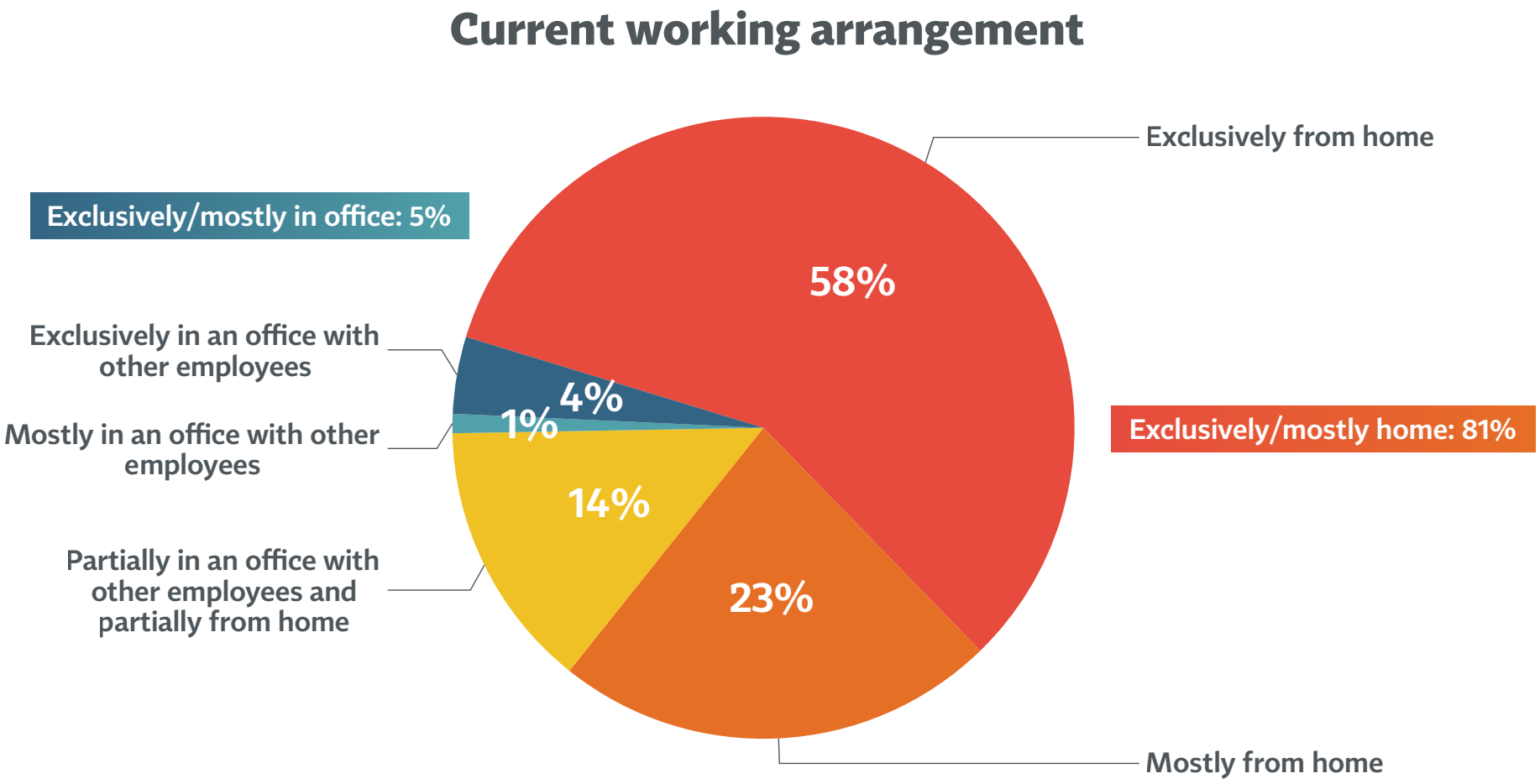
Fewer employers are collecting COVID-19-related health data from their employees this year compared to last, though 70% still do

Data collected from employees during COVID-19 pandemic



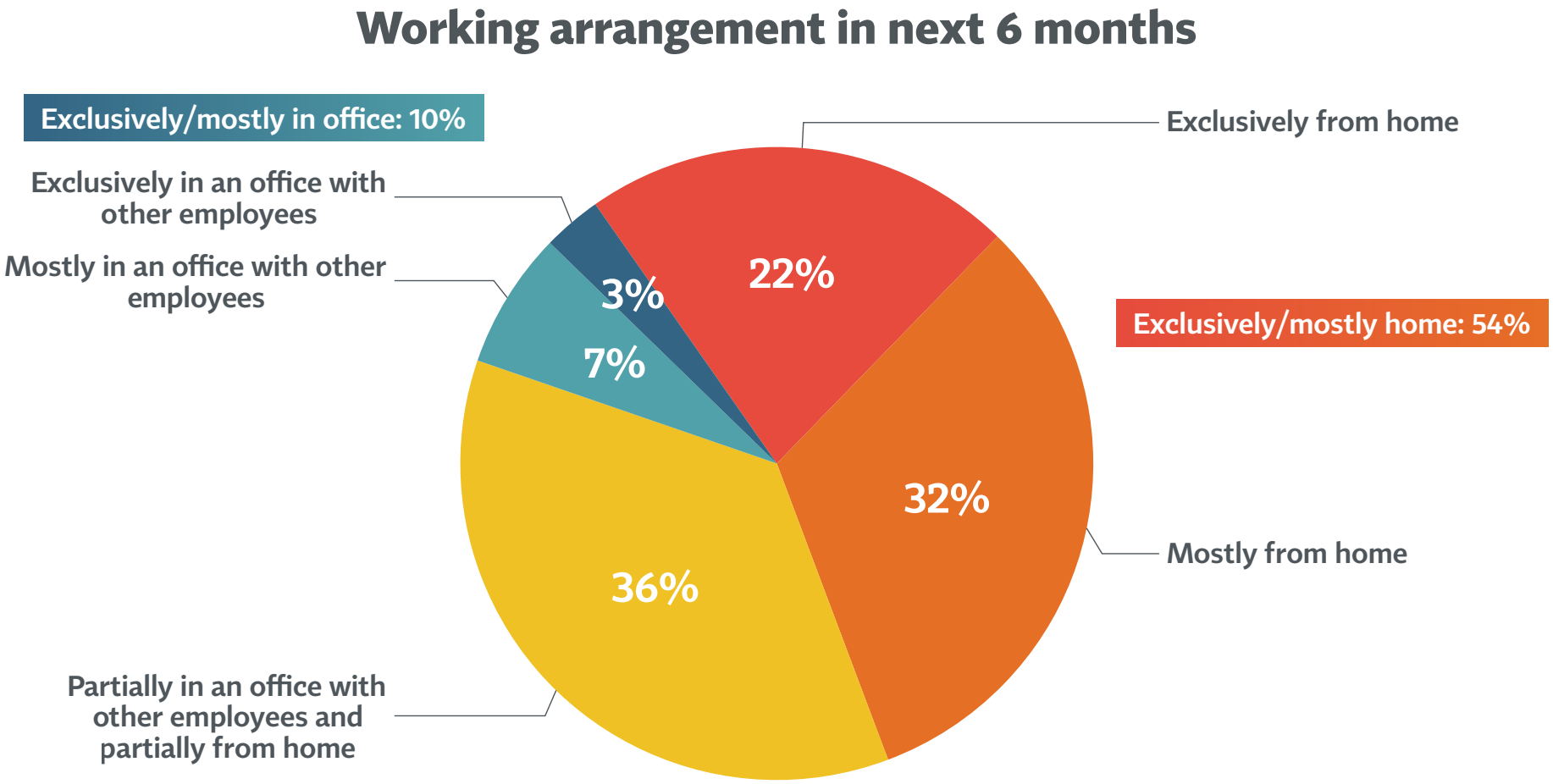
CV4: Since the COVID-19 pandemic began, has your organization collected any of the following data from employees?

Privacy pros continue to work mostly from home, although the proportion of those exclusively remote is down to 58% from 71% in 2020



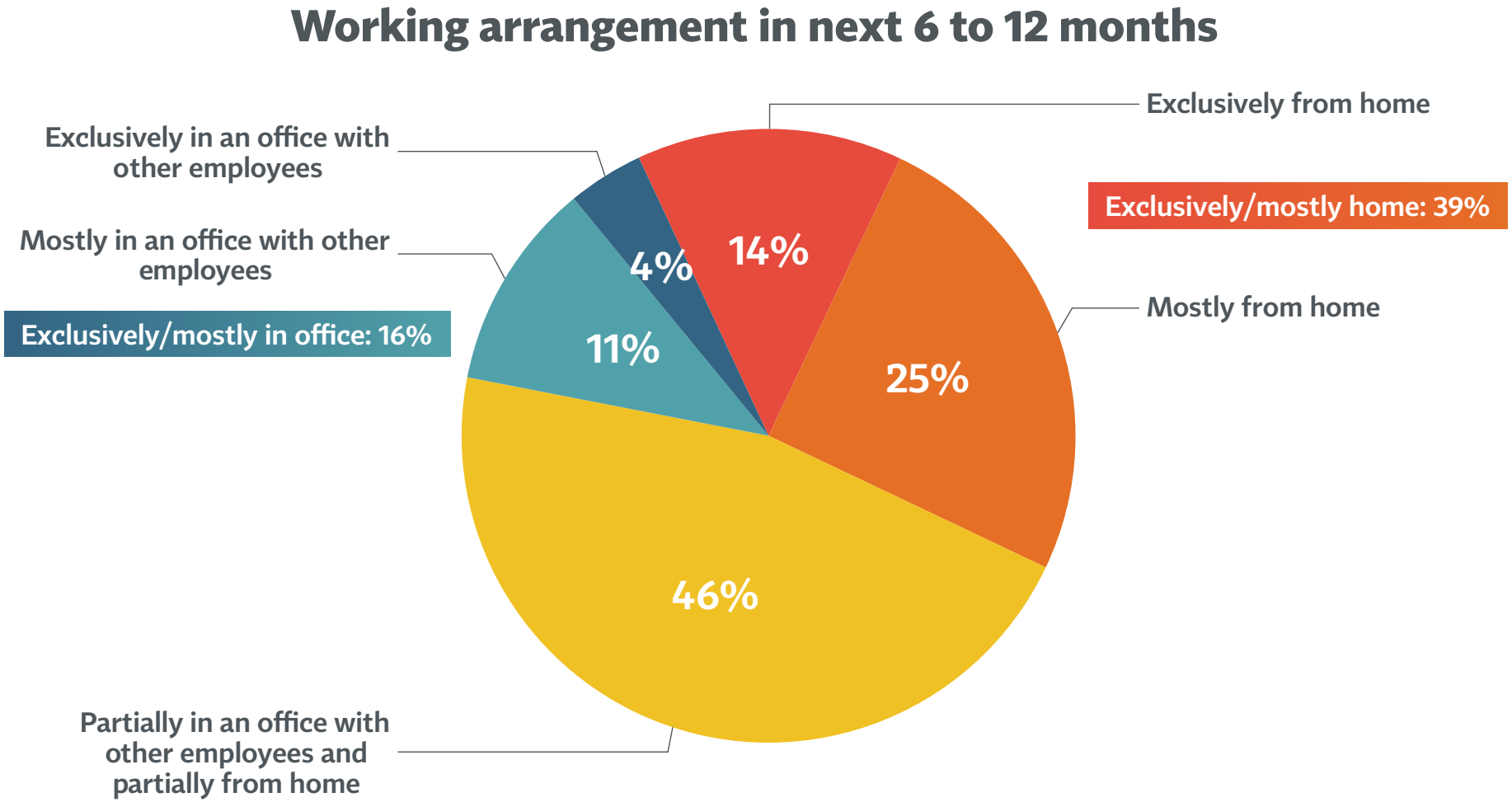
CV7: Which of the following best describes your current personal working arrangement?

The proportion expecting to work exclusively from home drops after 6 months, to just over 1 in 5



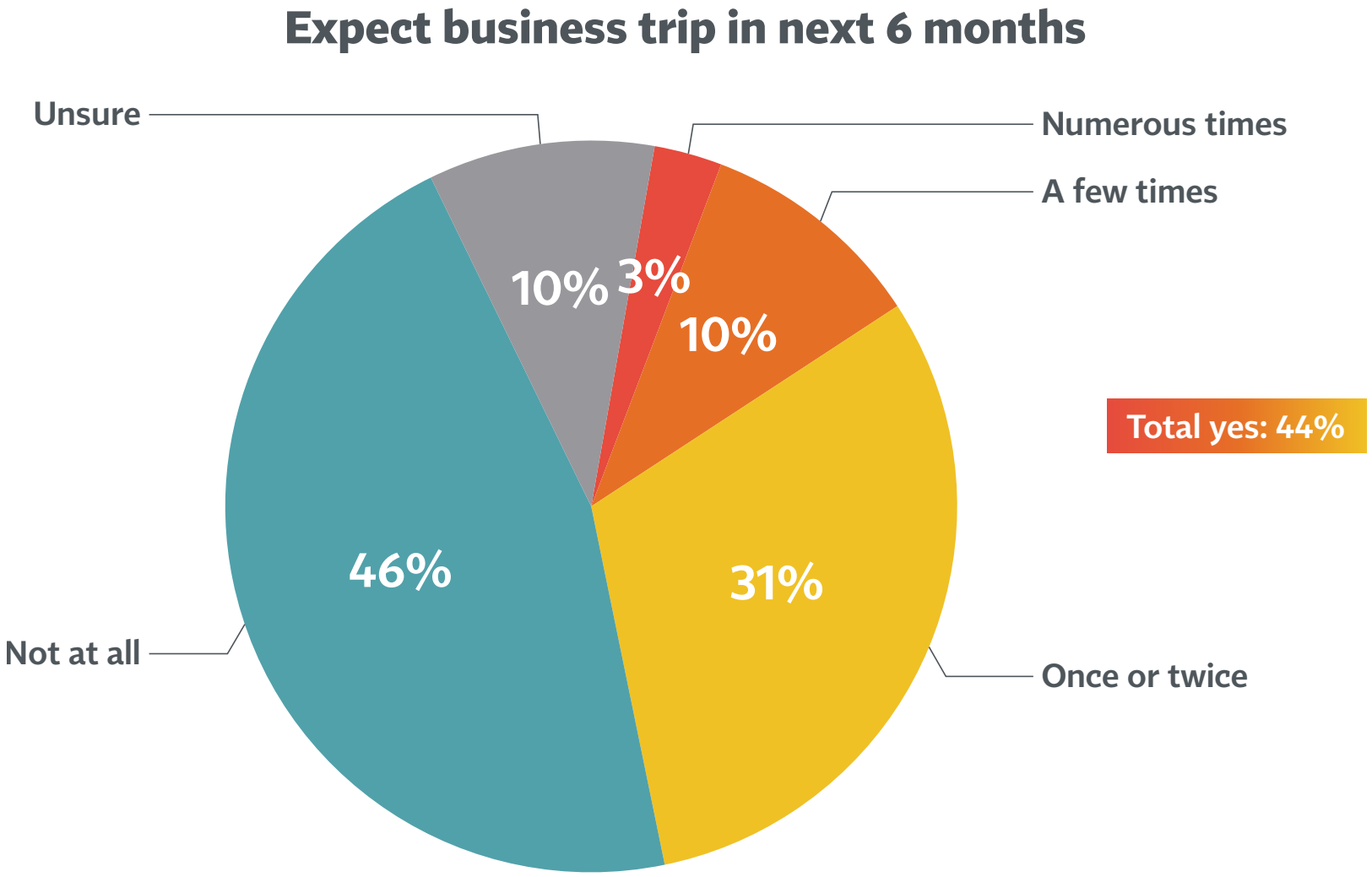
CV9: Over the next six months or so, I expect to work:

Looking out 6 to 12 months, 14% expect to work exclusively from home and 4% expect to be exclusively in an office, with the rest (82%) hybrid



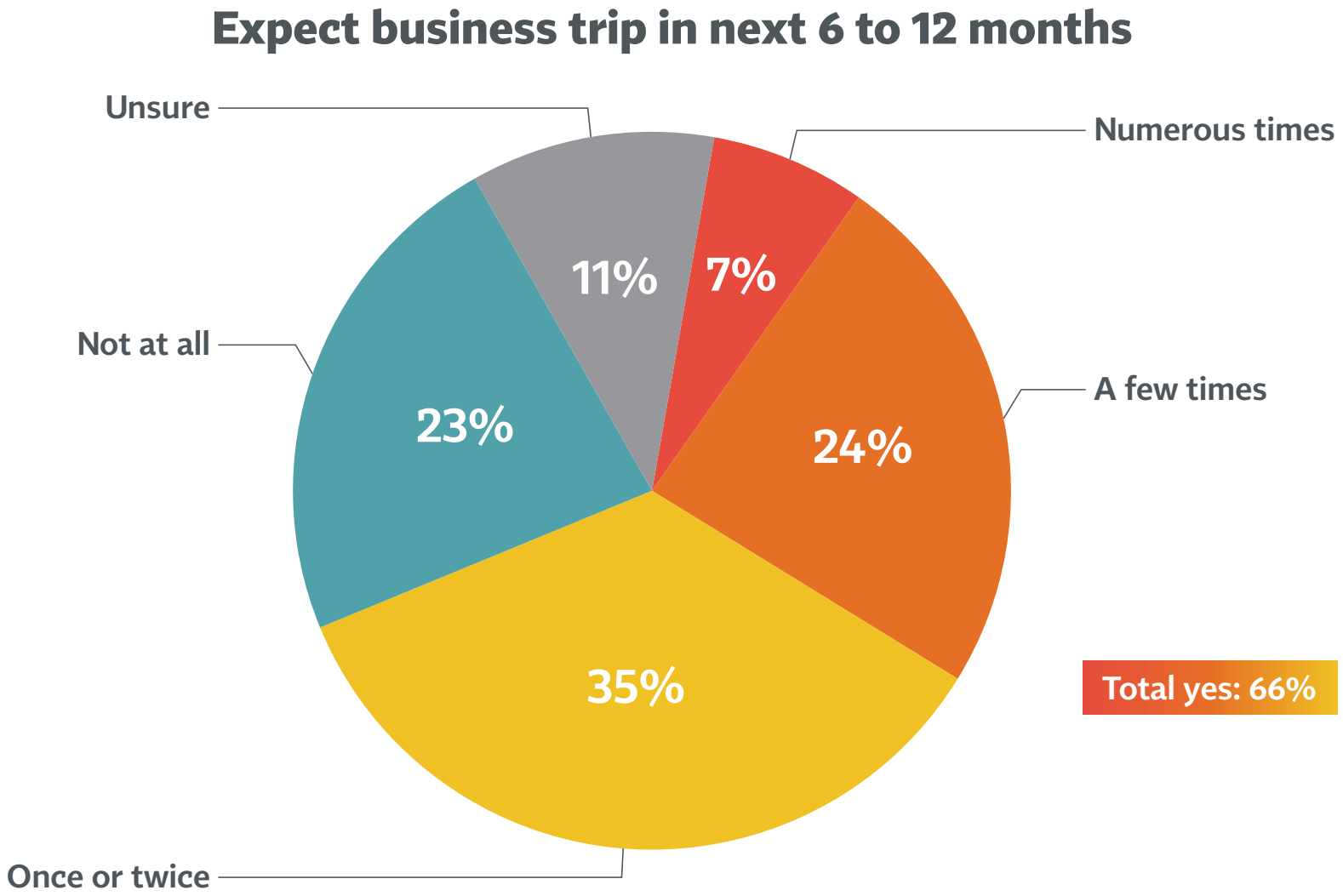
CV9A: Six to twelve months from now, I expect to work:

Over the next 6 months, about 4 in 10 expect to travel for business, with most of these planning to do so once or twice



CV10: Over the next six months or so, I expect to go on business-related trips:

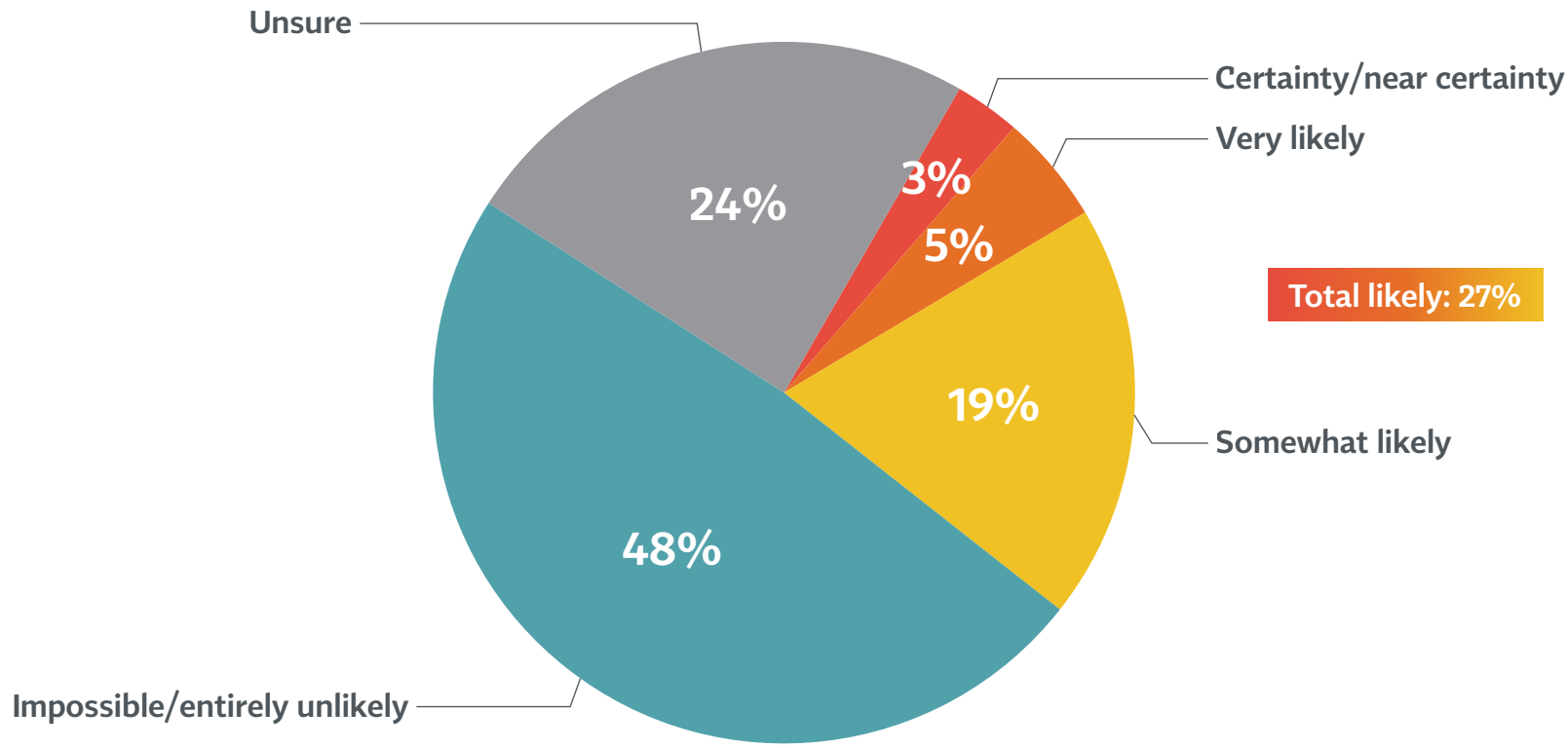
Over the next 6 to 12 months, however, the proportion expecting business travel increases to two-thirds



CV10a: Six to twelve months from now, I expect to go on business-related trips:

While 1 in 4 privacy pros are uncertain whether they will need a vaccine passport to return to the office, 1 in 4 also said it is at least somewhat likely

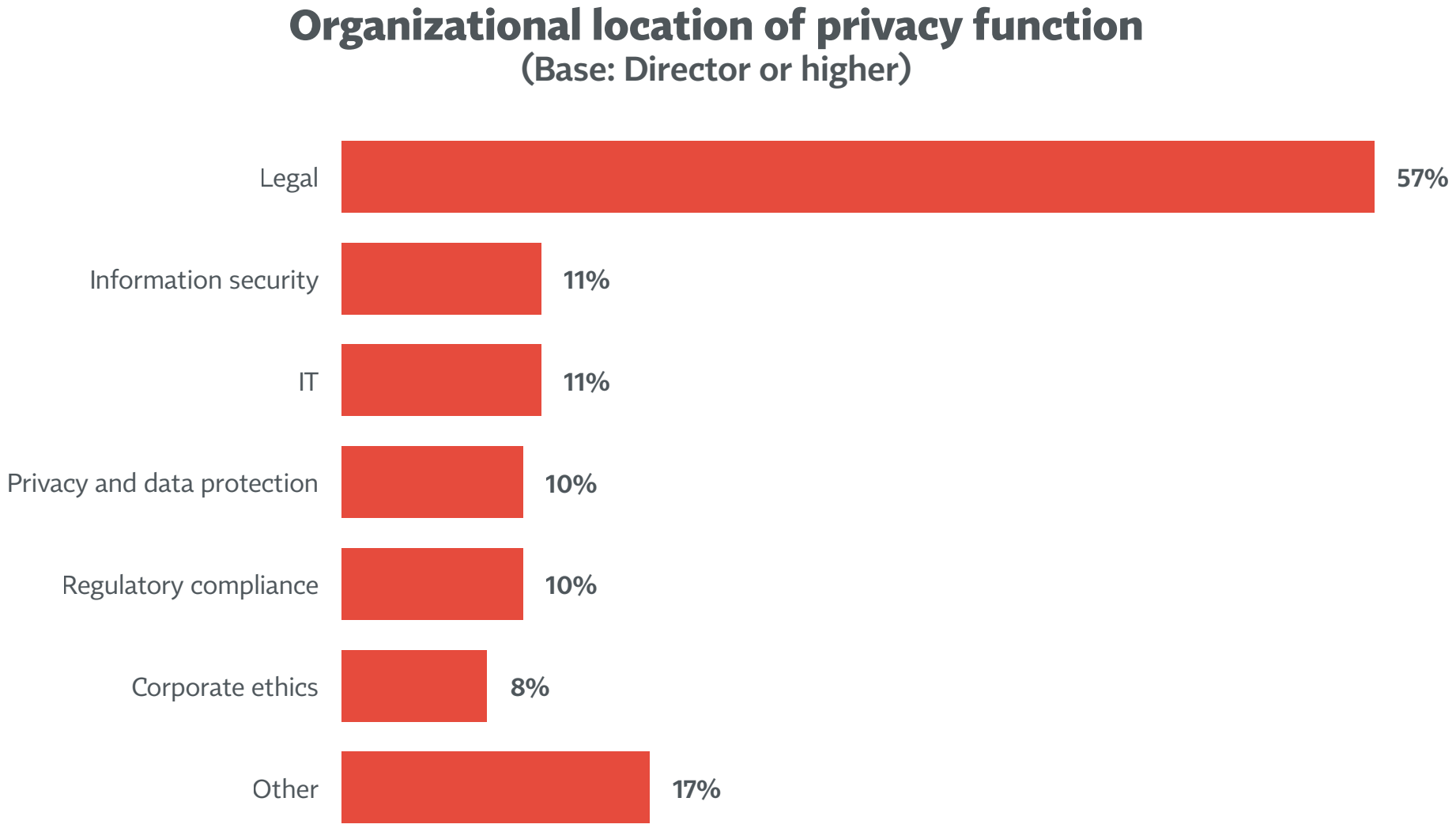
Likelihood of a COVID-19 vaccine passport requirement to return to work



CV11: How likely is your organization to mandate the possession of a COVID-19 vaccine passport or something similar as a requirement to enter and use its office workspace?

