# IAPP-FTI Consulting Privacy Governance Report 2020

iapp

FTI CONSULTING™

# Contents



# Executive Summary

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

This year's "Privacy Governance Report" is the product of a partnership between the IAPP and FTI Consulting, our new sponsor for this year's annual study that benchmarks the privacy profession. Now in its sixth year, this report takes a deep dive into the leadership structures, core functions, staff and budgets, and tasks and priorities of privacy programs around the globe. It provides key metrics on ongoing compliance with core pieces of privacy legislation, including the EU General Data Protection Regulation and California Consumer Privacy Act, and the effects of recent legal rulings and guidance from data protection authorities on processing operations. It also explores how privacy professionals delineate tasks, hold processors and vendors accountable, measure performance, and communicate privacy issues and data protection risks to both internal and external stakeholders.

What makes this year's report different from those of previous years, however, is undoubtedly the effects felt from the COVID-19 pandemic. The global spread of the virus, lockdowns, public safety measures, like handwashing, social distancing, face masks, testing, contact tracing, working from home en masse and the race to develop a safe and effective vaccine are a few of the defining issues of the year. Just 12 months ago, however, few of these challenges could have been anticipated. Without question, COVID-19 has brought about a sea change in the way we live, work, socialize, travel and care for ourselves. Moreover, privacy professionals, in particular, have been preoccupied throughout the year with untangling the nexus between the COVID-19 pandemic and the data protection and privacy risks that have arisen in its wake.

Thus, this year's "Privacy Governance Report" includes data on the impact of COVID-19 on privacy programs and the privacy profession, in general. It provides answers to critical questions, such as: How has COVID-19 affected perceptions about the importance of privacy within organizations? How are organizations handling the sensitive health data being collected from employees and others to respond to the pandemic? And how have the responsibilities of privacy professional changed in the COVID-19 era, especially given the ubiquity of remote work?

And yet, despite the pandemic, legislative activity in the world of privacy and data protection has not slowed down. If anything, it has accelerated this year. Indeed, 2020 has delivered several groundbreaking privacy developments. Foremost among these is the July decision by the Court of Justice of the European Union in the so-called "Schrems II" case, which invalidated the EU-U.S. Privacy Shield data transfer framework and left in limbo the legal status of standard contractual clauses to authorize data transfers outside of the EU. Also, in an abrupt September move, Brazil's General Data Protection Law came into effect, providing Brazilians with a comprehensive framework regulating the use of personal data. Moreover, in November, U.S. voters in the state of California approved the ballot initiative for the California Privacy Rights Act, which will amend and augment the currently-enforced CCPA, and is set to enter into force January 1, 2023, with a look-back to January 2022.

Indeed, all around the globe, the pace of legislative developments in privacy has continued to accelerate unabated. China unveiled its draft Personal Data Protection Law, largely modeled on the EU GDPR, for public consultation in October, and it is on track for adoption in early 2021. Similarly, due to the influence of the GPDR, Canadian firms are also likely to be subject to more rigorous privacy regulation in the years ahead, as lawmakers there have released a draft reform bill known as the Consumer Privacy Protection Act to replace the Personal Information Protection and Electronic Documents Act, which is nearing 20 years old. Meanwhile, India continues to debate passage of its Personal Data Protection Bill, which is also projected to become law sometime in 2021. Late this year, Singapore also made significant changes at the end of the year to its Personal Data Protection Act. Last but not least, more federal and state privacy legislation in the U.S. is pending, as well.

This year has also had an impact not only on organizations' bottom lines, but on the very way in which many of them do business, as well. Yet, with privacy being an increasingly central part of many business operations, total privacy spending is up year-over-year by about 8%. Other positive trends are also visible. Across the board, there is also more general satisfaction and optimism about budgets. More are saying their privacy budgets are sufficient to meet their obligations, and the percentage of privacy pros expecting to see a budget increase in the next 12 months outnumber those who expect no change. This year's survey shows another interesting development: U.S.-based firms outspending EU-based ones on privacy.

But this money is certainly not going to waste. GDPR compliance is up: 47% of respondents said they are "fully" or "very" compliant with GDPR versus 39% who said so last year. And given the broad impact of the newest entrant into force, the CCPA, organizations also need to devote significant resources to complying with the law. Indeed, firms in general appear to be taking a "play-it-safe" approach to CCPA compliance. While 17% of organizations that do business in California consider themselves to "sell" data under the definition of the CCPA, nearly twice as many, 32%, have a "Do Not Sell My Personal Information" link on their website. To say the CCPA has been a transformative law would be an understatement, as 38% of organizations also reported they have modified their business practices to avoid "selling" data under the CCPA. Most organizations had already been preparing for the passage of the CPRA in their CCPA compliance programs, so it appears privacy professionals will continue to have their work cut out for them in the years ahead.

While one can be hopeful that 2020 has truly been an outlier year given the occurrence of the COVID-19 pandemic, we should harbor no false hope that recent developments in privacy and data protection law are anomalies. Indeed, the years ahead are even more likely to increase focus by consumers and scrutiny by lawmakers and regulators on privacy and data protection issues and demand greater attention and resources from organizations to stay apace with these developments.

# Contents



# Research Objectives

The overarching goals of this research are to:

- Track changes in privacy staff sizes and privacy spending over time.
- Profile privacy program structures within organizations of various sizes and sectors.
- Explore firms' responses to privacy-related developments, such as the EU General Data Protection Regulation and California Consumer Privacy Act, as well as the impact of COVID-19 on privacy.

# Method

**General target**
Privacy professionals 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 technology vendors and other privacy professionals were filtered out.

**WEIGHTING:** The 2020 results were statistically weighted to match the employee size distribution of firms answering the 2019 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 2019 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's the result of an actual difference in the marketplace (versus mere sample fluctuation).

# Contents



# How the Work of Privacy Is Done

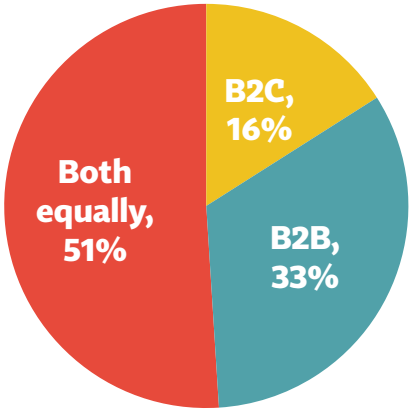
## Profile of a privacy professional: 2020

IAPP's membership grew to more than 65,000 in 2020. Responses to this survey reflect the diversity of this expanding global community of privacy professionals. Regarding the firmographics and demographics of the privacy profession, this survey brings to light the following trends:

- As in previous years, the tech/telecom/software industry is the most dominant within the privacy community, with 22% of respondents working within this broad swathe of the economy. Privacy professionals in the finance or insurance business were the next largest group, making up 17% of the sample. Other industries with large representations include health care/pharmaceuticals (10%) and consulting (4%). Privacy professionals within the public sector were also well represented in the survey, with 10% of respondents working for a government agency.
- Privacy professionals are spread throughout small, medium and large organizations. While privacy pros tend to work for larger firms — with 58% working at organizations with 5,000 or more employees — one in four privacy pros works for an organization that has fewer than 1,000 employees. In terms of the annual revenue of the firms where privacy pros work, there is also a great deal of variation. About 3 in 10 privacy pros are at an organization that has under $100 million in annual revenue, while another 3 in 10 are at one that generates between $1 billion and $25 billion. At the same time, about 20% work for companies with more than $25 billion in annual revenue, and another 20% at companies that pull in somewhere between $100 million and $999 million. About half (51%) of the organizations that house privacy professionals are hybrid enterprises, a combination of business-to-business and business-to-consumer models. One-third are strictly B2B, while the rest (16%) are B2C companies.