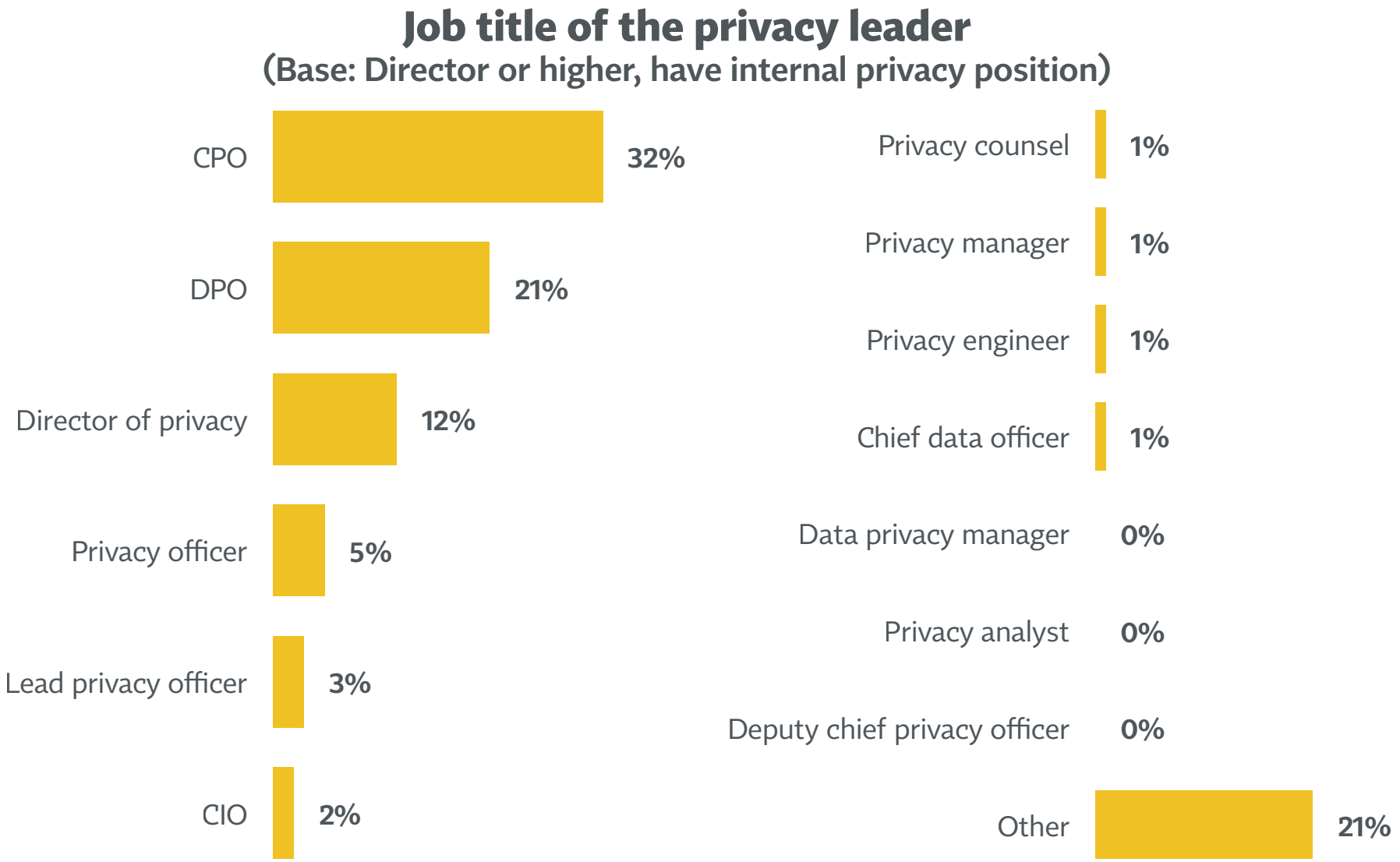
Contents

The privacy team is most likely to be housed within an organization's legal department



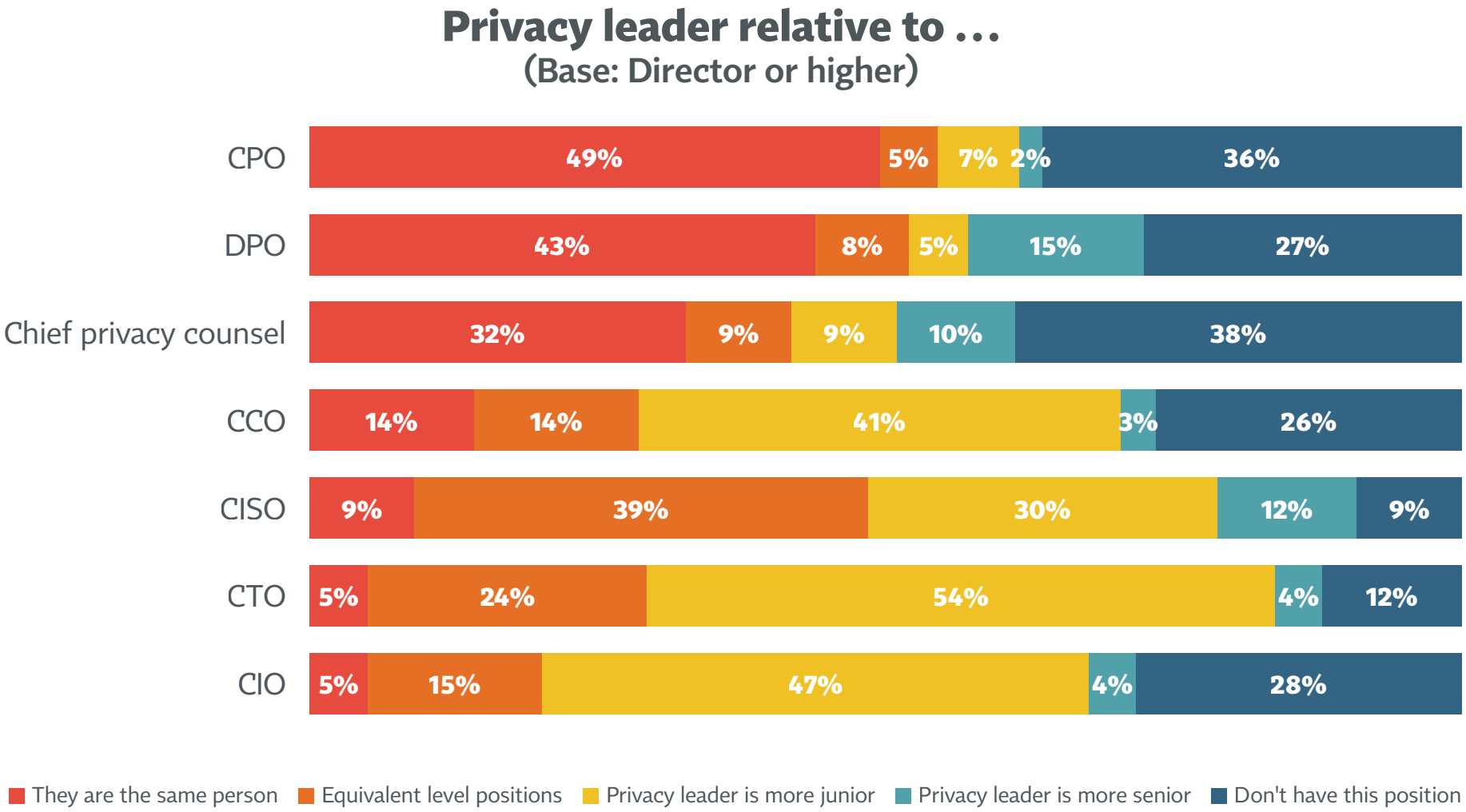
F12: Within which department at your company is the privacy team located?

The most common job title for an organization's privacy leader is CPO, followed by DPO and director of privacy



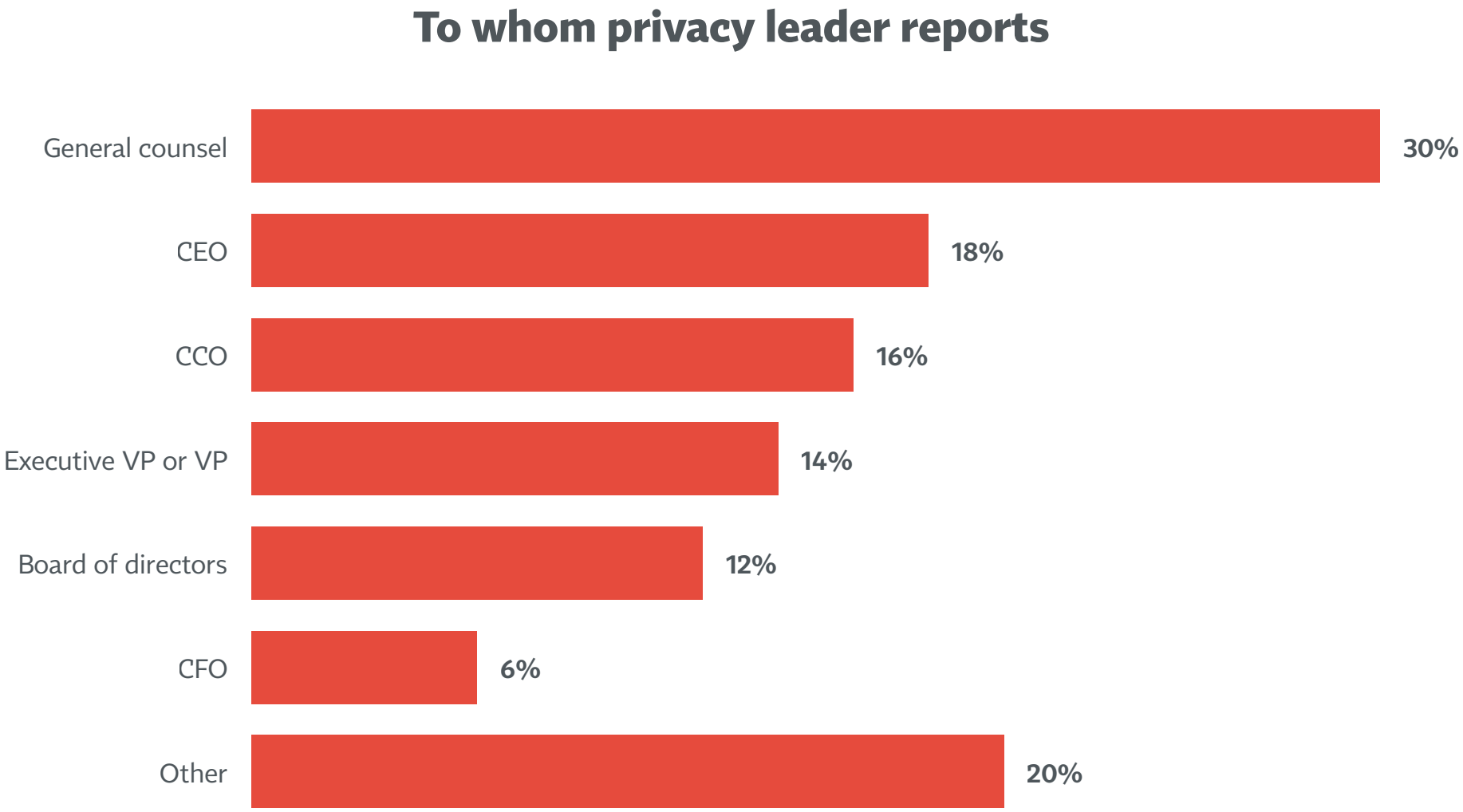
F21: What is the job title of the privacy leader in your company? By "privacy leader," we mean the person who is responsible for managing and overseeing your organization's privacy program.

Privacy leaders are frequently the same/equivalent level to CPOs, DPOs and CISOs but tend to be junior to CCOs, CTOs and CIOs



F22d: How does the position of the privacy leader compare with that of your company's [role], if any?

Nearly half of privacy leaders report to either the general counsel (30%) or CEO (18%)



F25: To whom in your company does the privacy leader report?

As in prior years, privacy leaders at smaller companies are the most likely to report directly to the CEO

BY COMPANY REVENUE

	<$100M	$100M–$999M	$1B–$24.9B	$25B+
Privacy leader reports to:				
General counsel	**20%**	32%	39%	35%
CEO	**29%**	20%	**9%**	0%

BY EMPLOYEE SIZE

	<5K	5K–24.9K	25K–74.9K	75K+
Privacy leader reports to:				
CEO	**25%**	14%	6%	4%
CCO	**9%**	21%	20%	**37%**

Significantly different than other segments

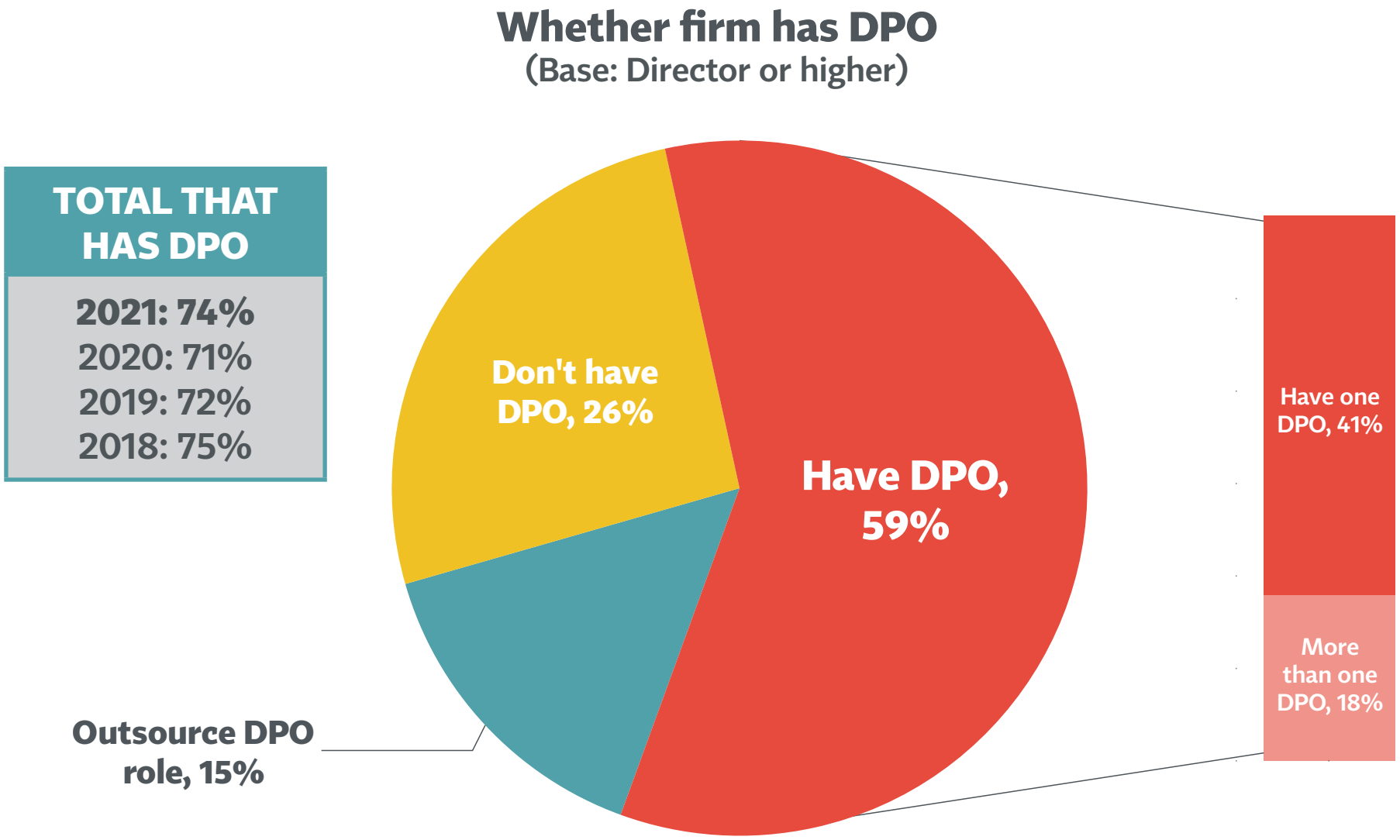
While EU privacy leaders are more likely to report to the CEO or board, those in the US are more likely to report to the general counsel

BY HQ LOCATION

	U.S.	EU
Privacy leader reports to:		
General counsel	34%	27%
CEO	**12%**	24%
Board of directors	**5%**	**27%**

Significantly different than other segments

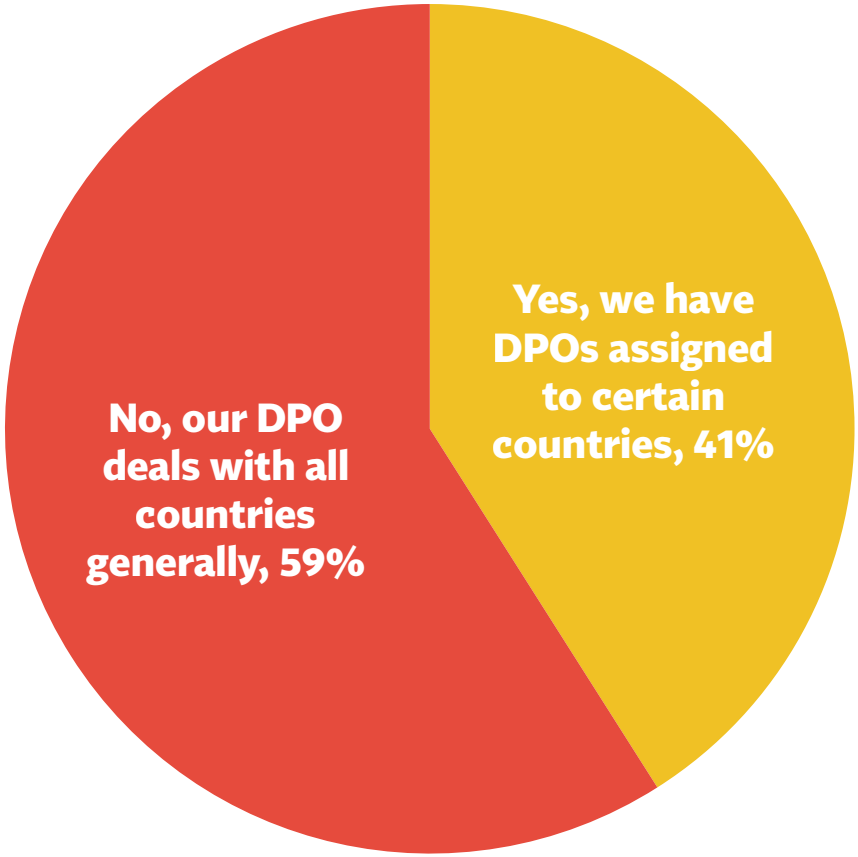
3 in 4 firms have a DPO, with 15% outsourcing the role (up from 8% in 2020)



F28New: Is there a data protection officer at your organization, either working directly for it or outsourced by it? (This may be you.)
F30: How many data protection officers work for your organization?

6 in 10 organizations with an in-house DPO said the position handles matters across all countries, while 4 in 10 have country-specific DPOs

Whether internal DPOs are country specific
(Base: Director or higher with internal DPO)



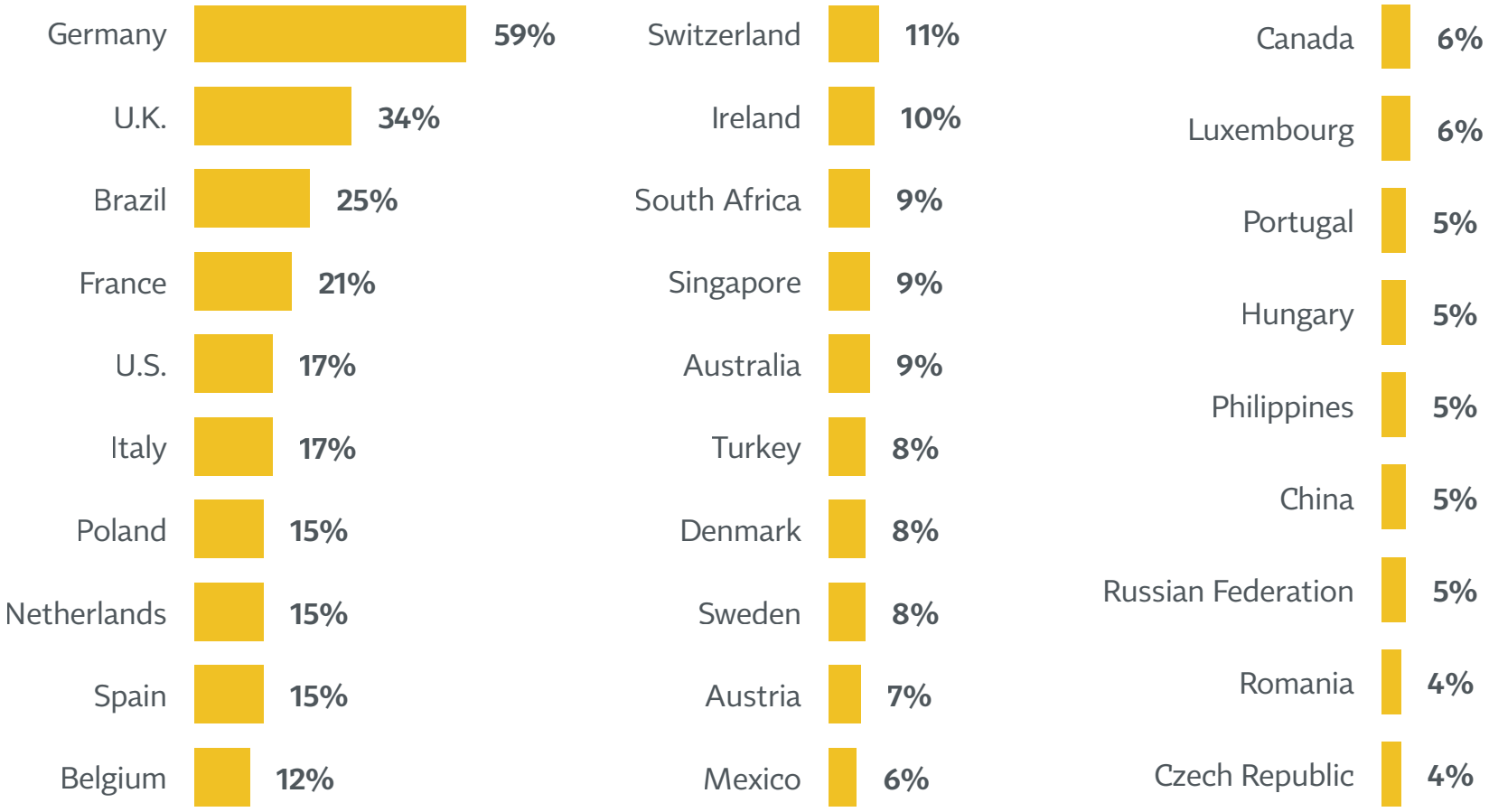
F30a: Are any of your data protection officers country specific?