### Company profiles

#### Business type




#### Industry sector

| | |
|---|---|
| Tech, telecom, software | 22% |
| Finance, insurance | 17% |
| Health care, pharma | 10% |
| Government | 8% |
| Consulting services | 4% |
| Education and academia | 4% |
| Retail | 4% |
| Energy/mining/utilities | 4% |
| Transportation | 3% |
| Food, drink or tobacco | 2% |
| Legal services | 2% |
| Marketing | 2% |
| Media | 2% |
| Nonprofit | 2% |
| Business services and supplies | 2% |
| Conglomerates | 2% |
| Other | 10% |

#### Employees

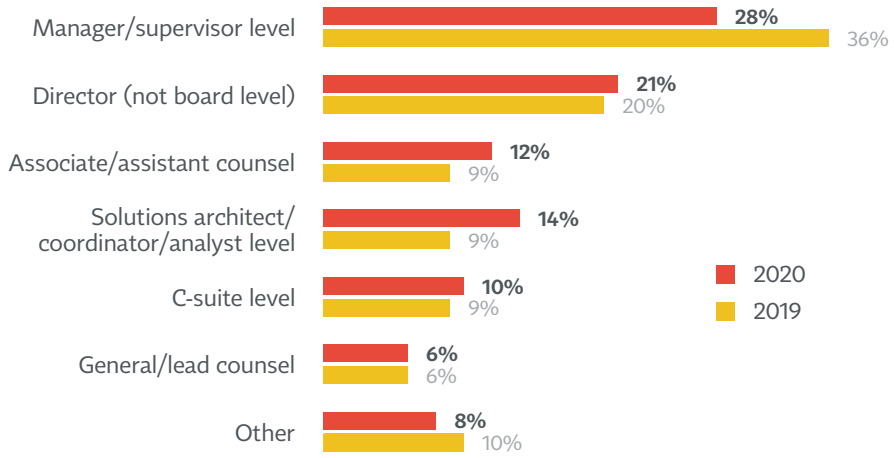
| | |
|---|---|
| Under 100 | 10% |
| 100–999 | 15% |
| 1K–4.9K | 16% |
| 5K–24.9K | 22% |
| 25K–74.9K | 17% |
| 75K+ | 19% |

## PRIVACY PROS AT A GLANCE

In **2020**, the most common characteristics for a "typical" privacy pro are:

- Based in the **U.S. or EU.**
- Works in **tech, finance, insurance, health care or government.**
- Works at a **B2B/B2C** firm that employs **5,000 or more** employees with annual revenue **more than $1 billion**.
- Is a **director/manager/supervisor** with a title such as **DPO or CPO.**
- Is just as likely to be **male or female**.

### Respondent level in company




- The privacy profession is truly global. More than half (56%) of respondents this year were based in the U.S., up from 36% last year. EU-based respondents made up 17% of respondents, down from 35% in 2019. In addition, 10% of respondents were U.K.-based, and 6% more were in Canada, while the remaining 11% included respondents from Australia/New Zealand, countries in Europe outside the EU or elsewhere. The shifts in the geographic makeup of the respondent base may stem from the change in timing of the survey, fielded in the summer rather than the spring this year, rather than from changes in the demographics of the profession.

- The full range of positions available to privacy professionals were also represented in this year's survey, from the C-suite to the analyst level. About half of respondents work at the manager/supervisor (28%) or director, non-board (21%) level. Associate/assistant counsel (12%) and solutions architect/coordinator/analyst (14%) were the next largest groups, followed by the C-suite occupants (10%). Regarding particular job titles, data protection officer was the most visible, with 19% having that title. Chief privacy officer was the second-most prevalent position of the privacy pros who took the survey, with 14% having that title. Privacy managers (11%), privacy officers (10%) and privacy analysts (9%) made up nearly one-third of the field. Substantial groups of respondents also held the titles of director of privacy (6%) and data privacy manager (5%).

- The gender profile of the survey reflected a near even split between male (50%) and female (48%) privacy pros, with 2% identifying as non-binary.