The countries most likely to have a dedicated DPO are Germany, the UK and Brazil

To which countries DPOs are assigned

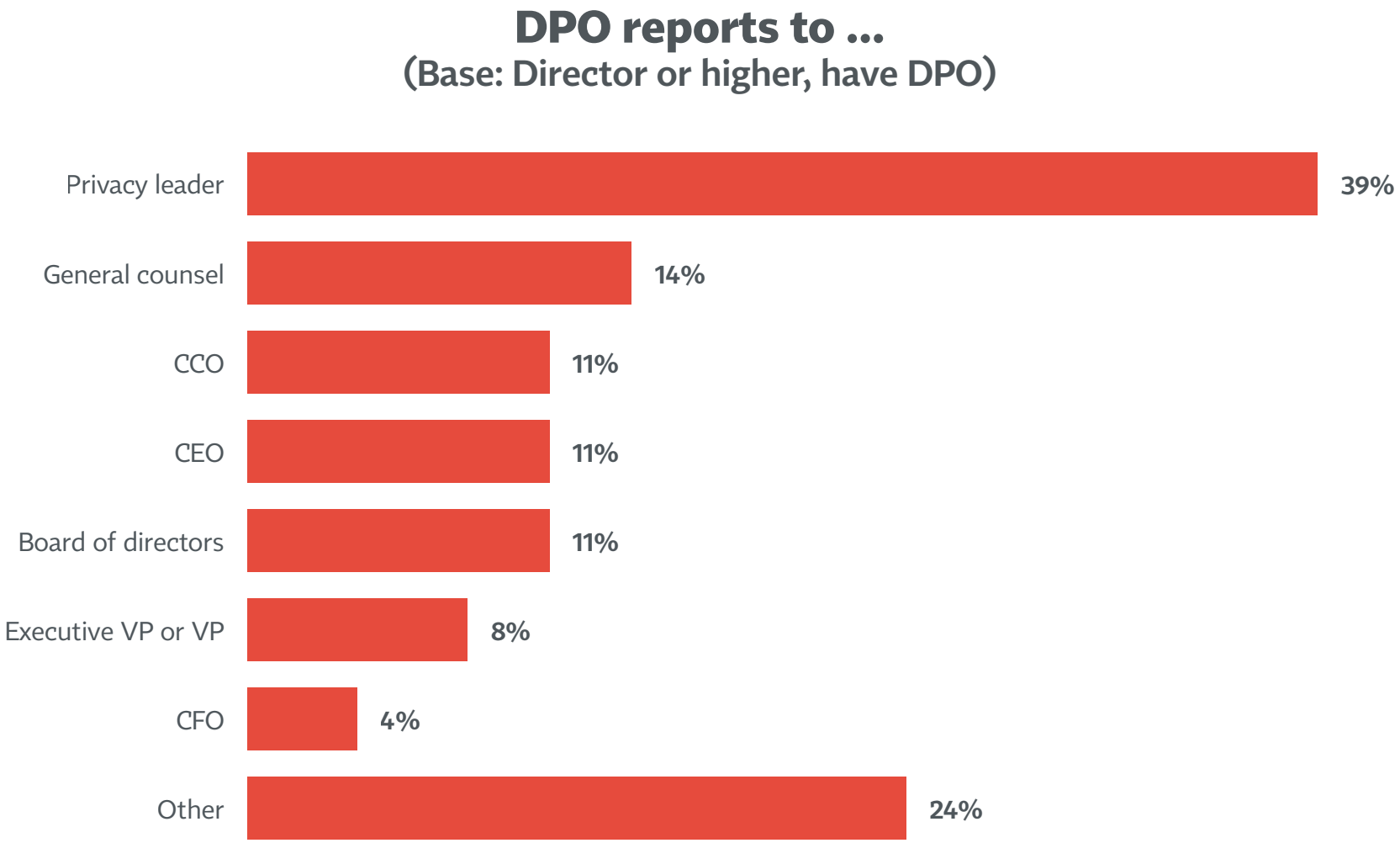
(Base: Director or higher with internal DPO assigned to specific country)

**Countries with more than 3% DPO assignment shown*



F30b: Please indicate for which countries you have a unique data protection officer.

DPOs are most likely to report to the privacy leader, general counsel or CCO



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

In the EU, the privacy leader is much more likely to be the DPO than in the US, where fewer organizations have a DPO

Privacy leader relative to DPO

BY COMPANY HQ

	U.S.	EU
They are the same person	**29%**	65%
Don't have a DPO	**35%**	12%

Significantly different than other segments

Contents

Firms have an average of 18 full- or part-time privacy staff, with more in the EU than US

Mean privacy staff size

	Overall
Full-time privacy staff	7
Part-time privacy staff	11

BY HQ LOCATION

	U.S.	EU
Full-time privacy staff	6	9
Part-time privacy staff	11	12

NOTE: Outliers over 999 removed.

F1: How many of the employees in your company are ... ?

Privacy staff sizes differ by firm size, with the largest firms relying much more on part-time staff than smaller firms

Mean privacy staff size

BY EMPLOYEE SIZE

	<5K	5K–24.9K	25K–74.9K	75K+*
Full-time privacy staff	3	5	13	35
Part-time privacy staff	4	10	33	31

BY COMPANY REVENUE

	<$100M	$100M–$999M	$1B–$24.9B	$25B+*
Full-time privacy staff	4	3	11	17
Part-time privacy staff	5	4	13	50

* Small sample size

NOTE: Outliers over 999 removed.

F1: How many of the employees in your company are ... ?

Privacy staff is largest in regulated firms and those serving both consumers and other businesses

Mean privacy staff size

BY INDUSTRY CATEGORY

	Regulated	Unregulated	Government*
Full-time privacy staff	8	7	4
Part-time privacy staff	18	9	9

BY CONSUMER TARGET

	B2B	B2C	Both
Full-time privacy staff	5	5	10
Part-time privacy staff	11	4	14

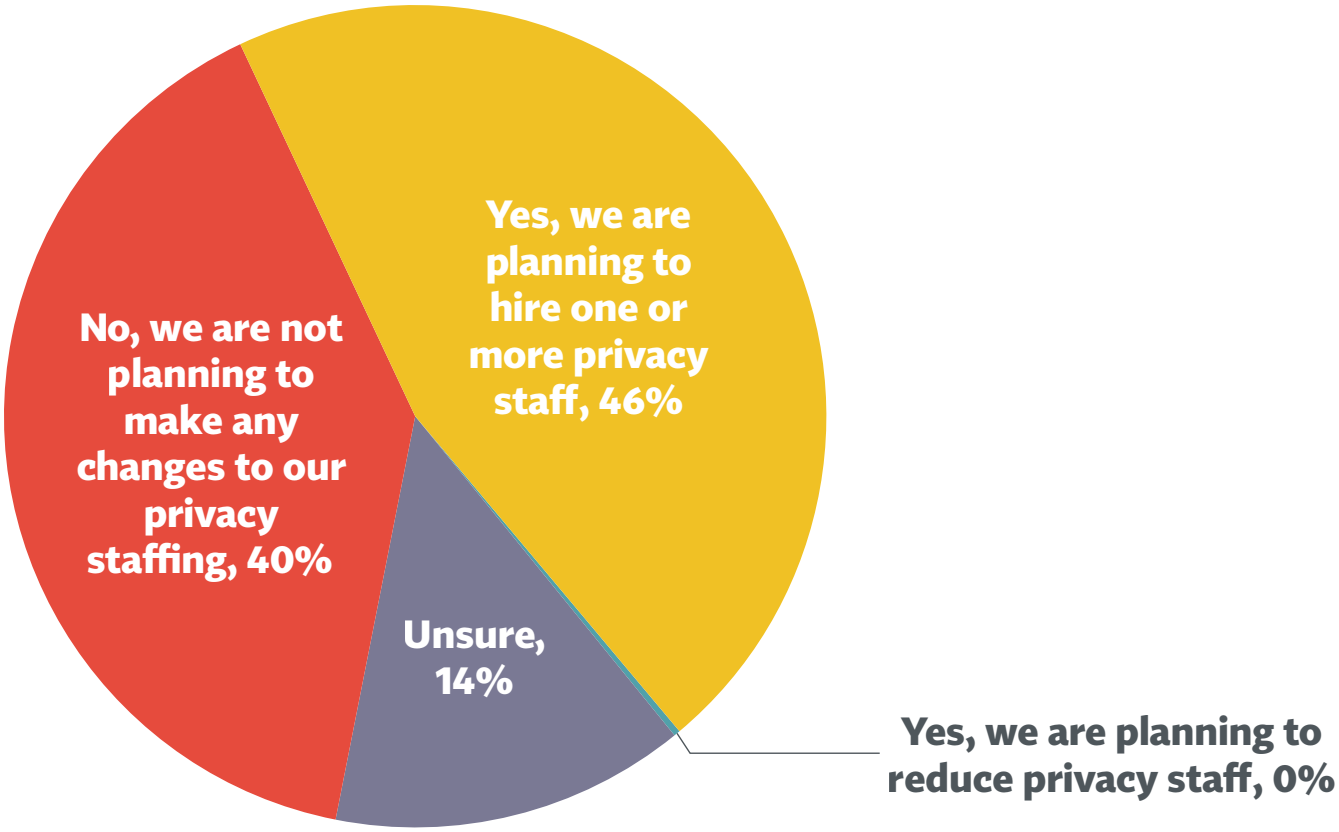
* Small sample size

NOTE: Outliers over 999 removed.

F1: How many of the employees in your company are ... ?

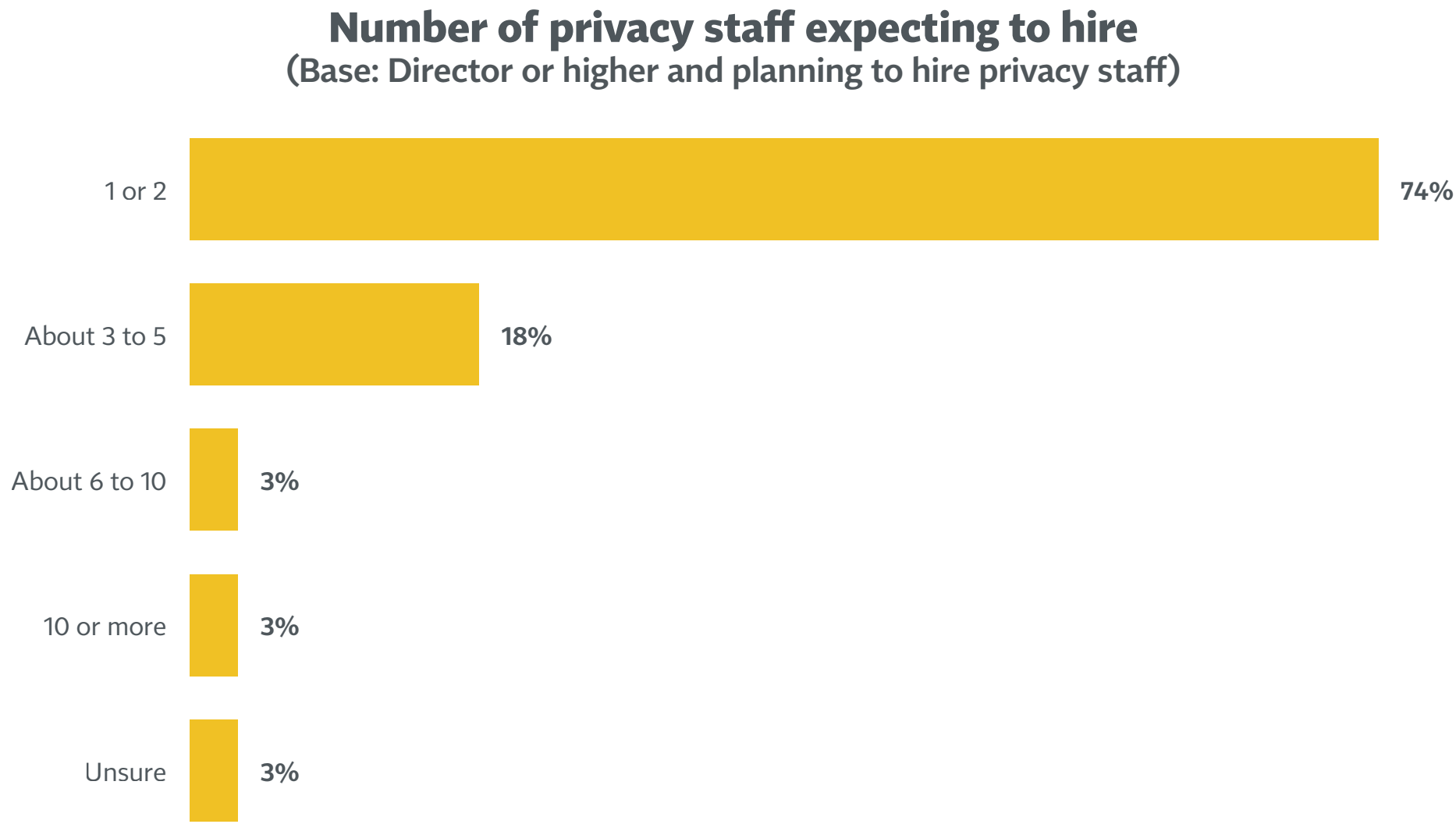
45% of privacy pros at the director level or higher expect their organizations to hire more privacy staff over the next 6 months

Expected staffing increases or reductions
(Base: Director or higher)



F2c: Over the next six months or so, is your organization planning to make any changes related to its privacy staffing?

Among those expecting to hire more staff, most (74%) plan to hire for 1 or 2 positions



F2d: Over the next six months or so, about how many new privacy staff are you planning to hire?

Privacy spending has increased significantly since 2020, with the typical (median) organization's privacy budget being $350K

Estimated privacy spend
(Base: Director or higher)

TOTAL PRIVACY SPEND

2021 MEAN: $873,000
2020 MEAN: $676,000
2019 MEAN: $622,000

2021 MEDIAN: $350,000
2020 MEDIAN: $300,000
2019 MEDIAN: $200,000

F4a: What was your organization's total privacy spend last year?

Privacy spending increases dramatically once one reaches the top tiers of company size, as measured by employees or revenue

Mean estimated privacy spend (000)
(Base: Director or higher)

BY EMPLOYEE SIZE

	<5K	5K–24.9K	25K–74.9K	75K+*
Total privacy spend	$538	$821	$2,075	$1,308

BY COMPANY REVENUE

	<$100M	$100M–$999M*	$1B–$24.9B	$25B+*
Total privacy spend	$427	$299	$1,351	$2,038

* Small sample size

Other than in the smallest firms, median privacy spending has increased since 2020 at firms of all sizes

Mean estimated privacy spend (000)

(Base: Director or higher)

BY EMPLOYEE SIZE

	<5K		5K–24.9K		25K–74.9K*		75K+*	
	2021	2020	2021*	2020	2021*	2020	2021*	2020*
Total privacy spend	$200	$200	$512	$250	$1,000	$870	$800	$750

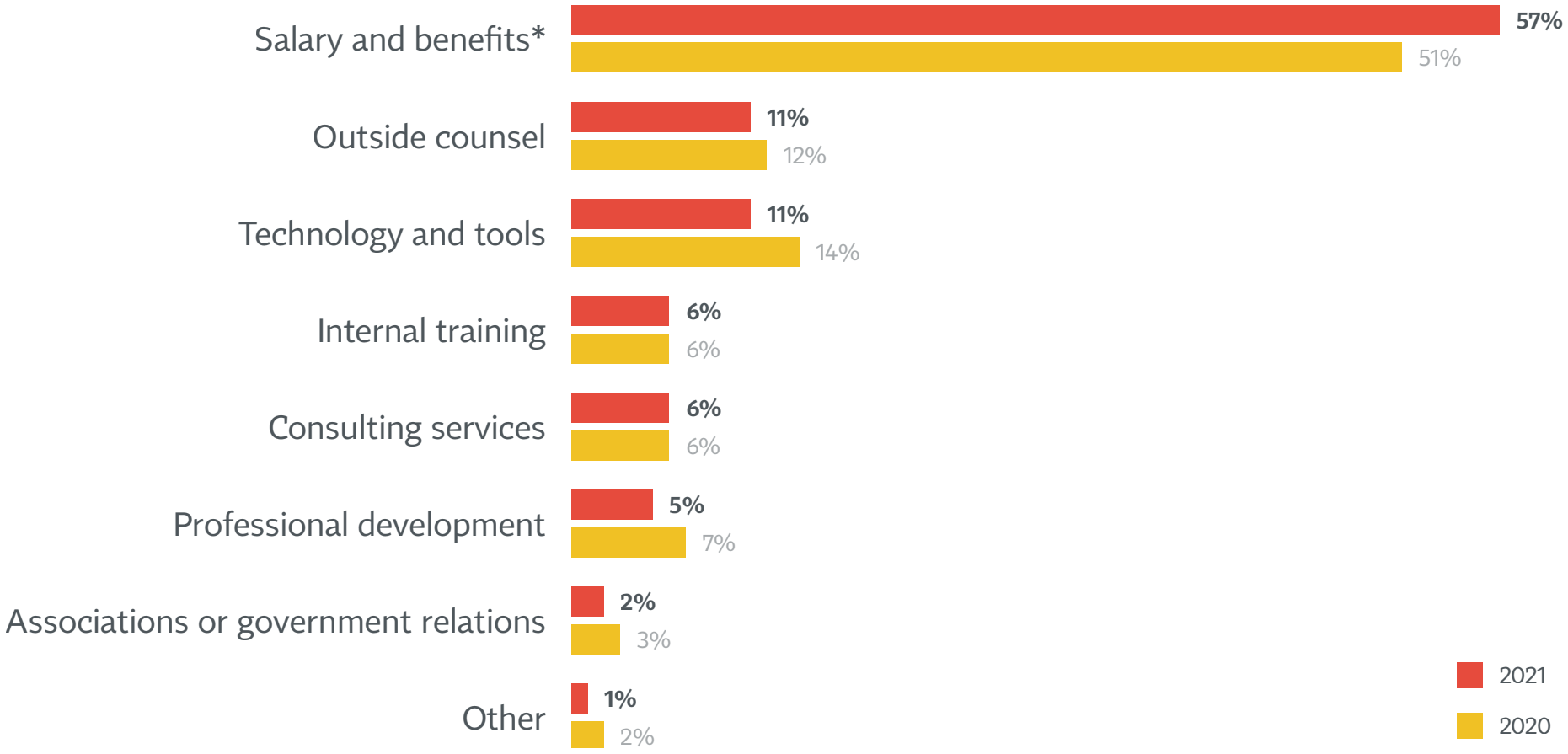
BY COMPANY REVENUE

	<$100M		$100M–$999M		$1B–$24.9B		$25B+	
	2021*	2020	2021*	2020	2021	2020	2021*	2020*
Total privacy spend	$343	$357	$213	$254	$815	$1,038	$1,850	$1,556

* Small sample size

The majority (57%) of firms' privacy budget goes toward salaries and benefits

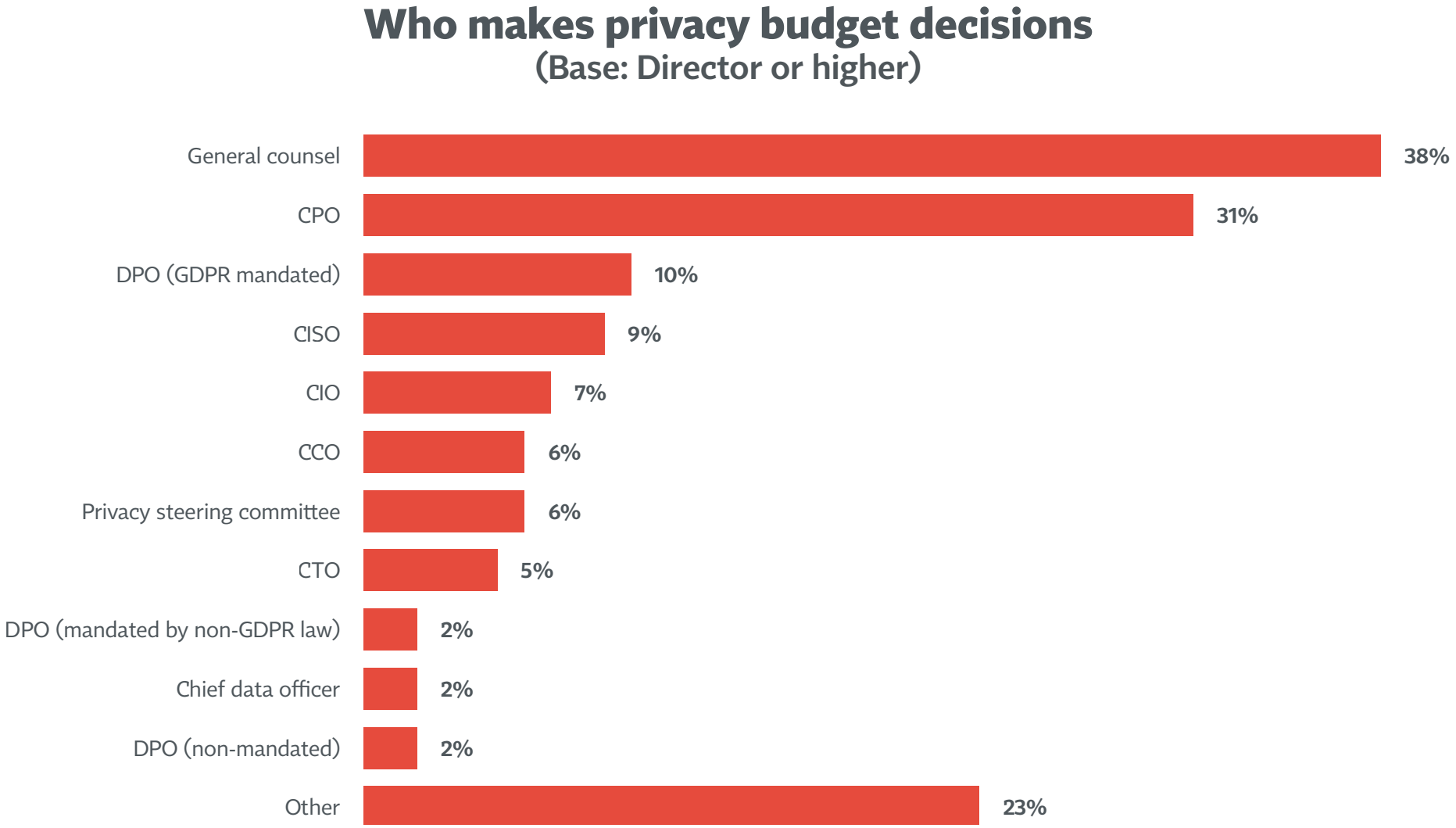
Distribution of privacy budget components
(Base: Director or higher)



This response was changed in 2021 to "Salary and benefits" from "Salary and travel" in previous years, suggesting that the percentage increase year-over-year may be understated since this category no longer includes travel.