## The effect of COVID-19 on the work of privacy professionals

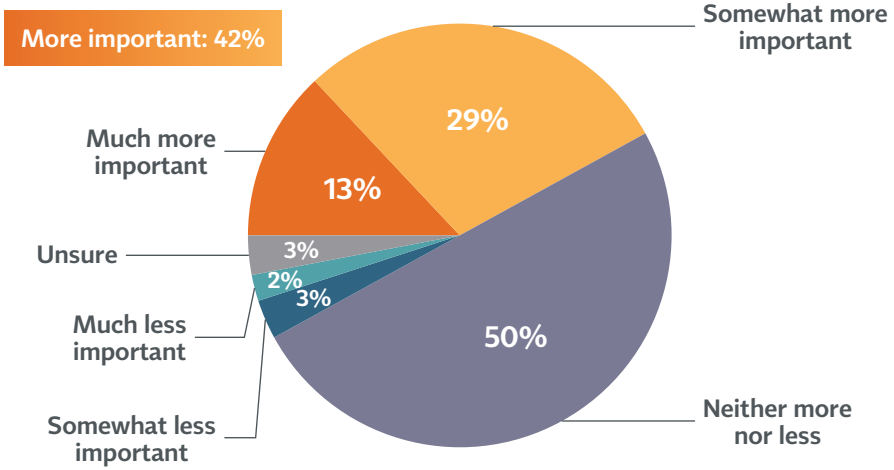
It is not an overstatement to say the COVID-19 pandemic has reshaped daily life around the world. Neither would it be an exaggeration to say it has had an enormous impact on the privacy profession. But what kind of impact has it had more precisely? How are privacy professionals and the privacy profession as a whole responding and adapting to the pandemic?

For one, regarding the importance of privacy itself, COVID-19 has brought greater attention to privacy within many organizations. **More than 40% of respondents reported privacy has become more important within their organization in the wake of COVID-19**, while only 5% said it has become less important.

Given the direct relevancy of privacy and data protection to the collection, processing and use of employee health data while implementing new workplace safety protocols, this comes as little surprise. Indeed, about half of our respondents this year tell us that their organization is collecting health status information from its employees. More than one-third of organizations have taken the temperatures of employees (37%) and recorded personal travel histories (35%). Meanwhile, about 30% are collecting the COVID-19 test results of their employees, while 29% are collecting information from employees that can be used in contact tracing. Overall, only 24% of organizations have not collected any of these types of data from their employees since the pandemic began.

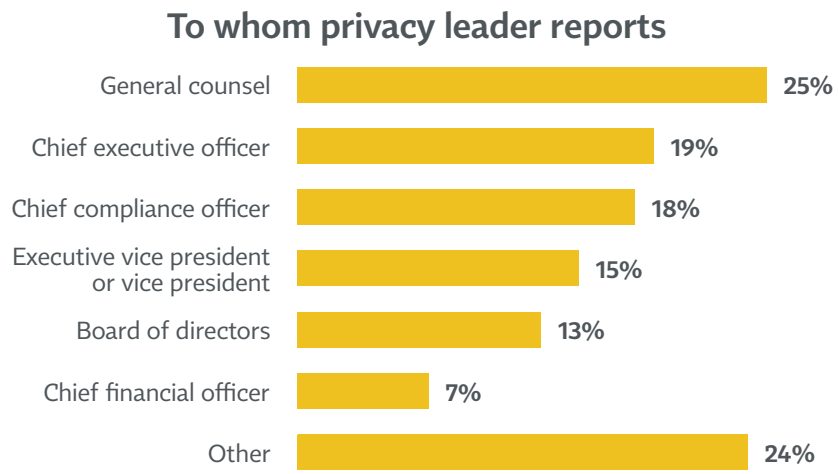
COVID-19 has also substantively changed the day-to-day tasks of many privacy professionals. More than half of privacy pros said maintaining and consulting on employee privacy has become more of a priority for them.

Impact of COVID-19 on privacy importance




Relatedly, half of privacy pros have also needed to spend more time on assessing platforms that enable remote work or employee engagement. This should also be unsurprising to many, as 7 in 10 respondents reported they were working completely remote at the time of the survey (August through September 2020). About another 2 in 10 were working partially remote, while fewer than 1 in 10 were working in an office full time. Thus, in addition, some privacy professionals have also needed to grapple with issues concerning the monitoring of remote employees. In total, 16% of organizations have either begun or increased the extent to which they monitor their employees during the pandemic.

Much work will need to be done to ensure all this new data is maintained and eventually deleted in accordance with privacy and data protection principles and best practices. It seems many privacy professionals are well on their way to managing the risks such data may present, with about 45% of respondents saying they have conducted a privacy




risk assessment or data protection impact assessment with regards to data collected from employees in the context of COVID-19. Yet, at the same time, 45% of organizations that have collected employee health data or have employees working from home have not (yet) conducted a DPIA.