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

Privacy budget decisions are most likely to be made by general counsels and CPOs

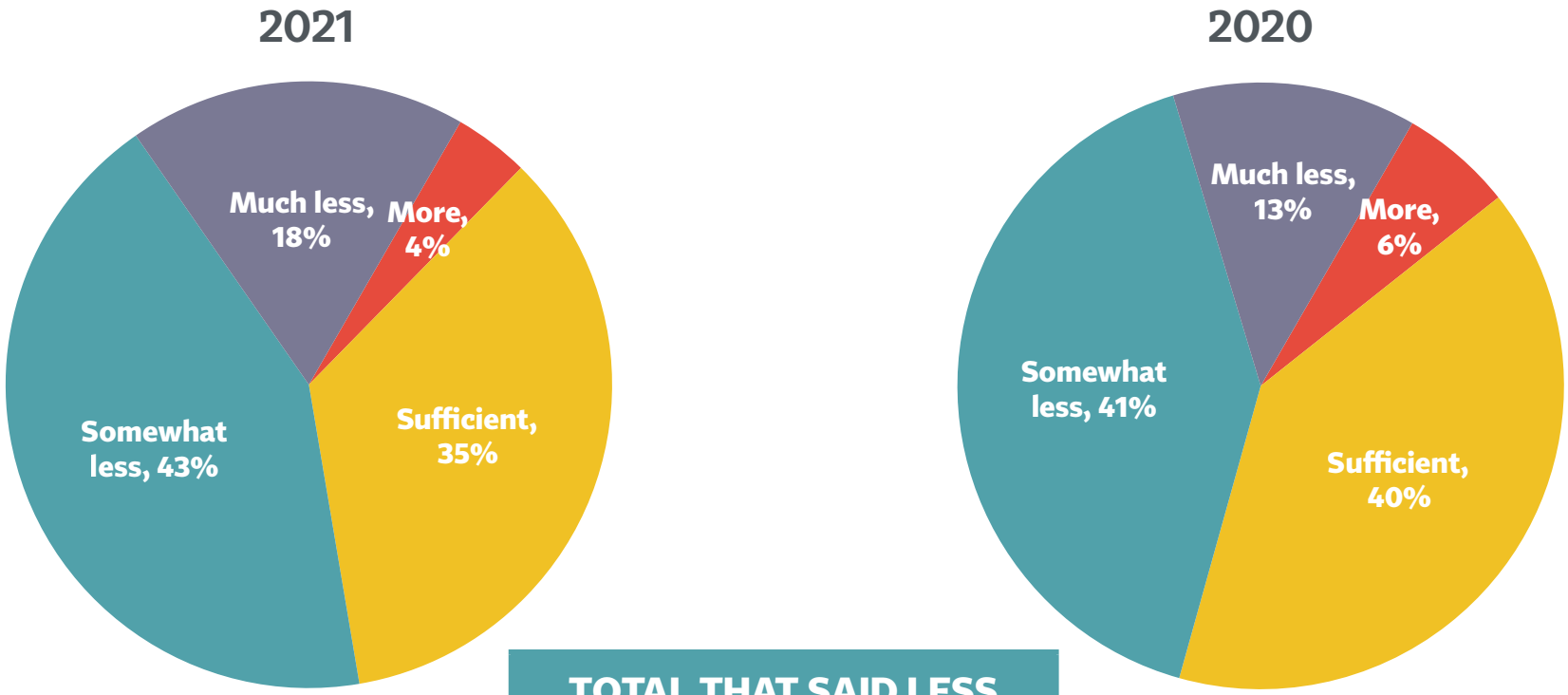


F3b: Who makes privacy budgeting/purchasing decisions at your organization?

After dropping in 2020, the proportion feeling their budget is less than sufficient to meet their needs is back up to 2019 levels

How sufficient is privacy budget versus obligations?

(Base: Director or higher)

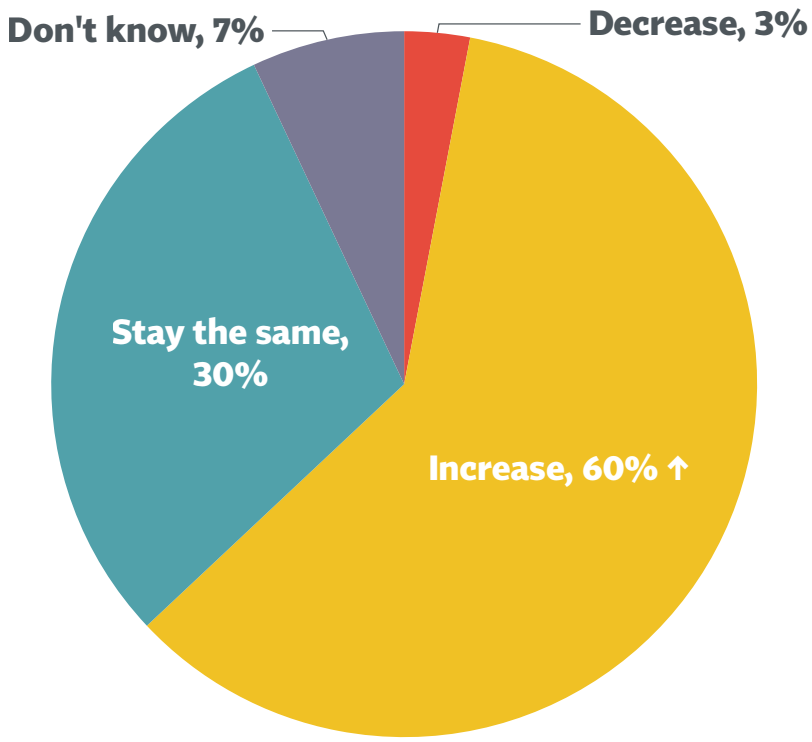


TOTAL THAT SAID LESS THAN SUFFICIENT
2021: 61%
2020: 54%
2019: 62%
2018: 65%

F6: How sufficient would you say that your company's privacy budget is to meet your privacy obligations?

6 in 10 privacy pros expect their budget to increase over the next 12 months, while almost none expects it to decrease

In next 12 months, privacy budget will ...
(Base: Director or higher)



↑ Significantly different from 2020

% privacy budget increase/decrease
(Base: Director or higher)

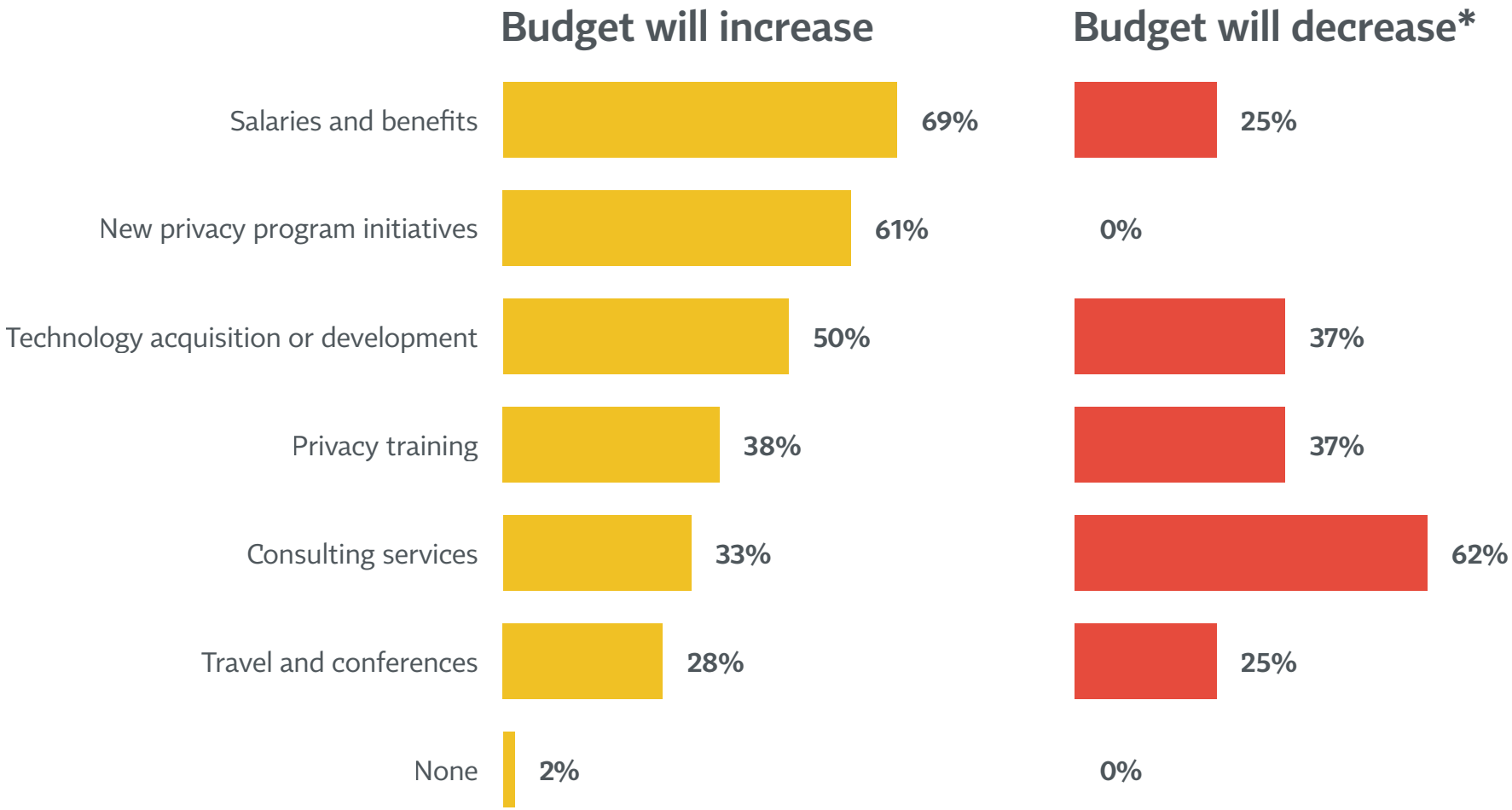
	Budget will increase	Budget will decrease*
Mean % change	32%	-22%
Median % expected change	20%	-20%

* Small sample size

F5: In the next 12 months, you expect your company's privacy budget will …
F5a: By how much do you expect the total amount your company spends on privacy, including salaries and benefits, will [increase/decrease] in the next 12 months?

Among those expecting a budget increase, most think it will go to salaries; most expecting a decrease foresee cuts to consulting

Impact of budget increase/decrease
(Base: Director or higher)



** Extremely small sample size (n=8); interpret with caution*

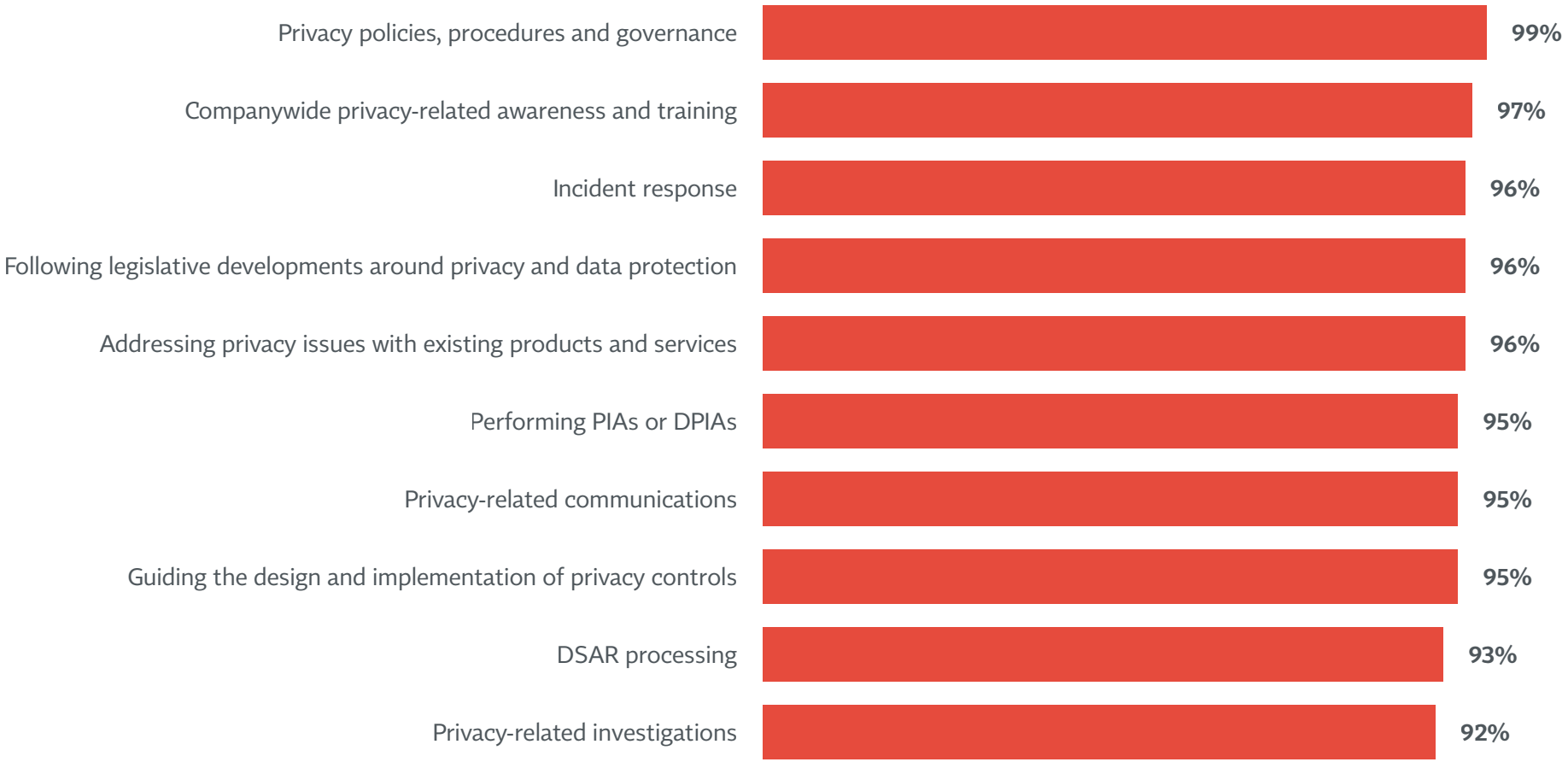
F5b: Will the change in spend affect any of the following?

Contents

Privacy policies, training and incident response are among the tasks virtually all privacy teams are responsible for

Privacy team responsibilities

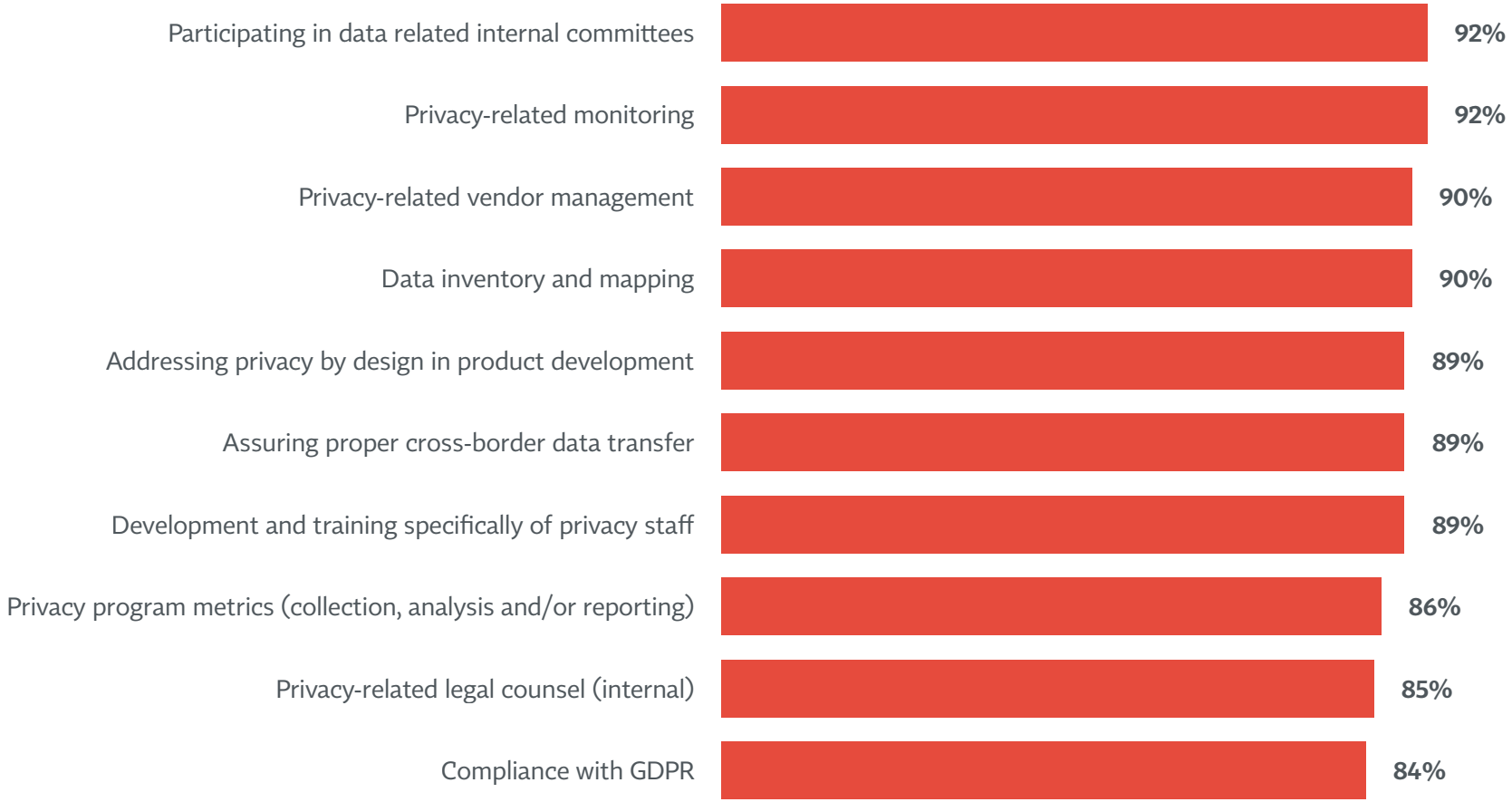
(Respondents could choose as many as they liked, includes those saying I do this and privacy team does this)



D4c/d: Which of the following are you or someone else on the privacy team responsible for accomplishing on an annual basis?

Data-related committees, monitoring and vendor management are additional tasks most privacy teams engage in

Privacy team responsibilities
(Respondents could choose as many as they liked, includes those saying I do this and privacy team does this)

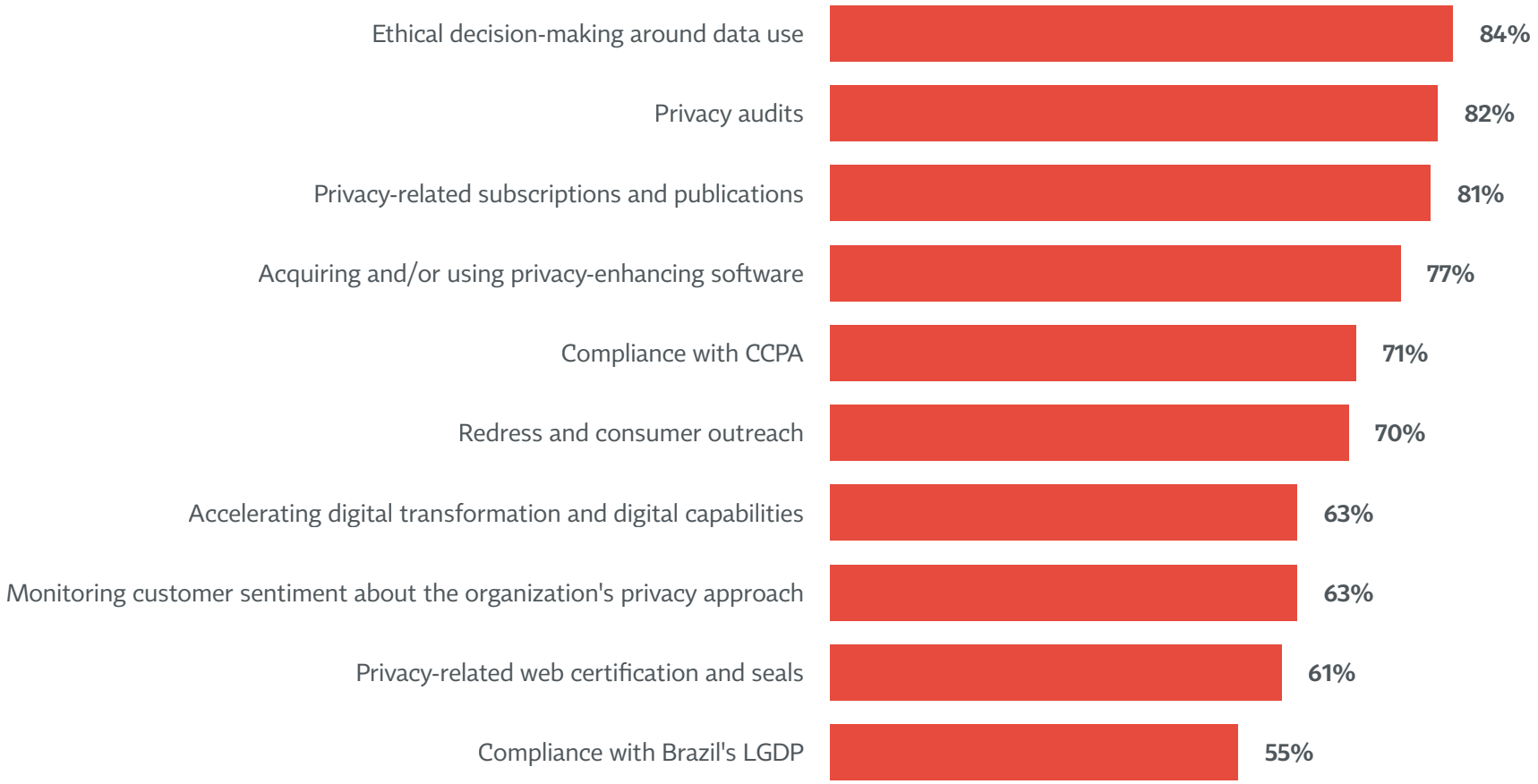


D4c/d: Which of the following are you or someone else on the privacy team responsible for accomplishing on an annual basis?

Digital transformation, customer sentiment monitoring and privacy web certs/seals are tasks undertaken by fewer privacy teams

Privacy team responsibilities

(Respondents could choose as many as they liked, includes those saying I do this and privacy team does this)



D4c/d: Which of the following are you or someone else on the privacy team responsible for accomplishing on an annual basis?

US-based privacy pros focus more on vendors, CCPA and LGPD, and consumer sentiment than EU peers

BY COMPANY HQ

	U.S.	EU
Privacy responsibilities		
Privacy-related vendor management	**95%**	90%
Compliance with GDPR	83%	**98%**
Compliance with CCPA	**92%**	40%
Monitoring customer sentiment about the organization's privacy approach	**65%**	49%
Compliance with Brazil's LGPD	**68%**	33%

Significantly different than other segments

On the whole, the smallest firms by revenue have fewer privacy responsibilities than the largest firms

BY COMPANY REVENUE

	<$100M	$100M–$999M	$1B–$24.9B	$25B+
Privacy responsibilities				
Companywide privacy-related awareness and training	**94%**	98%	99%	100%
Following legislative developments around privacy and data protection	**92%**	97%	99%	100%
Guiding the design and implementation of privacy controls	**91%**	96%	99%	97%
DSAR processing	**85%**	94%	98%	100%
Participating in data-related internal committees	84%	94%	**98%**	100%
Assuring proper cross-border data transfer	**80%**	91%	93%	98%
Privacy program metrics (collection, analysis and/or reporting)	85%	**77%**	92%	94%
Compliance with CCPA	56%	66%	**83%**	**98%**
Compliance with Brazil's LGPD	44%	48%	62%	**85%**

Significantly different than other segments

Similarly, the smallest firms by employee size also tend to have fewer responsibilities than larger firms

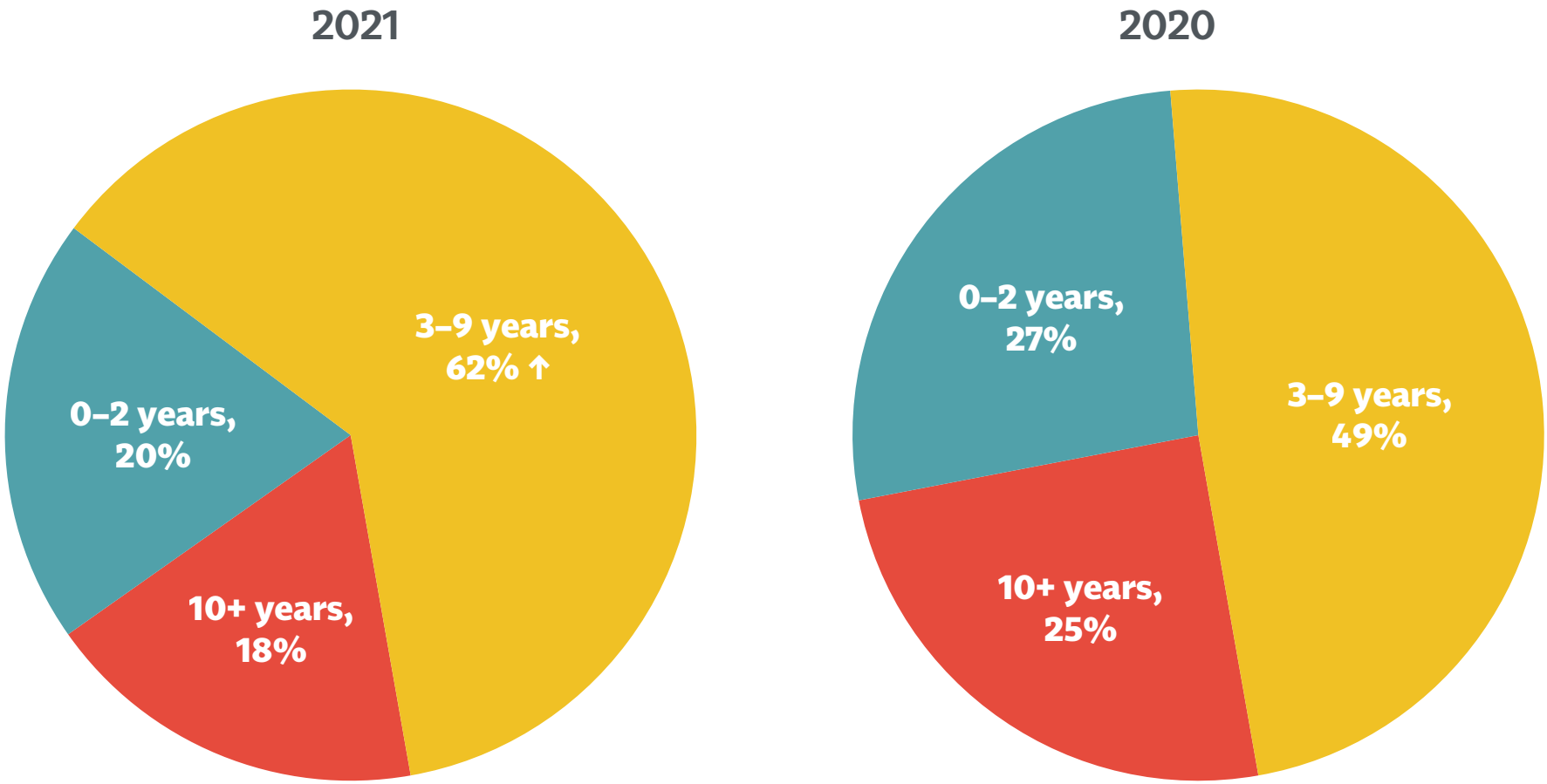
BY NUMBER OF EMPLOYEES

	<5K	5–24.9K	25–74.9K	75K+*
Privacy responsibilities				
Privacy-related communications	**92%**	99%	98%	100%
DSAR processing	**89%**	96%	98%	98%
Participating in data-related internal committees	**88%**	95%	100%	100%
Development and training specifically of privacy staff	**84%**	94%	94%	98%
Privacy program metrics (collection, analysis and/or reporting)	**81%**	90%	96%	96%
Privacy-related legal counsel (internal)	**80%**	87%	98%	90%
Compliance with CCPA	**60%**	74%	**94%**	**97%**
Compliance with Brazil's LGPD	**45%**	57%	69%	**84%**

Significantly different than other segments * Small sample size

Privacy programs are maturing: 6 in 10 firms have had a privacy program for 3 to 9 years, up from just half in 2020

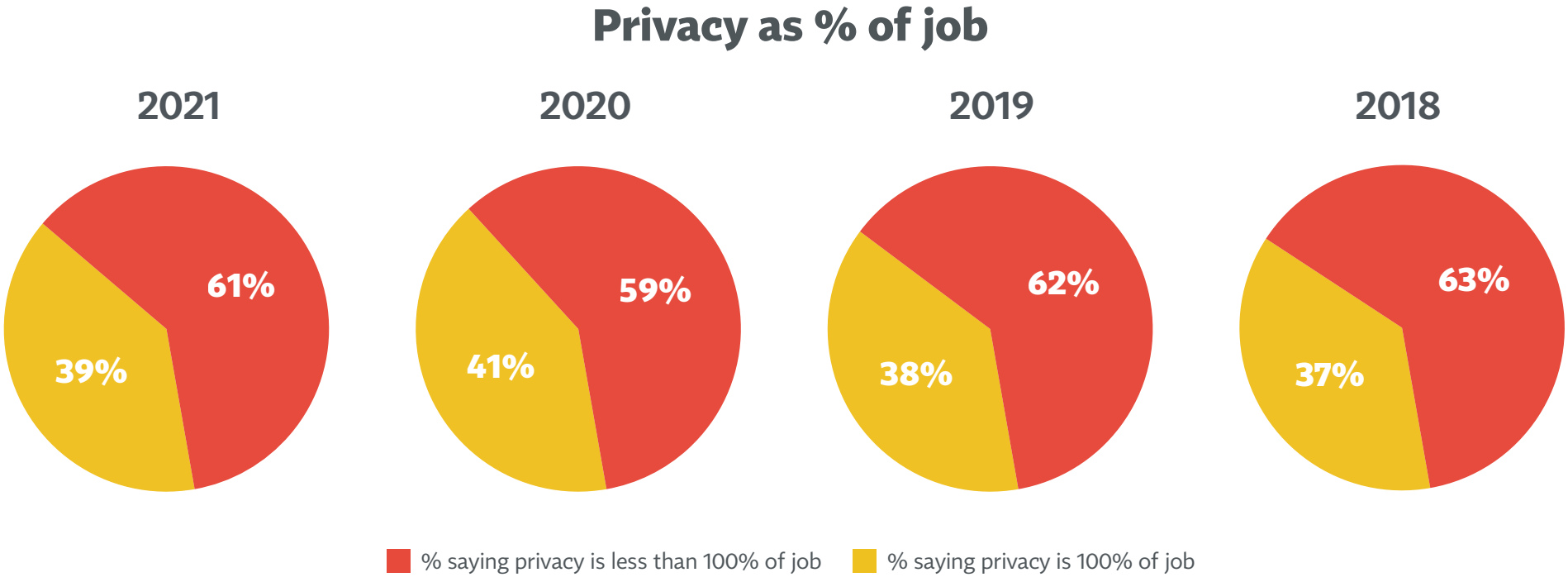
Number of years with privacy program



↑ Significantly different from 2020

E2: For how many years has your company had a dedicated privacy program?

4 in 10 respondents work exclusively on privacy, while the remainder divide their time with other tasks



PRIVACY AS % OF TOTAL JOB (MEAN)
2021: 76%
2020: 73%
2019: 72%
2018: 71%

D1: About what proportion of your work and time revolves around privacy responsibilities?

Privacy pros at the smallest firms spend less of their time on privacy than those in larger firms

BY EMPLOYEE SIZE

	<5K	5K–24.9K	25K–74.9K	75K+*
Mean % of time spent on privacy	**69%**	**83%**	**88%**	**93%**

BY COMPANY REVENUE

	<$100M	$100M–$999M	$1B–$24.9B	$25B+*
Mean % of time spent on privacy	**69%**	72%	**83%**	**91%**

BY COMPANY REVENUE

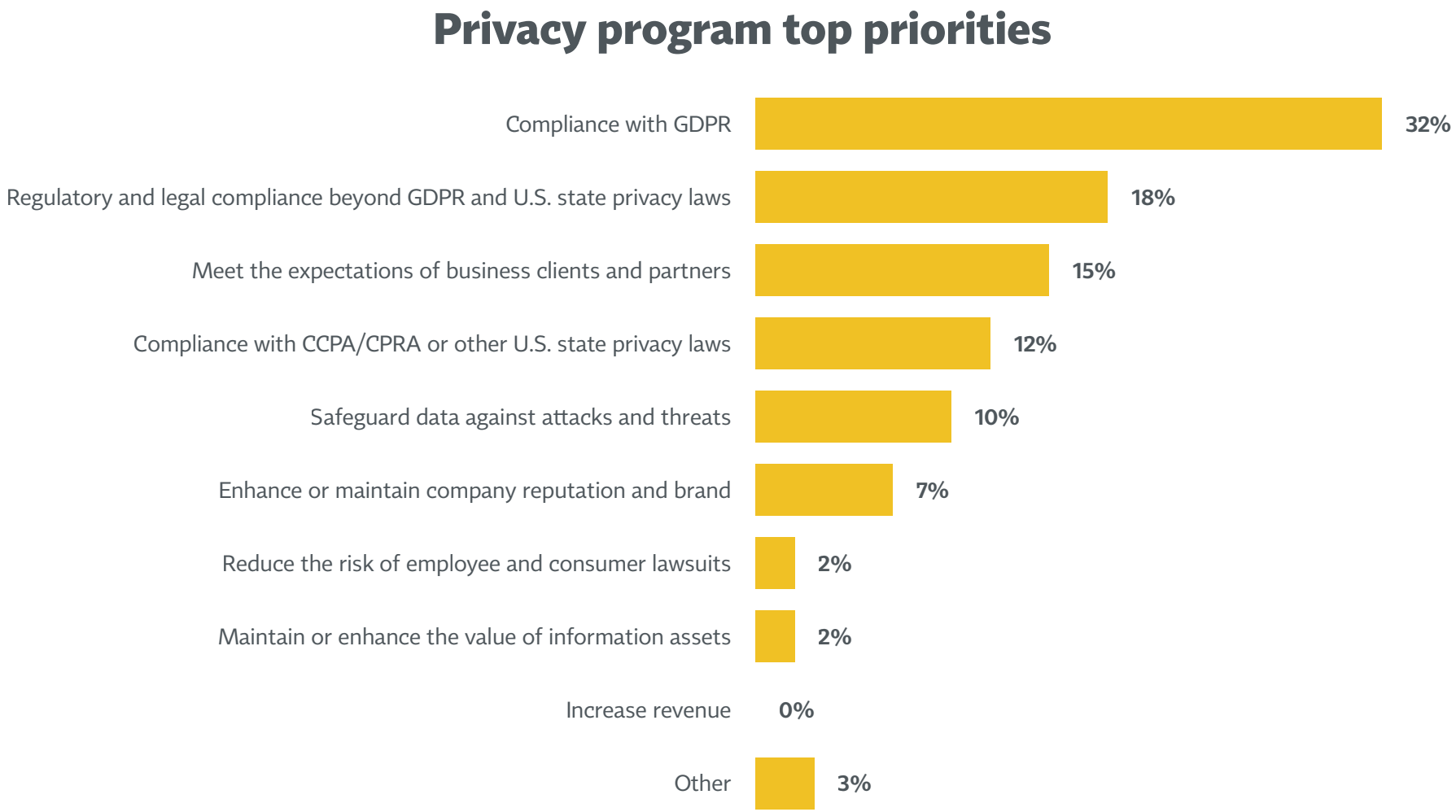
	<$100M	$100M–$999M	$1B–$24.9B	$25B+*
Median % of time spent on privacy	80%	80%	100%	100%

Significantly different than other segments

* Small sample size

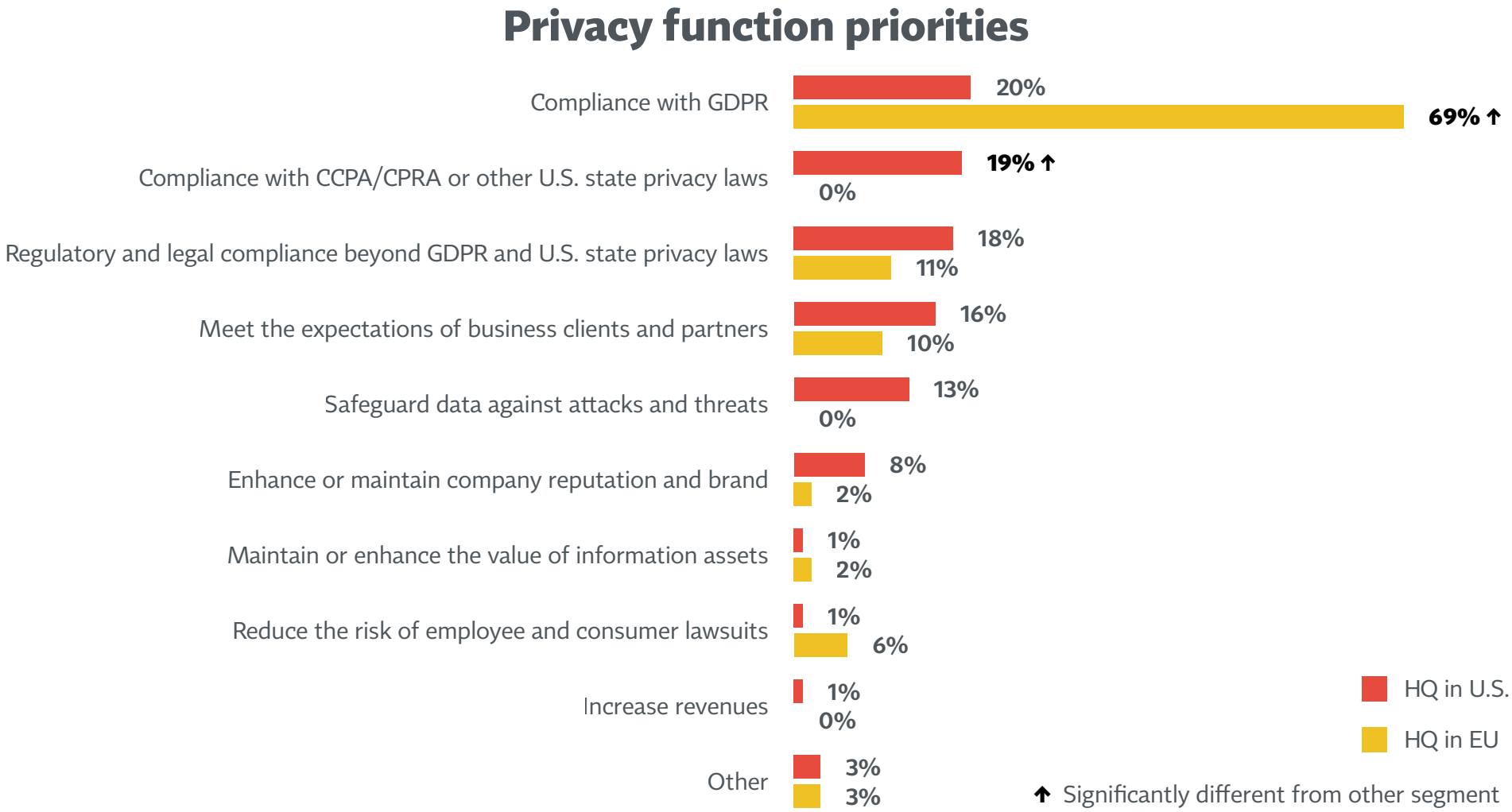
Contents

Compliance with GDPR, US state laws, such as CCPA/CPRA, and other laws and regulations continue to rank as top privacy priorities



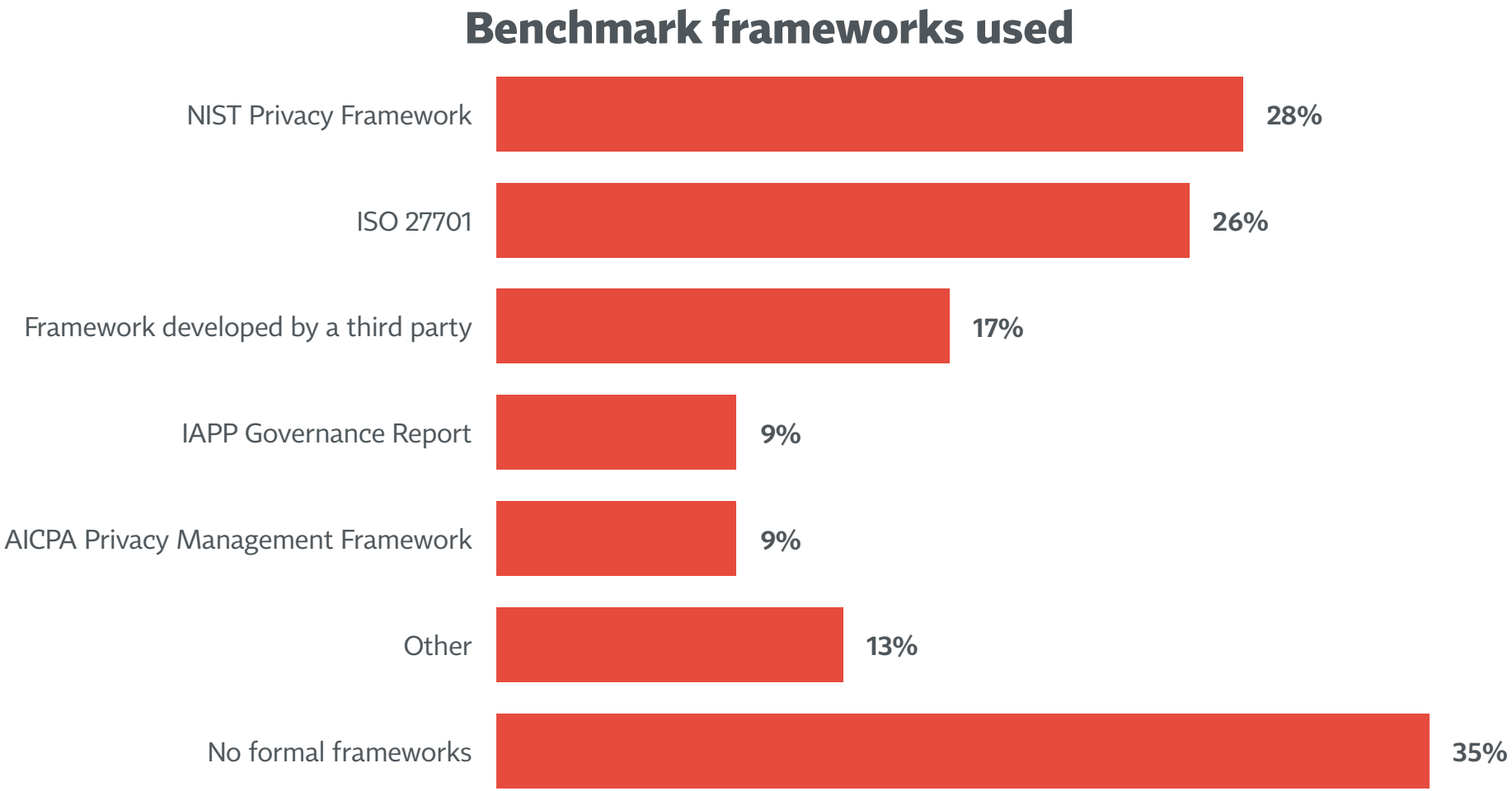
E3: Which of the following is the highest priority within your privacy program?

Whereas nearly 7 in 10 EU privacy pros rate GDPR compliance as their top priority, only 2 in 10 US privacy pros do so



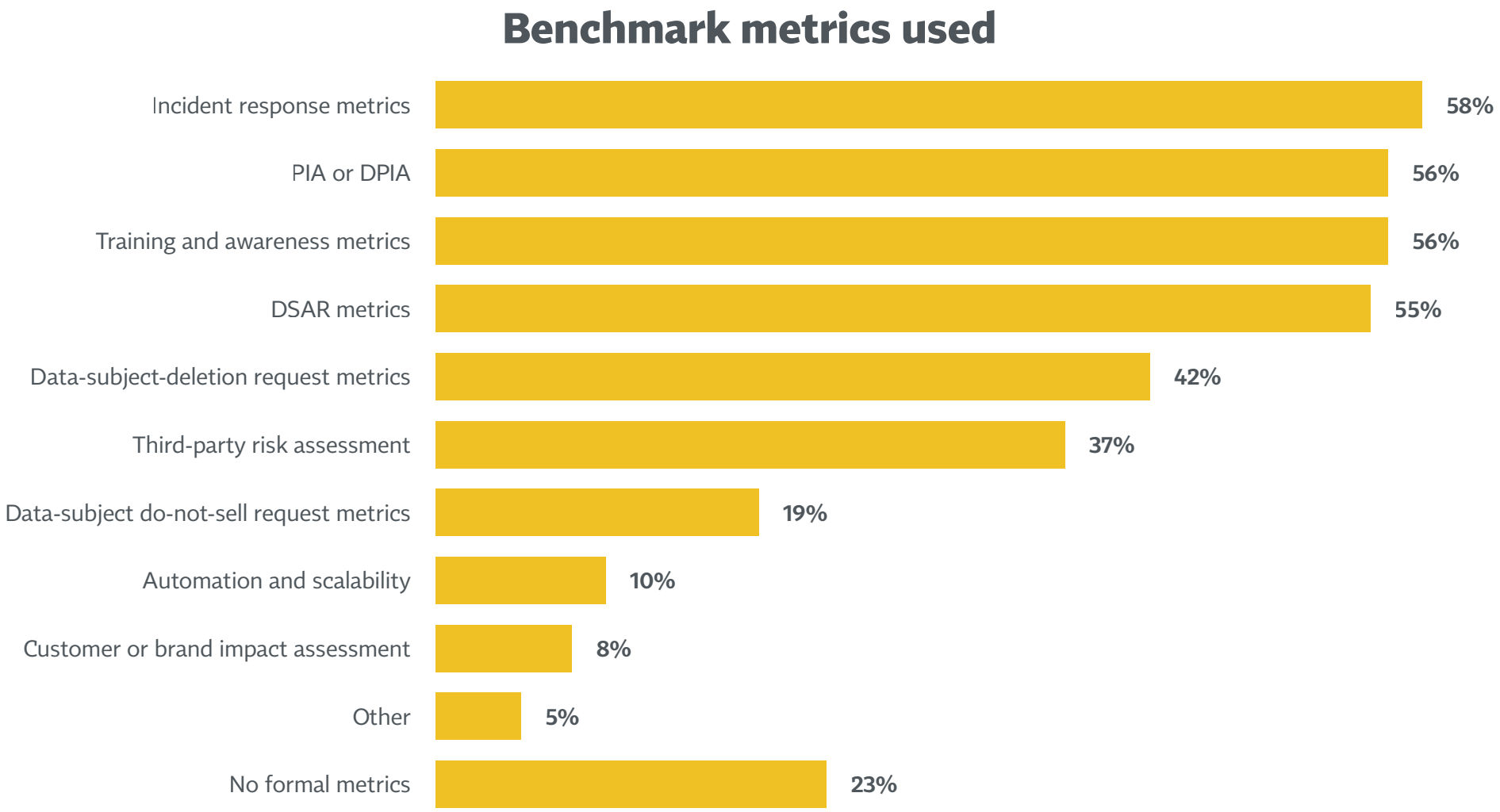
E3: Which of the following is the highest priority within your privacy program?

More than 1 in 4 organizations use NIST's Privacy Framework or ISO 27701 as benchmarks



F42: Which framework(s) does/do you use to measure/benchmark your privacy program?

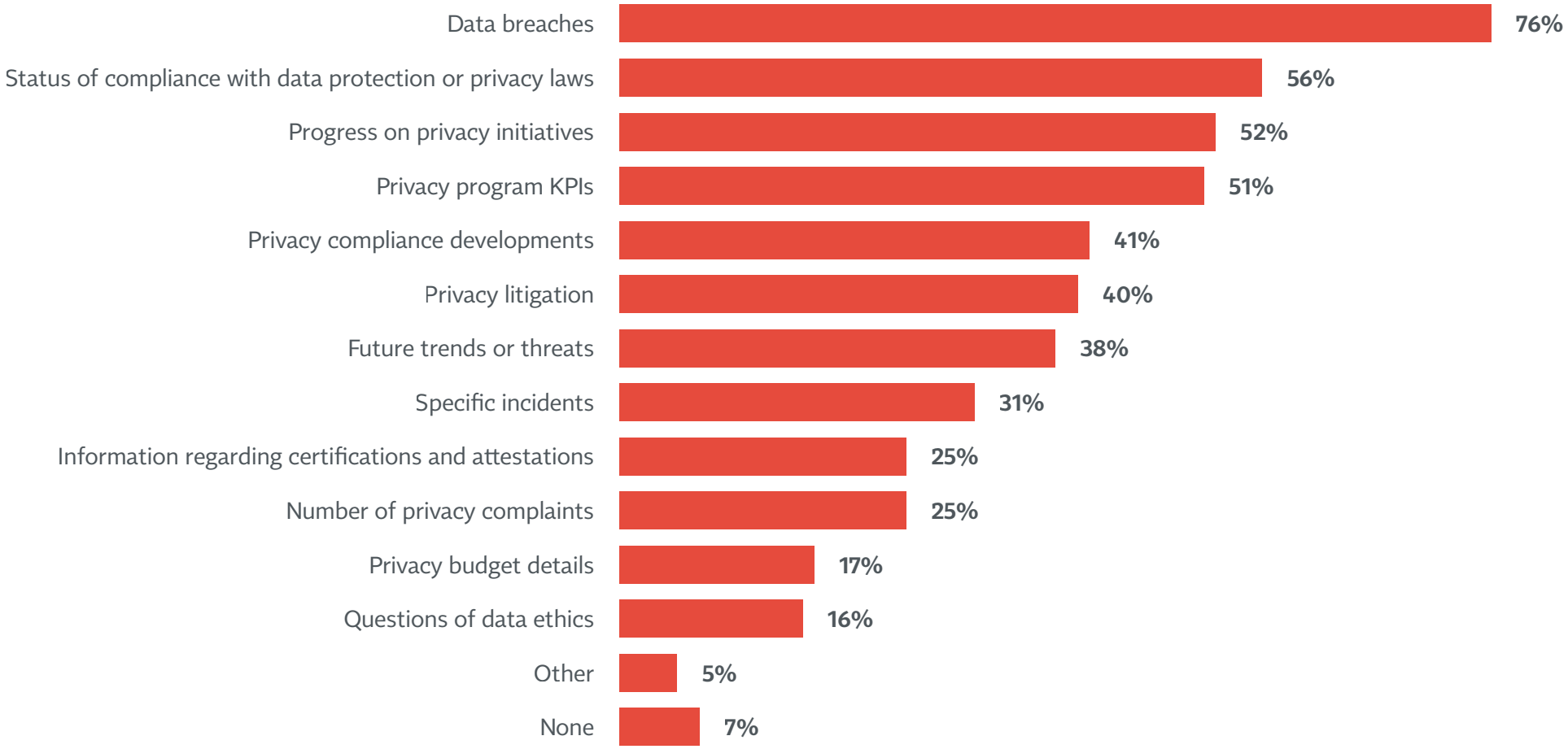
The most common metrics used for benchmarking involve incident response, impact assessments, training and DSRs



F43: Which metrics do you use to measure/benchmark privacy program performance?