In addition, just over one-third of privacy pros reported working harder on safeguarding company data against scams, in which the U.S. Federal Trade Commission has noted an uptick due to COVID-19. The sharing of personal data with third parties, government entities and/or researchers in efforts to mitigate the pandemic has also brought about a host of new privacy challenges, with 35% of privacy pros reporting this has become more of a priority in recent months.

Overall, the importance of privacy has only increased the wake of COVID-19. Yet, the privacy profession has faced several new and significant challenges due to the pandemic, which are likely to persist into the months and years ahead. Most of these revolve around the massive switch to remote work that most firms pursued and the increased collection of employee health data to mitigate the spread of the disease.

Privacy professionals are finding ways to cope with these challenges by placing more priority on these new tasks and assessing the risks inherent to this increase in both the types and the quantity of data being processed on a regular basis.

## Privacy leadership and reporting structures

Another area in which the IAPP-FTI Consulting "Privacy Governance Report" provides unique insights is the structure and function of privacy leadership within organizations. All respondents are asked to self-report whether they are the "privacy leader" — that is, the most senior employee responsible for privacy within an organization who has oversight of its privacy program.

Although this could theoretically be anyone from the CEO down, in about 4 out of 10 organizations it is the CPO. In another 13% of organizations, the DPO is the privacy leader. In another 9%, the privacy leader is the director of privacy.

Interestingly, firms where the DPO is the privacy leader differ from firms where another role is the privacy leader in several notable respects: Smaller firms — in terms of the number of employees and annual revenue — tend to have a DPO serving as the privacy leader. However, these firms also tend to employ significantly more people to work on privacy. In addition, these firms are more often based elsewhere than the U.S., and almost all of them have privacy teams that are responsible for GDPR compliance.

When they are not the DPO, privacy leaders tend to be an equivalent position (10% of the time) or a more senior position (25% of the time). More often than not, the privacy leader is also equivalent to the chief information security officer (41% of the time) or in a more junior position than the CISO (29% of the time).

Privacy leaders report most frequently to the general counsel (in 25% of organizations), CEO (in 19% of organizations) or the chief compliance officer (in 18% of organizations). Executive vice presidents (15%) and board of directors (13%) are also frequently reported into by an organization's privacy leader, whoever that may be. Privacy leaders at smaller firms are more likely to report directly to the CEO, likely because they would lack many of the intermediary positions, such as chief compliance officer or general counsel, that exist between the privacy leader and CEO at larger firms.

There are also some trans-Atlantic differences in how the privacy leadership is organized within organizations. Privacy leaders at U.S.-based firms are less likely to report to the CEO or board of directors and more likely to report to general counsel than are privacy leaders at EU-based firms.

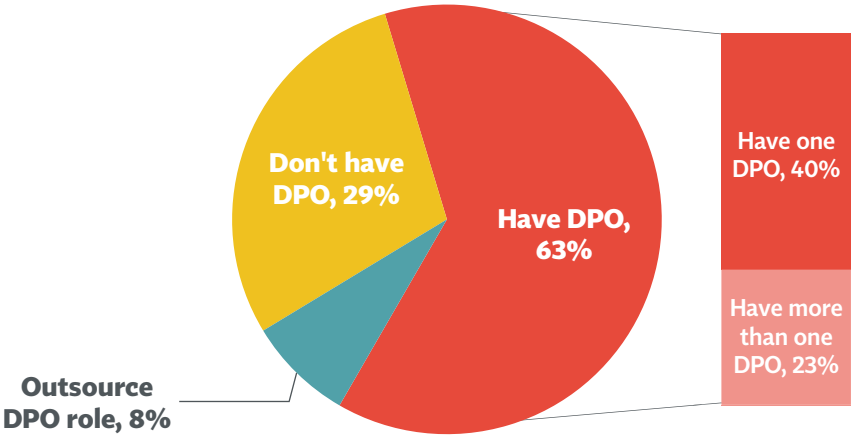
## The ranks of DPOs continue to swell

The GDPR had served as an initial catalyst for the growth of the DPO role. IAPP's analysis a year after GDPR implementation showed 500,000 organizations had already registered a DPO to fulfill the law's requirements.