Data breaches are the topic privacy teams most commonly report to the board, followed by status of privacy law compliance

Specific privacy topics reported to board
(Base: Director or higher)



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

Tech/telecom companies more likely to report privacy compliance, incidents and information regarding certs/ attestations to the board

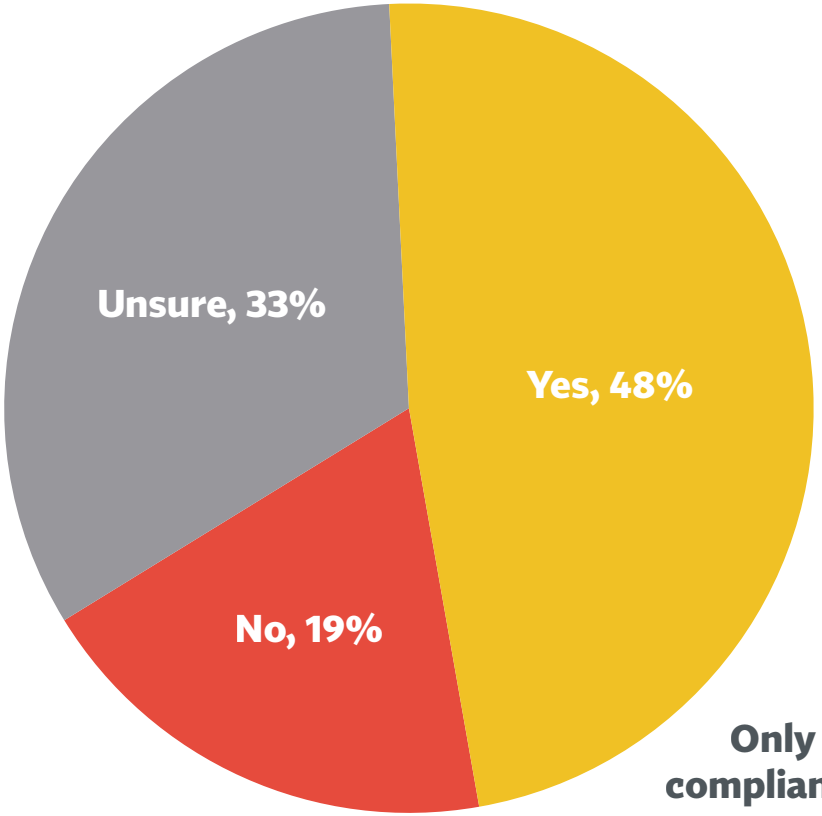
BY INDUSTRY

	Financial services and insurance	Health care and pharma	Tech/ telecomm	Government
Topics reported to the board				
Privacy compliance developments	40%	**21%**	**55%**	33%
Specific incidents	33%	24%	**41%**	53%
Information regarding certification/attestations	14%	17%	**41%**	13%
Number of privacy complaints	31%	27%	23%	**47%**

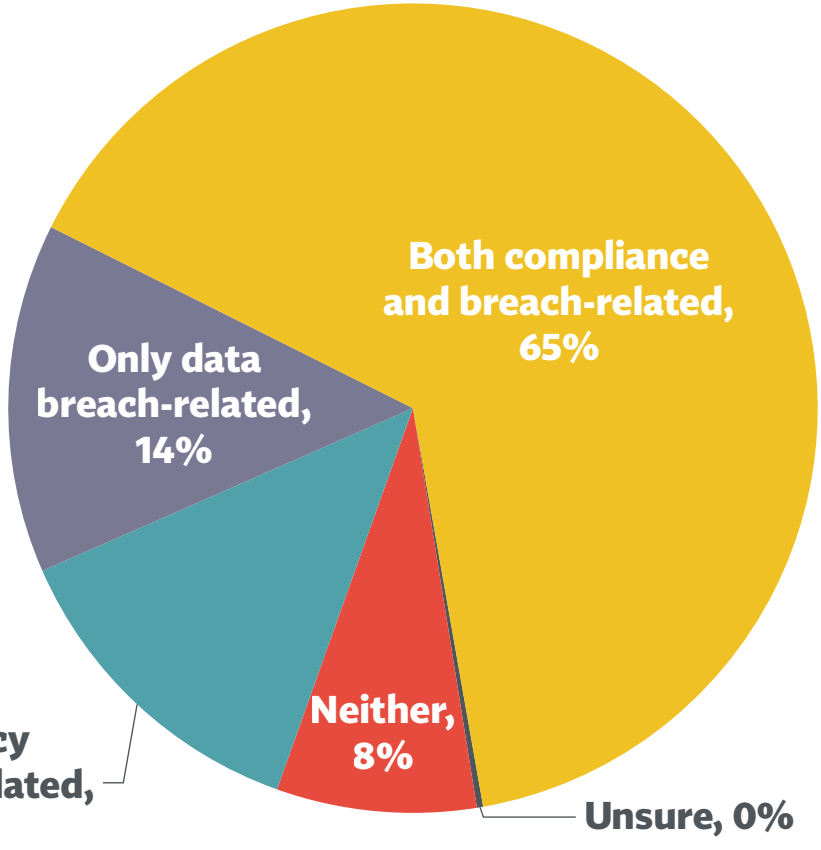
Significantly different than other segments

Half of publicly traded firms include privacy issues in disclosures and reports; most said both compliance and data breach risks are reported

Privacy risks communicated
(Base: Publicly traded)



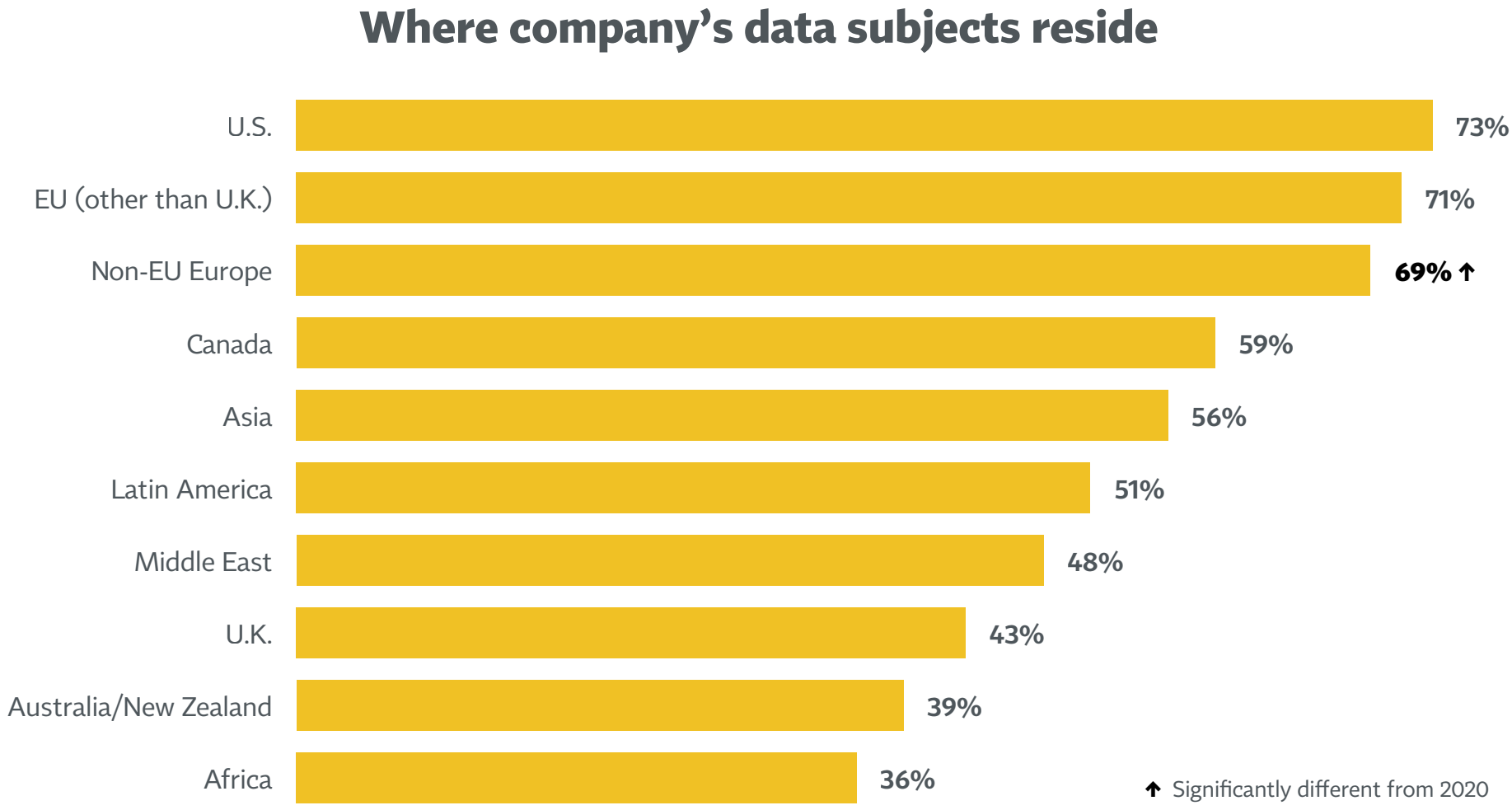
What is communicated
(Base: Privacy items disclosed)



F45: Are your organization's privacy-related risks included in any financial notices, disclosures, shareholder communications or annual reports?
F46: Do these financial notices, disclosures, shareholder communications or annual report mention data breach–related risks or privacy compliance–related risks (such as regulatory fines, litigation or class actions), or both?

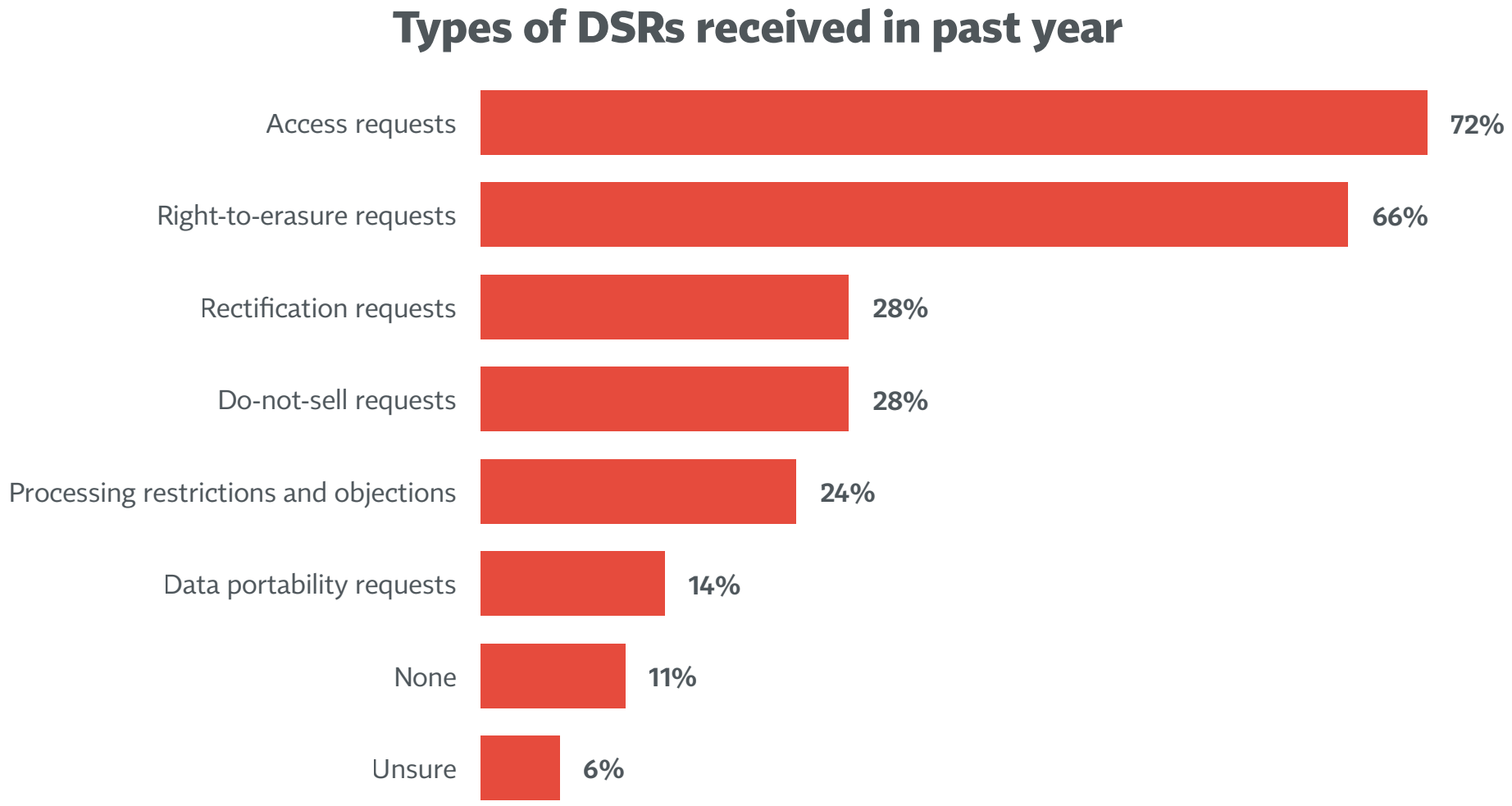
Contents

3 in 4 firms collect information from data subjects in the US, slightly more than those collecting information from EU data subjects



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

Access requests and right-to-erasure requests are the most common DSRs across firms, with at least two-thirds receiving them



R2: Which types of data subject requests has your organization received over the past year?

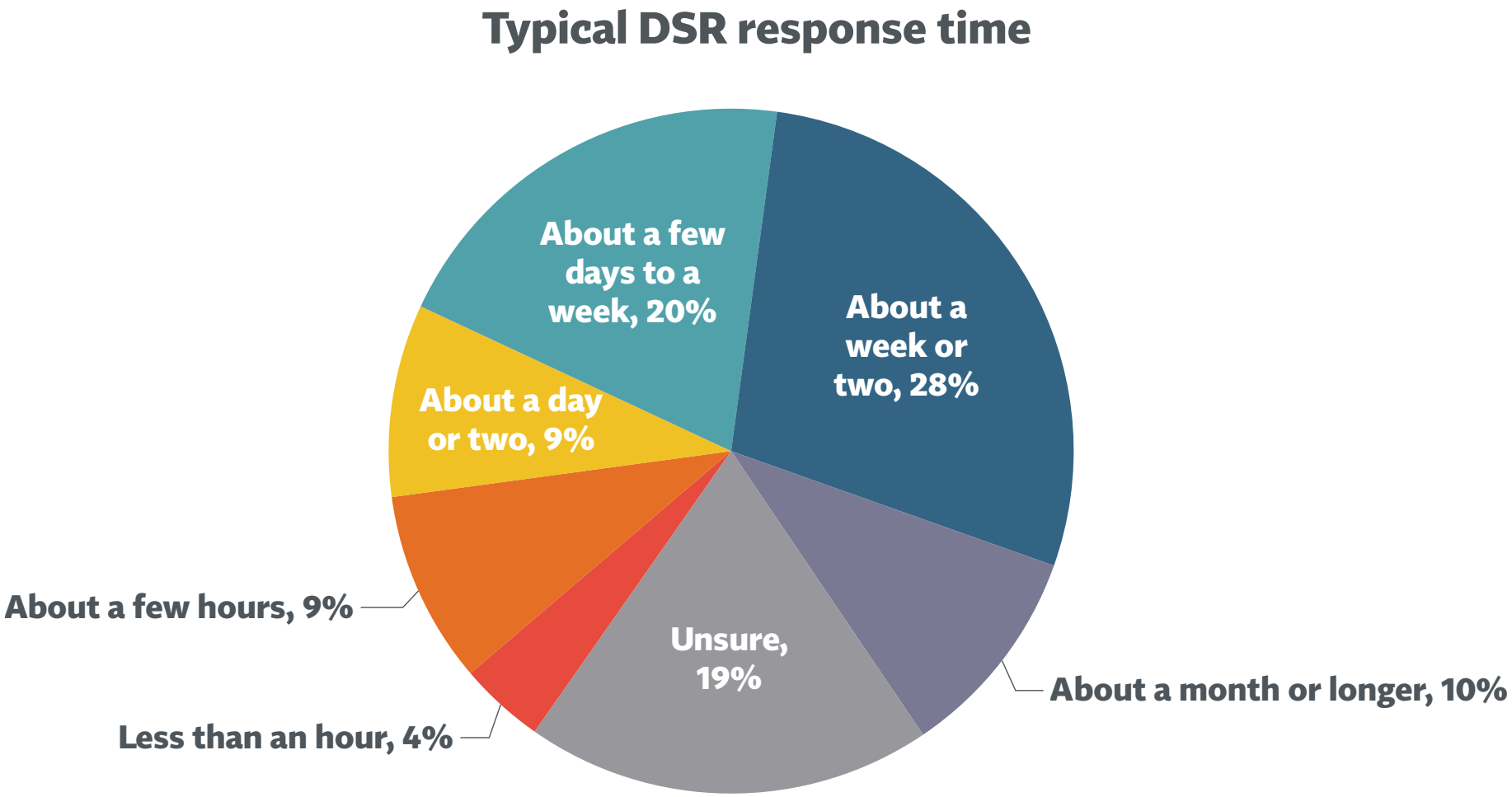
More tech/telecom companies receive do-not-sell requests compared to other industries, while government agencies are least likely to receive DSRs

BY INDUSTRY

	Financial services and insurance	Health care and pharma	Tech/ telecomm	Government
Type of DSR				
Right-to-erasure requests	57%	62%	71%	**32%**
Do-not-sell requests	**13%**	25%	**38%**	**3%**
Data portability requests	18%	8%	12%	**3%**

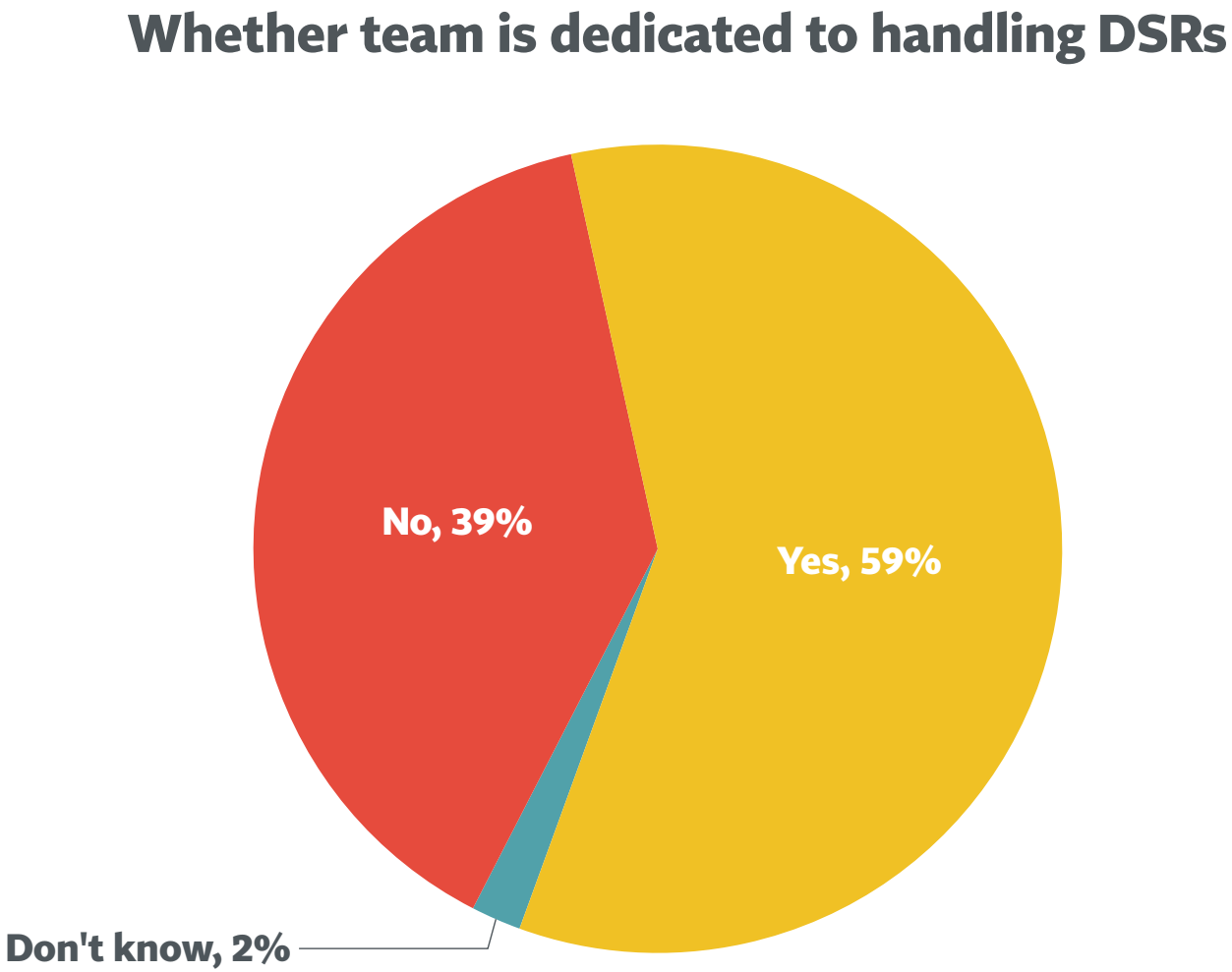
Significantly different than other segments

Most firms said they usually take at least a few days to respond to DSRs, with nearly 4 in 10 saying they take at least a week



R5: For most data subject requests, approximately how long does it take your organization to respond to each request?

6 in 10 organizations have a team dedicated to handling DSRs



R6: Is there a team at your company dedicated to handling data subject requests?

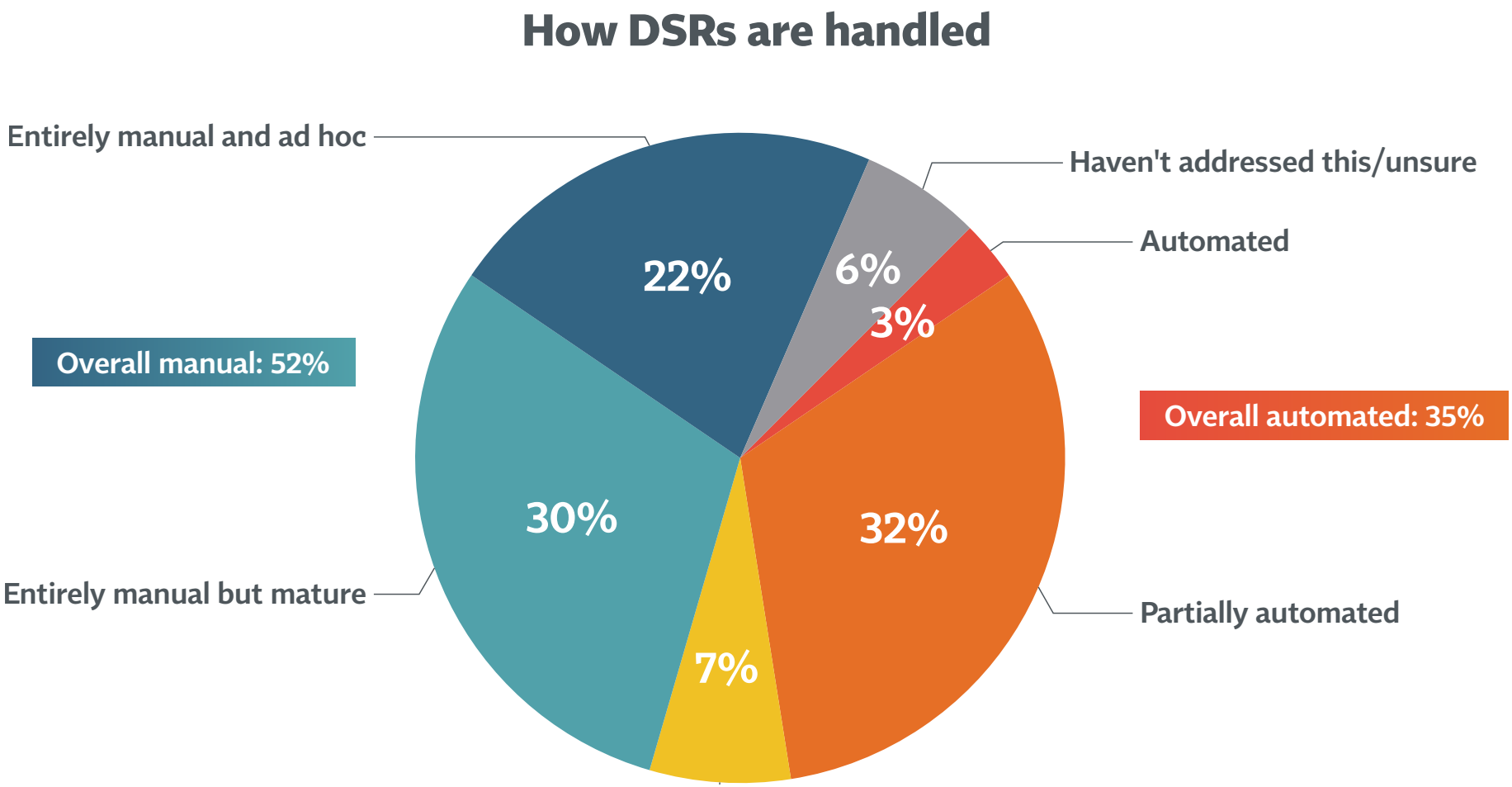
Compared to other industries, a smaller proportion of tech/telecom companies have a dedicated team in place to handle DSRs

BY INDUSTRY

	Financial services and insurance	Health care and pharma	Tech/ telecomm	Government
Have a team for handling DSRs				
Yes	71%	47%	**49%**	49%
No	**22%**	51%	**48%**	46%
Unsure	**7%**	2%	3%	5%

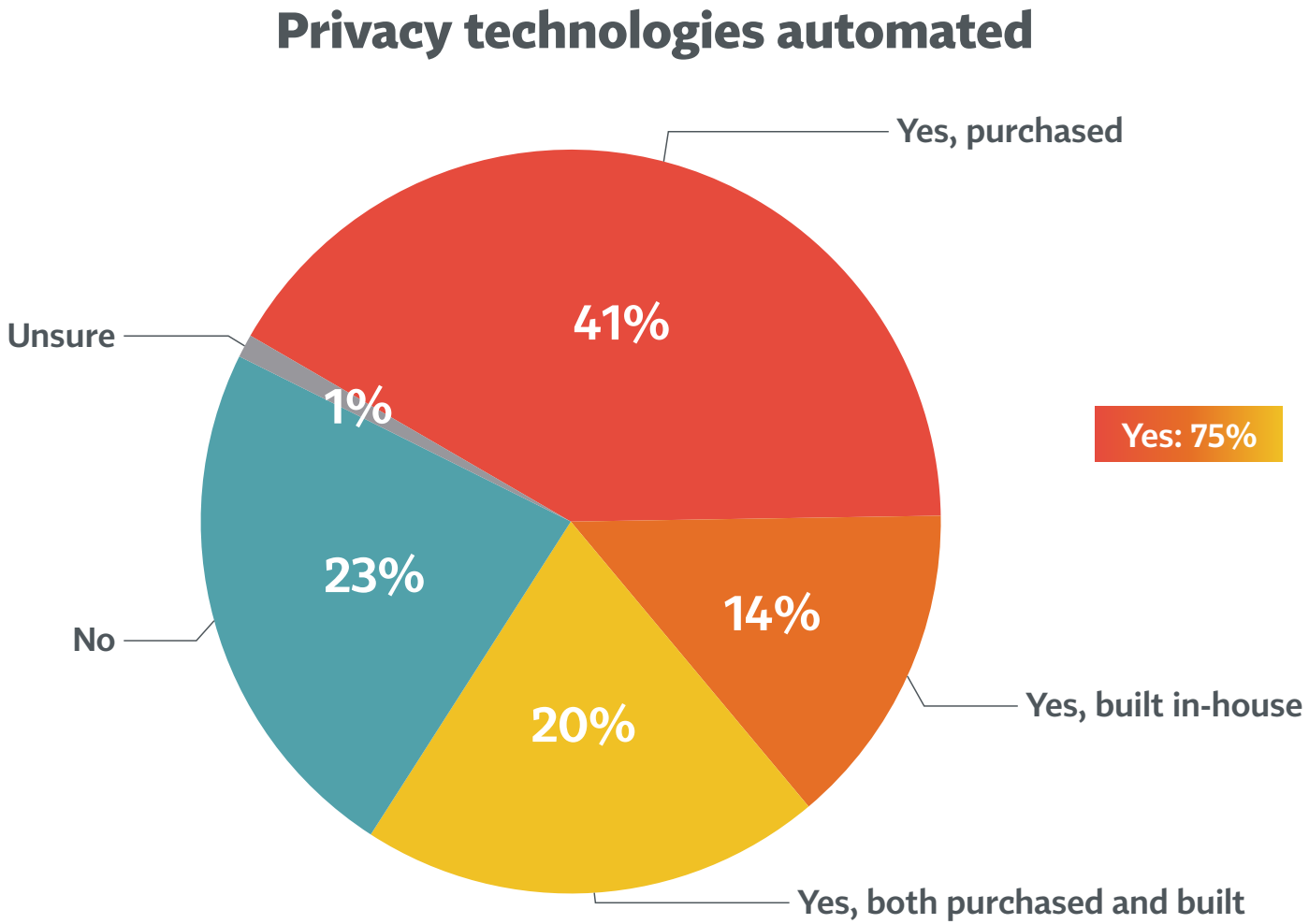
Significantly different than other segments

More than half of organizations handle DSRs manually, while 1 in 3 have automated the process



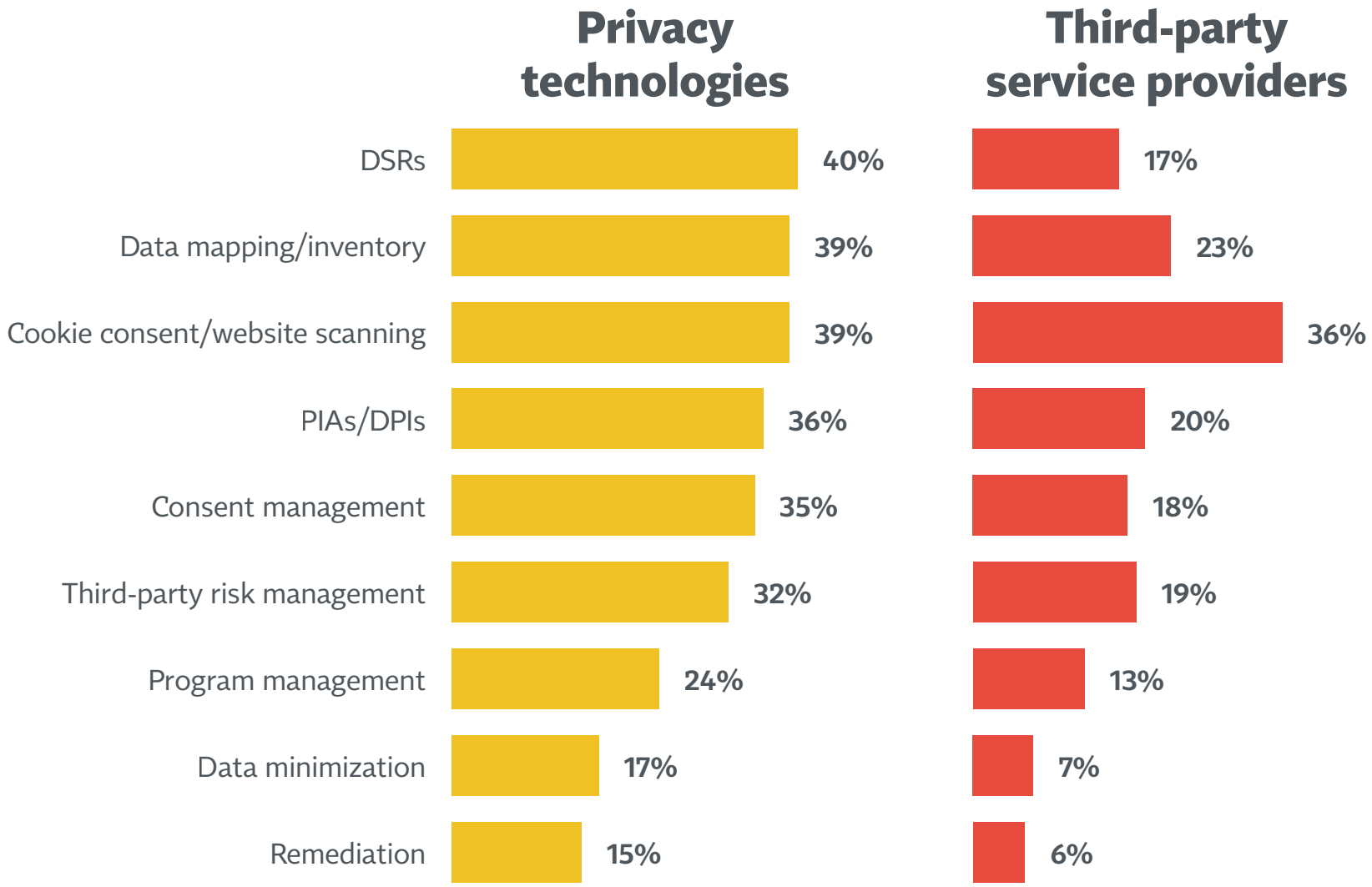
J23: How is your company addressing data subject requests, such as access, portability, right to be forgotten requests or objections to processing?

Across all privacy functions, about 3 in 4 firms have some automated technologies in place, with most having purchased them



P3: Has your organization purchased or built privacy technologies to automate any portions of your privacy program?

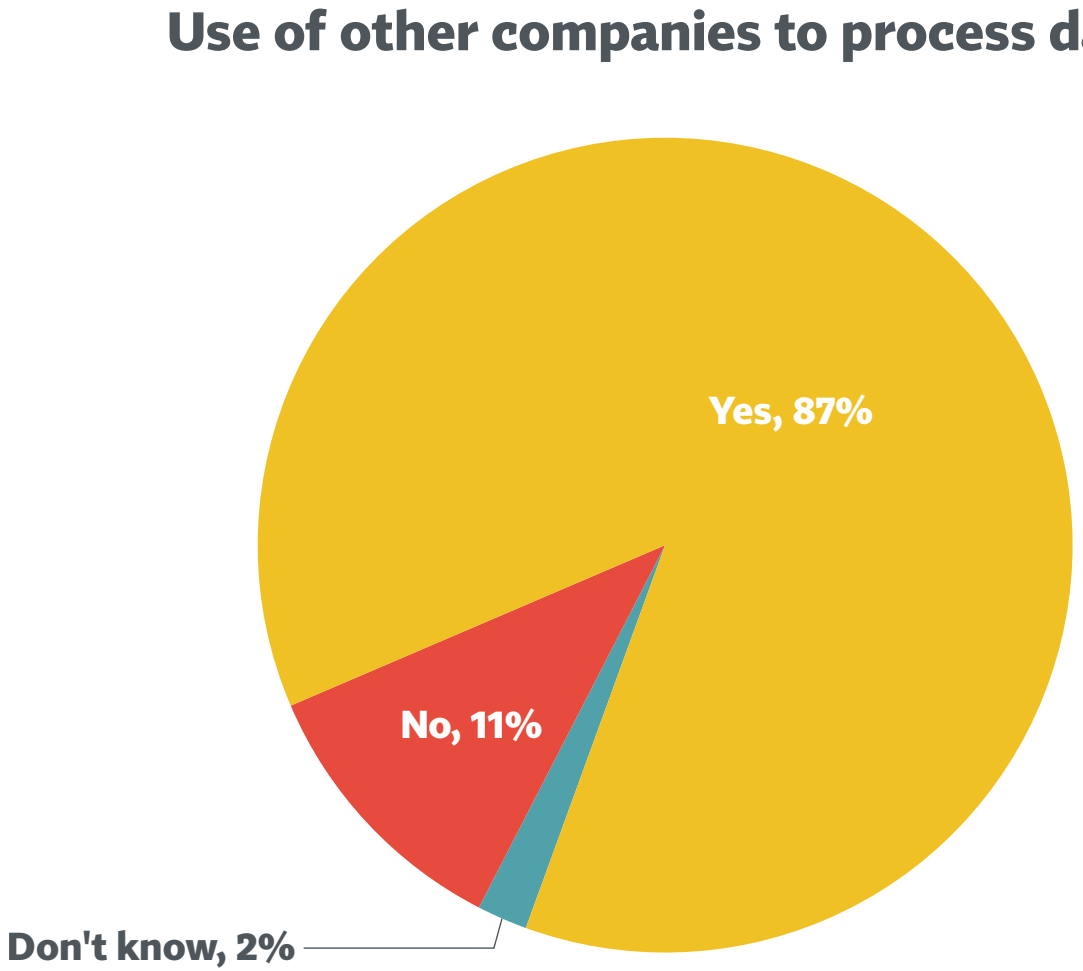
Privacy technologies are most frequently used for DSRs, data mapping, cookie consent and DPIAs, each more often than service providers



P4: Has your organization used privacy technologies or third-party service providers to perform any of the following tasks? Please check all that apply — if you have used both for a given task, select both.

Contents

The vast majority of firms (87%) use vendors to process personal data



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

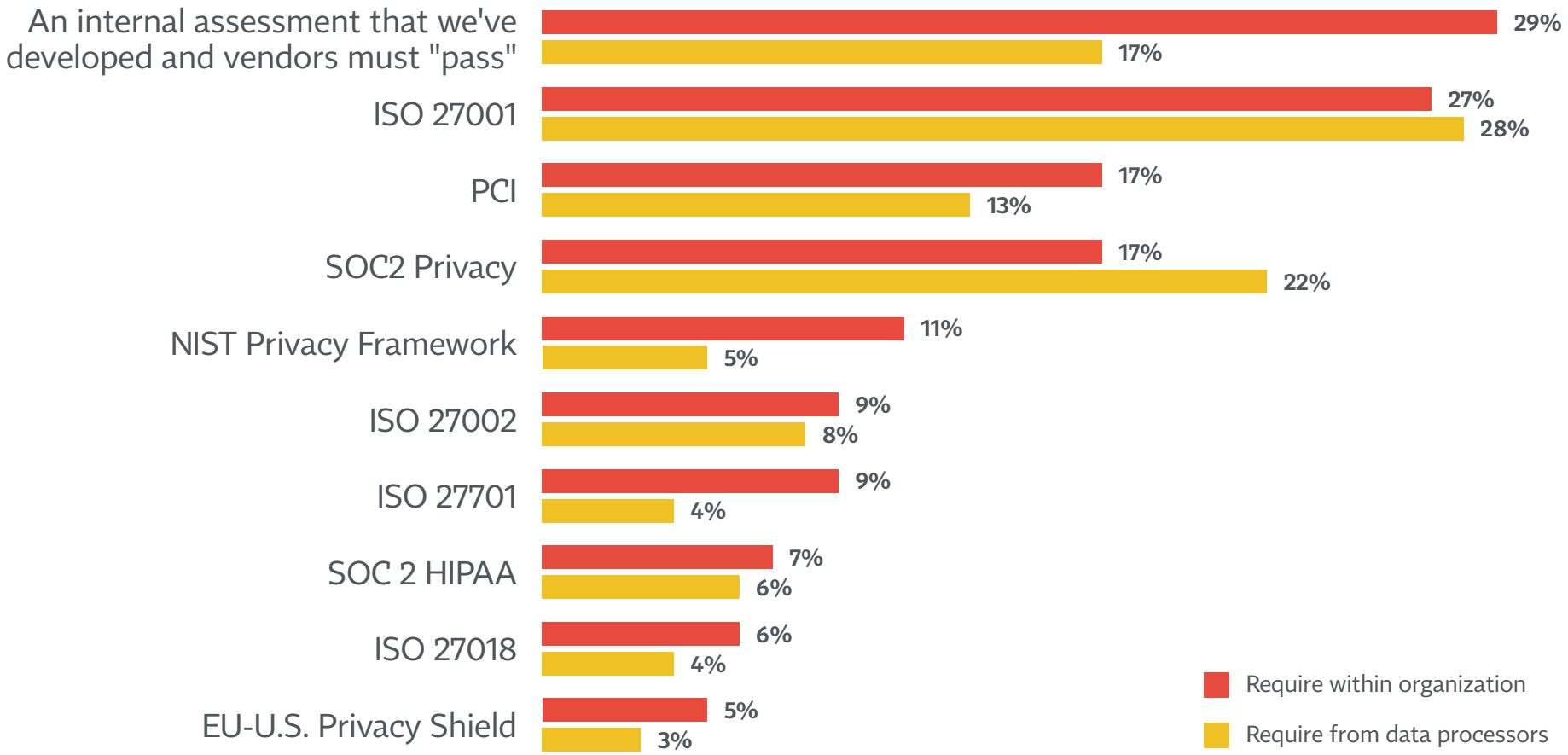
Contractual assurances, questionnaires and third-party audits are the most commonly used vendor accountability tools

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?

Internally developed assessments and ISO 27001 are the most common certs required within organizations

Certifications and audits required



K3: Which, if any, third party audits or certifications does your company require within your organization or from its data processors?

US firms are more likely than EU firms to require a variety of certifications, including SOC2 Privacy and NIST's Privacy Framework

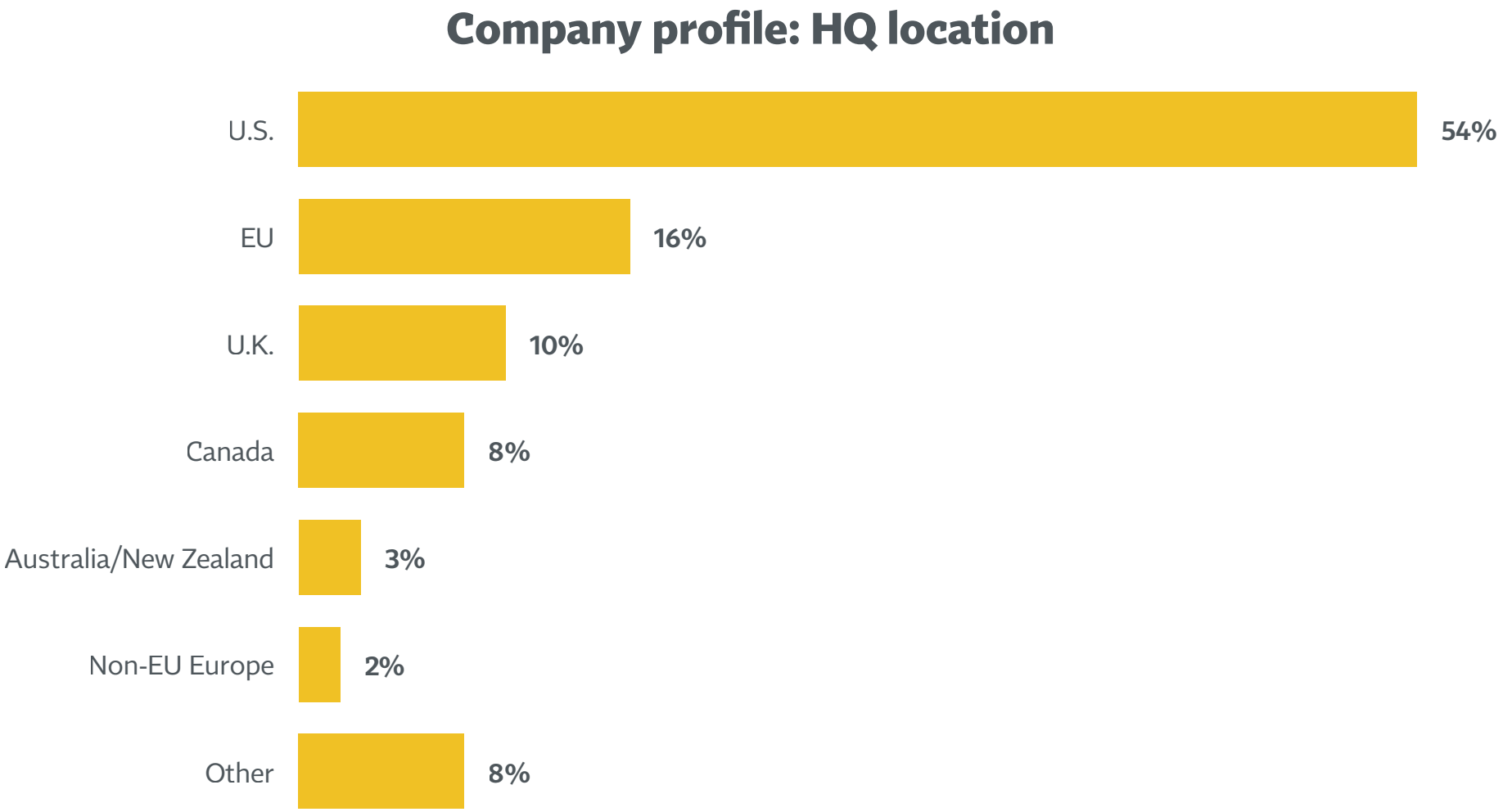
BY HQ LOCATION

	U.S.	EU
Require within organization		
SOC2 Privacy	**24%**	7%
NIST Privacy Framework	**16%**	7%
SOC 2 HIPAA	**10%**	2%
EU-U.S. Privacy Shield	**8%**	0%
TrustArc (formerly TRUSTe)	**5%**	0%
Require from data processors		
SOC2 Privacy	**28%**	14%

Significantly different than other segments

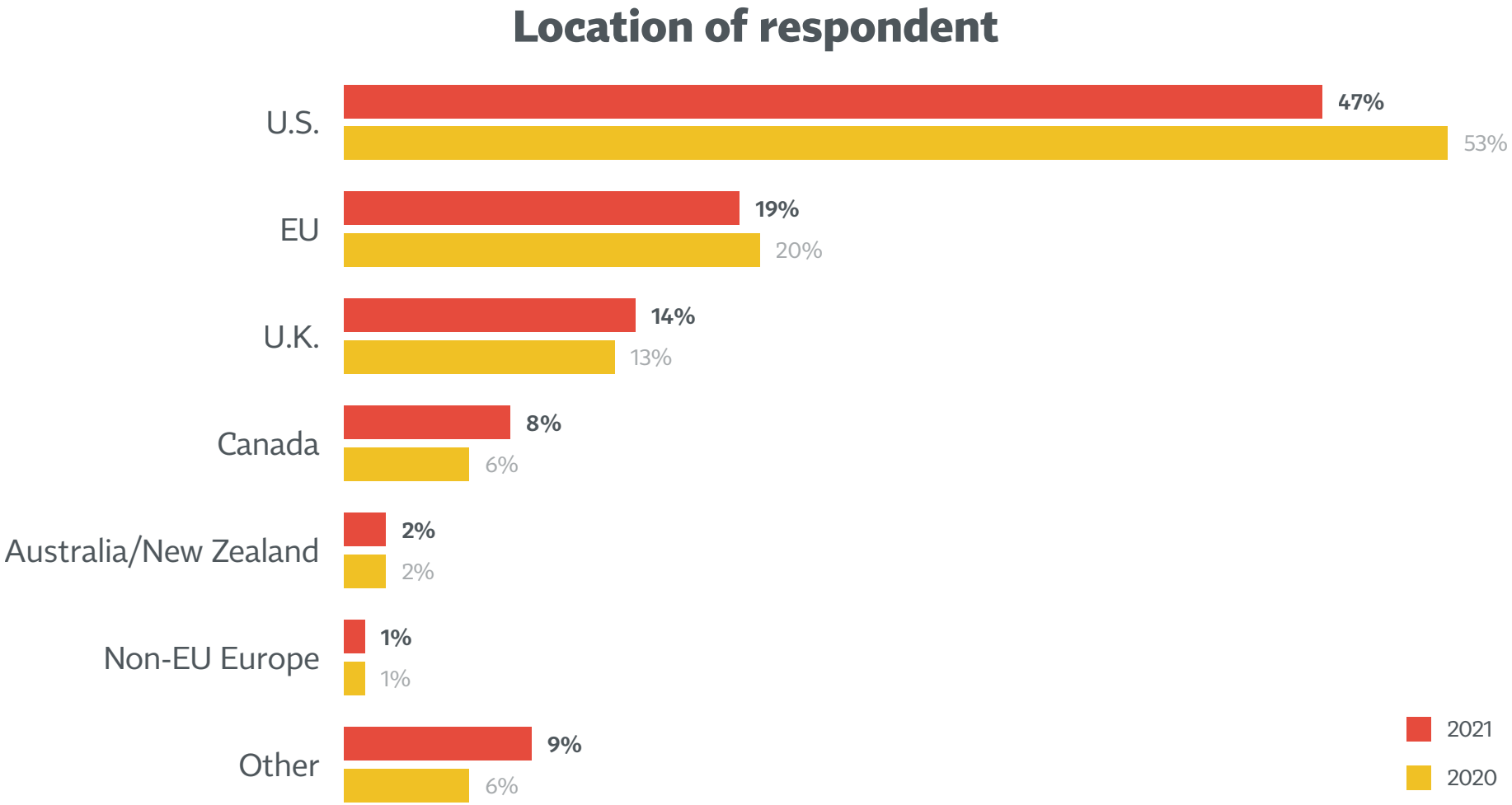
Contents

8 in 10 respondents work for a firm headquartered in either the US (54%), EU (16%) or UK (10%)