This year, it is Brazil's LGPD that is poised to trigger the most growth in the role of DPO. A recent study by IAPP estimated the newly implemented law will require 50,000 DPOs in Brazil alone.

Indeed, we see the increased presence of the DPO in our survey, in which about one in five respondents holds the title. Sixty-three percent of the firms surveyed have their own in-house DPO, with another 8% outsourcing the role. Of those with an in-house DPO, most have just one, although about one-third of them have two or more. DPOs are also much more likely to be found working in the private sector than in the public sector, with 68% of government agencies surveyed found to be lacking the DPO role. Additionally, B2B firms, as well as hybrid B2B/B2C firms, were much more likely to have a DPO than B2C firms.

**Whether firm has DPO**




DPOs tend to report into the organization's privacy leader (39%), general counsel (19%) or chief compliance officer (13%). The rest report directly into those higher up the corporate ladder, with 12% reporting to the board of directors, 8% reporting to an executive vice president and another 8% reporting directly to the CEO.

Given the influence of the GDPR, it is unsurprising perhaps that a significantly higher number of DPOs are based in the EU compared to the U.S. While 20% of respondents based in the U.S. held the title of DPO, 45% of EU-based respondents were DPOs.

While most DPOs are currently mandated by the GDPR, we can expect to see increases in the number of DPOs mandated by non-GDPR laws, such as Brazil's LGPD, in the near future.

## Take the good with the bad: Privacy staff and budget

This year's survey data points to both positive and negative trends in the status, as well as expectations about the future of staffing and budgets within the privacy profession.

While privacy staff numbers have been on the rise in recent years, COVID-19 may be weakening this trend. Indeed, about 45% of organizations have put in place or plan to put in place hiring freezes across the board for both privacy and non-privacy roles (another 1% has instituted or expect to institute a hiring freeze of privacy roles only, whereas 8% expect a freeze only for non-privacy roles). Moreover, about 71% expected the current number of full-time privacy staff to remain the same in the coming year, and about 86% expected the number of part-time privacy staff to remain the same over the next 12 months.

Notwithstanding these facts, net expectations about future hiring remain in positive territory. All told, expectations among privacy pros point to an 11% increase in full-time privacy staff and a 4% increase in part-time privacy staff in the coming year.

The average number of full-time privacy staff at organizations this year was 15, while the average number of part-time privacy staff was 18. Not surprisingly, firms that employ more people overall and have higher annual revenues also tended to employ more full-time and part-time privacy staff. Moreover, on average, EU-based organizations employ 13 full-time privacy staff, a few more than the average full-time privacy staff at U.S.-based organizations, which is 9. However, U.S.-based firms have on average more people working part-time on privacy (21) compared to their EU counterparts (15).

**Privacy staff: Mean**

| | Overall |
|---|---|
| Full-time privacy staff | 15 |
| Part-time privacy staff | 18 |

**Mean privacy staff size by HQ location**

| | U.S. | EU |
|---|---|---|
| Full-time privacy staff | 9 | 13 |
| Part-time privacy staff | 21 | 15 |

Data on privacy budgets paint a much brighter picture. Mean privacy spend is at $676,000 this year, up from $622,000 last year, an increase of about 8%. As was true of privacy staff sizes, larger organizations by total employees and company revenue tend to have significantly higher privacy budgets, as well. Indeed, for companies with annual revenues of $25 billion or more, their mean privacy budget is about $2 million.

Another factor influencing the size of the privacy budget is whether the firm operates in a highly regulated industry, such as banking, finance, health care and insurance. Organizations that operate within other, less-regulated industries tend to spend significantly less on privacy overall. Whereas the mean privacy spend for an organization in more regulated industries is about $1.8 million, the mean privacy spend for organizations in less regulated industries is about $450,000.