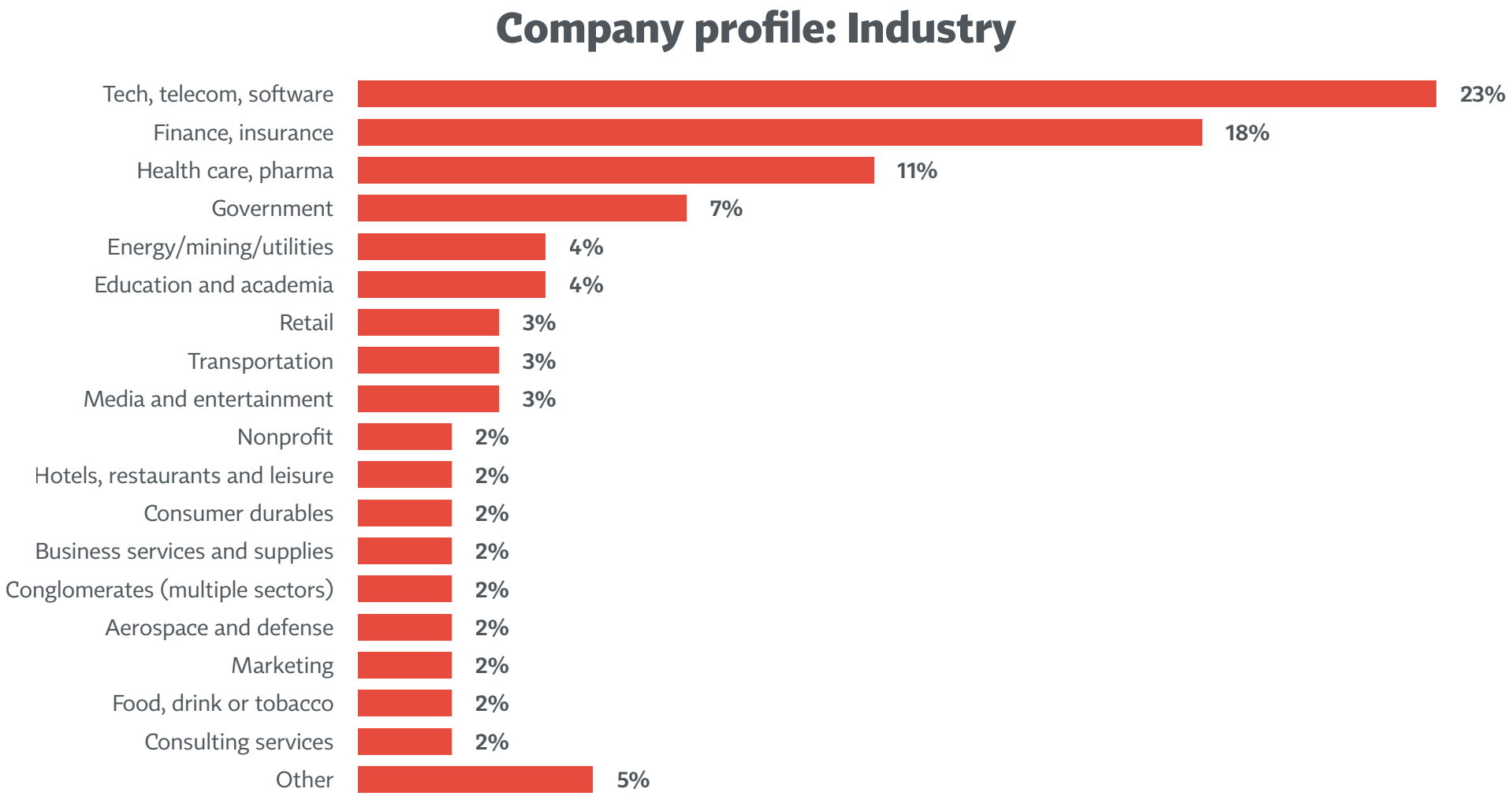
A4: What is the primary location of your company's headquarters?

About half (47%) of respondents are based in the US, 19% in the EU and 14% in the UK



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

As in prior years, privacy pros working in tech, telecommunications and software make up the largest industry group

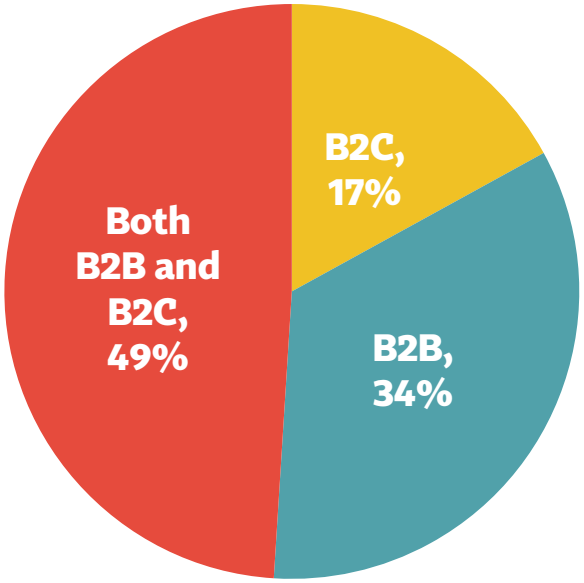


A1: Which sector listed below best describes how your company would be classified?

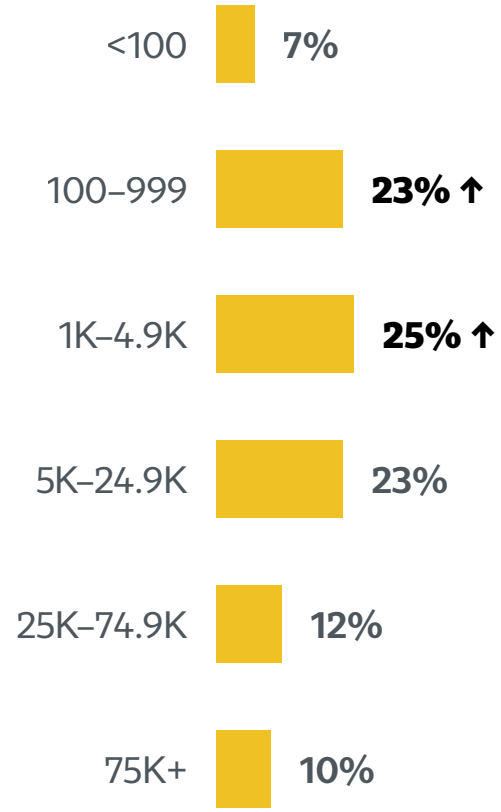
30% of respondents work at organizations with fewer than 1K staff, 25% with between 1K and 5K, and 45% with 5K staff or more

Company profiles

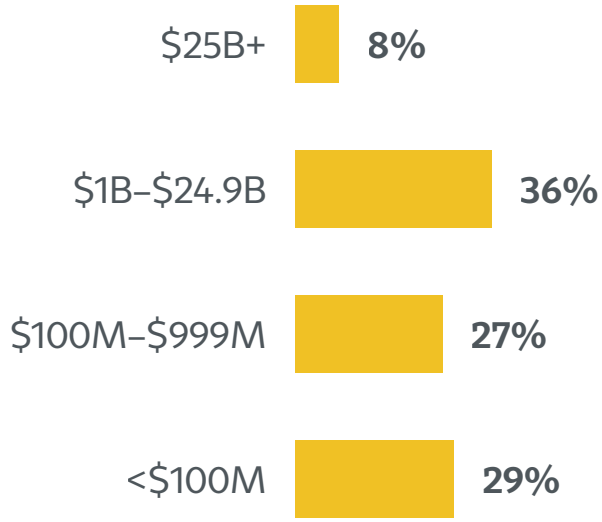
Business type



Employees



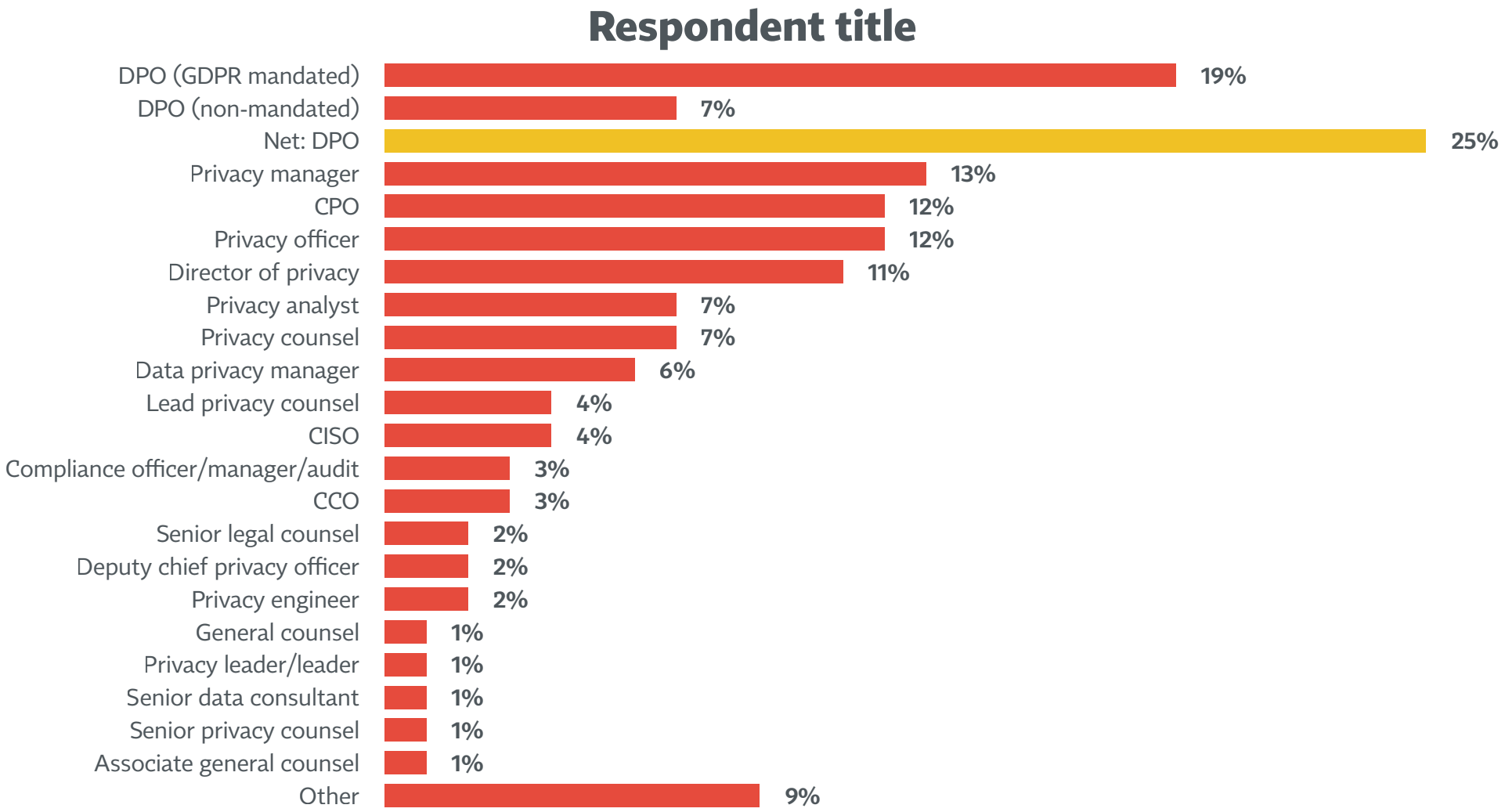
Revenue



↑ Significantly different from 2020

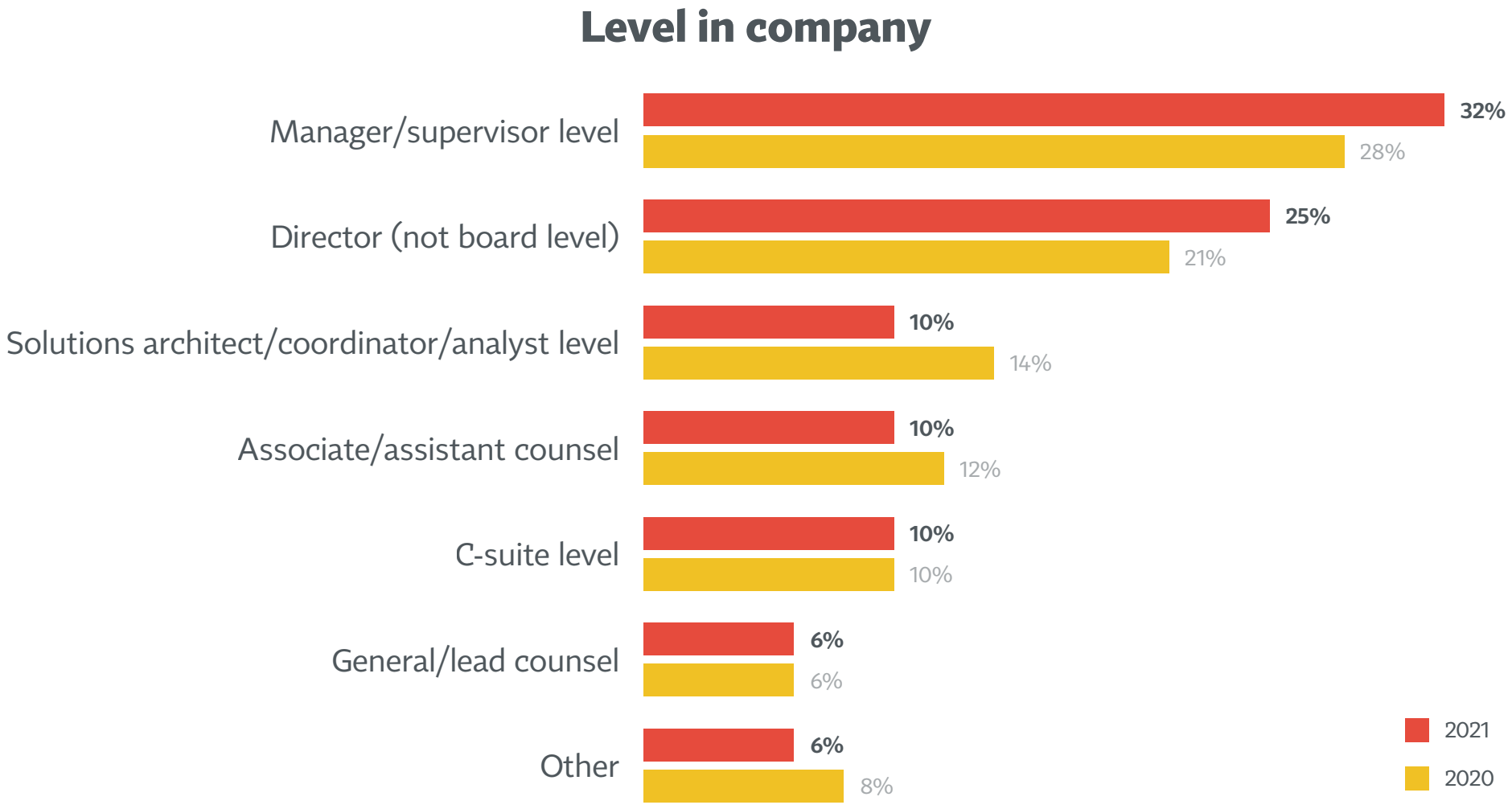
A1a: Does your company primarily serve:
A3: What is the total number of employees, full-time and part-time, in your company?
A2: Keeping in mind this survey is confidential and your individual information will not be shared, please tell us your company's annual revenue.

Half of respondents held the job title of DPO (25%), privacy manager (13%) or CPO (12%)



D2A: What is your job title?

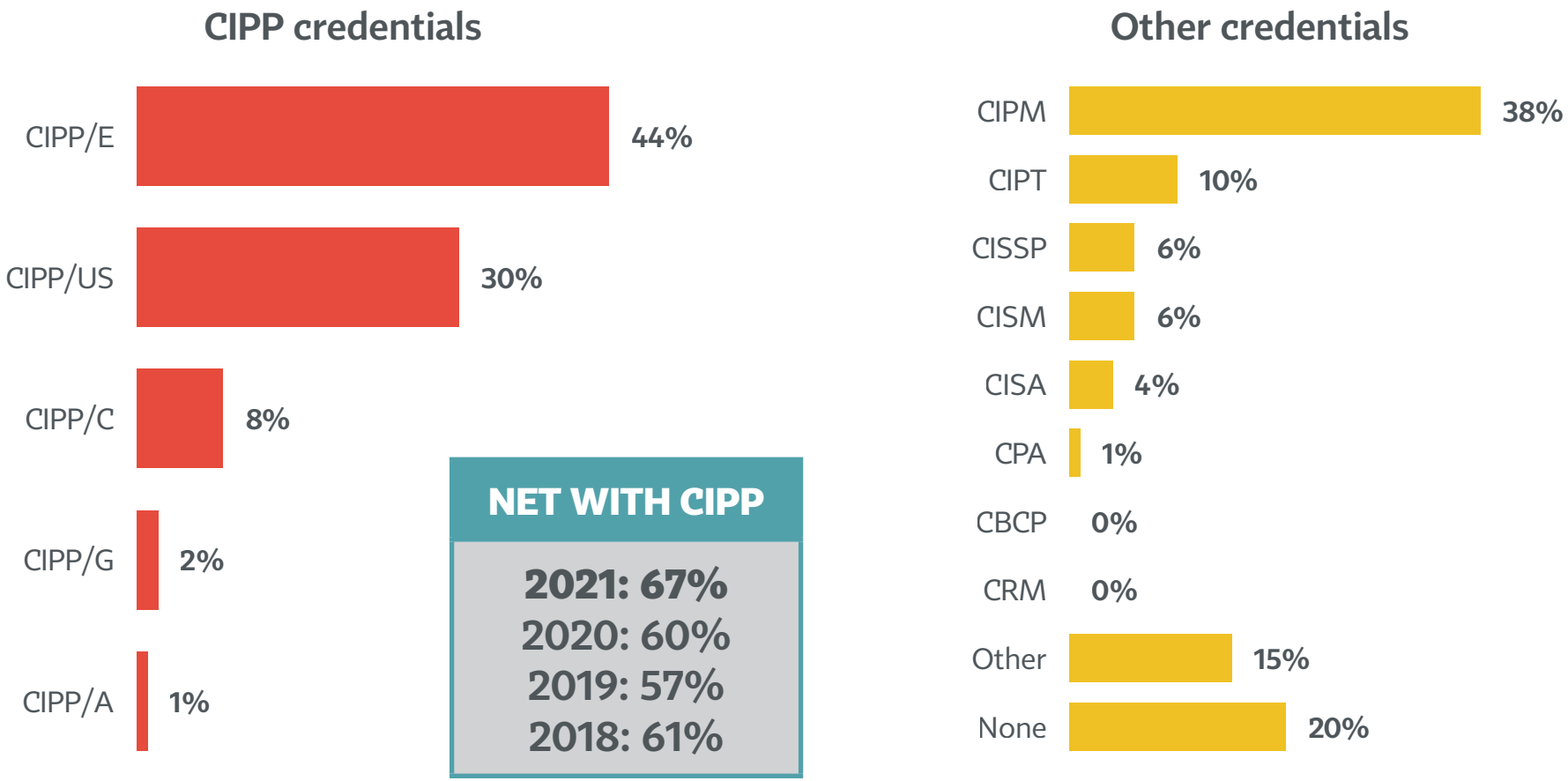
One-third of privacy pros are at the manager/supervisor level, while another one-fourth are directors



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

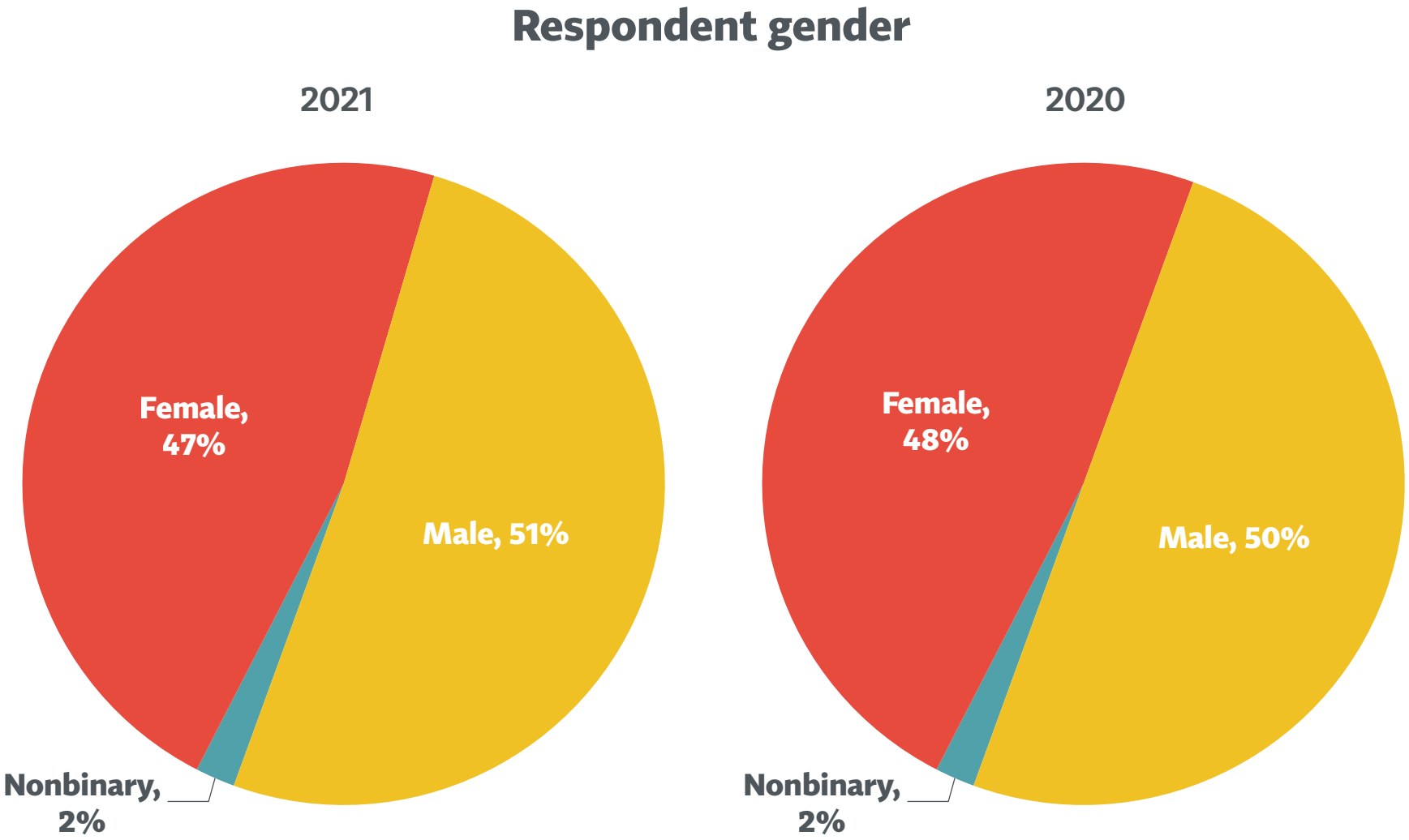
Two-thirds (67%) of survey respondents have a CIPP credential, the highest proportion since 2018

Credentials held



I10: Which certifications do you hold?

Survey participants this year are roughly split evenly between males and females, with 2% identifying as nonbinary



I12: Are you ...

Contents

Method

General target
Privacy pros from across the IAPP database.

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

Response
A total of 473 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 GDPR and CCPA and being affected by the COVID-19 pandemic.

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 tech vendors and other privacy pros were filtered out.

WEIGHTING: The 2021 results were statistically weighted to match the employee size distribution of firms answering the 2020 survey. This matching allows us to make apples-to-apples comparisons between findings from the two years.

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

SIGNIFICANT DIFFERENCES: Some findings in the report are flagged as "statistically different" from either 2020 or from other segments. A significant difference is one that is large enough (considering the base number of respondents) that we can feel at least 95% confident it is the result of an actual difference in the marketplace (versus mere sample fluctuation).

Contact

Angela Saverice-Rohan
EY Americas' Privacy Leader
Angela.SavericeRohan@ey.com

Fabrice Naftalski
Partner - Data Protection & Privacy - EY Law
Fabrice.Naftalski@ey-avocats.com

iapp

EY
Building a better working world