One more bright spot in the budget picture is that an increasing number of privacy professionals are getting the sense that their budget is sufficient to meet their privacy-

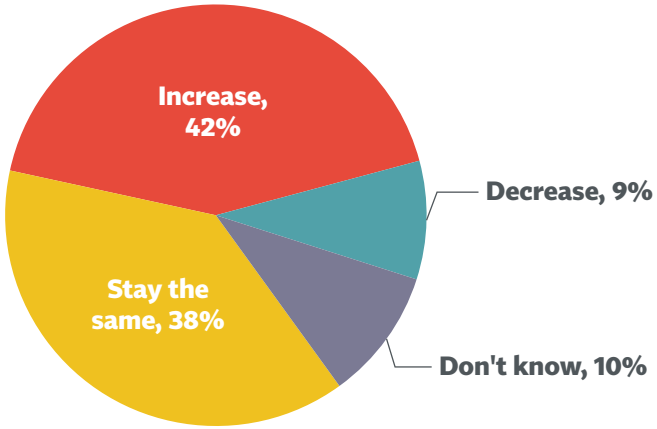
related obligations. Indeed, over the past few years, the percentage of respondents saying their budget is less than sufficient has dropped more than 10 percentage points, from 65% in 2018 to 54% in 2020. It is also worth noting the majority do not think their budget is insufficient by very much: 41% said their budget is "somewhat" less than sufficient to meet their obligations, while only 13% said their budget is "much" less than sufficient.

Regarding future budget projections, privacy professionals can be roughly divided into those who are optimistic and those who are ambivalent. A total of 42% of respondents expected their privacy budgets to increase (on average, they expect it to rise by about 27%). Another 38% of respondents believed their budget will more or less remain the same over the next 12 months. Only 9% expected to see a decrease in their privacy budget in the year ahead. For those expecting to see their budget swell, the majority (72%) thought it will impact salaries and benefits the most. Half believed the budget increase will lead to the creation of new privacy program initiatives, while 47% expected to see tool acquisition, and 43% anticipated the additional budget will go to more privacy training. For those forecasting a budget reduction, almost 60% believed the cuts will be made to tool acquisition and travel and conferences. Fewer than half (40%) of those foreseeing budget reductions expected it to affect salaries and benefits.

Regarding who at the organization makes the privacy budget decisions, respondents told us it is most often the general counsel (at 38% of firms) or CPO (at 36% of firms). Data protection officers (18%), CISOs (12%) and CCOs (11%) are also regularly in charge of privacy budgeting.

Overall, the picture in 2020 regarding privacy staff tells us that, while COVID-19 has introduced some hesitation into new hiring plans, both full-time and part-time roles in privacy remain in a strong position. Similarly, privacy budgets are up year over year, and more and more privacy pros, 46% in total this year, see their budgets as sufficient to meet their obligations. The vast majority (80%) of privacy pros also expected their budgets to remain the same or increase, and those that do expect a decrease are more likely than not to think salaries and benefits will not need to be downsized. All in all then, privacy budgets appear to be on stable footing.

**In next 12 months, privacy budget will …**




**% privacy budget increase/decrease**

| | Budget will increase | Budget will decrease* |
|---|---|---|
| Median % expected change | 15% | 25% |

* Small sample size

## Privacy teams: An ever-expanding suite of responsibilities

We also asked respondents to tell us about the duties for which they are responsible, as well as those that fall within the purview of the privacy team. Virtually all (98%) of respondents said privacy policies, procedures and governance fall within their or the privacy team's orbit. Tied for second place on the list of privacy responsibilities, which 96% of respondents affirmed they or the privacy team are responsible for carrying out, were addressing privacy issues with existing products and services and following legislative developments regarding privacy and data protection.

More than 9 in 10 privacy pros also said privacy-related awareness and training within the company, guiding the design and implementation of privacy controls, privacy-related communications, performing PIAs or DPIAs, and conducting privacy-related investigations were tasks for themselves or the privacy team.

A few slight differences appeared between privacy pros in the U.S. and those in the EU regarding their core responsibilities. For example, privacy professionals in the EU were more likely than their U.S. counterparts to say privacy-related monitoring, GDPR compliance and assuring proper cross-border data transfers were part of their or the privacy team's job description. Meanwhile, U.S. privacy pros were more likely than those in the EU to say ethical decision-making around data use and CCPA compliance were important parts of their work portfolios.

Regarding how the typical privacy professional divides their time, on average, they reported spending about 73% of their time on privacy-related work. Moreover, an increasingly large share said they devote 100% of their time to privacy tasks. In 2020, 41% of privacy pros said they spend all their working hours on privacy, whereas only 37% did so in 2018.

**BY RESPONDENT LOCATION**

| | U.S. | EU |
|---|---|---|
| **Privacy responsibilities** | | |
| Privacy-related monitoring | 80% | **91%** |
| Compliance with EU GDPR | 76% | **99%** |
| Assuring proper cross-border data transfer | 74% | **89%** |
| Ethical decision-making around data use | **84%** | 70% |
| Compliance with CCPA | **84%** | 41% |

Significantly different than other segments

Job satisfaction and perceptions about career advancement also remain high among privacy professionals. Overall, 8 in 10 privacy pros said they are either satisfied or very satisfied with their job. Another 13% said they are neutral, being neither satisfied nor unsatisfied, while just 7% reported being unsatisfied with their jobs. Likewise, about half (49%) expecting an upward career path, with 34% not seeing one, and 17% unsure of the direction their careers are headed.

We are also witnessing the maturing of privacy programs, with IAPP certifications playing an increasingly important role for the industry. The CIPP/E was the most popular credential amongst respondents, 36% of whom held it, followed by CIPM (held by 32%) and CIPP/US (held by 30%).

## The priorities of privacy pros: GDPR, CCPA and beyond

Issues of legal compliance remain at the heart of privacy professionals' duties and responsibilities. Yet, there is no single right way to approach compliance. Rather, compliance strategies showcase the breadth of efficiency, adaptation and creativity of privacy teams around the globe.

Indeed, as our data this year indicates, privacy professionals are taking a variety of approaches in their pursuit of compliance with laws, such as the GDPR, CCPA and LGPD. About 4 in 10 organizations are working toward a single privacy strategy that can be applied around the globe. Another 3 in 10, however, take an approach that segments data subjects by jurisdiction, handling each data subject's personal data according to the relevant local law. About 2 in 10 can pursue a more singular strategy of complying with the laws of a single jurisdiction, given that their data subjects are primarily in that one location.

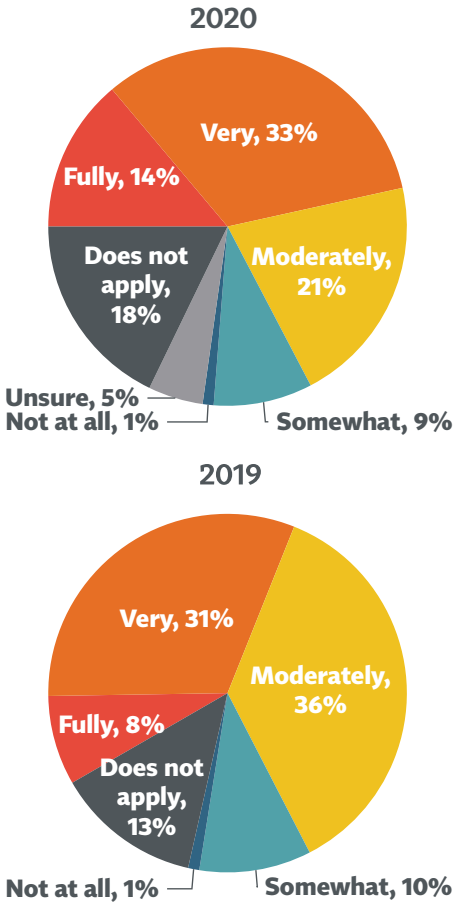
As was true in 2019, compliance issues — concerning the GDPR, CCPA and beyond — continue to remain the top priorities for privacy professionals. Overall, 30% of privacy pros said compliance with the GDPR remained their top priority.

## GDPR compliance and the impact of 'Schrems II'

Some notable differences exist between how U.S.-based and EU-based privacy pros prioritize various privacy functions. EU-based privacy pros place even more emphasis on GDPR compliance, with more than 60% saying it is their number one job, compared to just 16% in the U.S. who ranked it first. For a quarter of U.S. privacy pros, however, compliance issues beyond the GDPR and CCPA, such as state-specific and sectoral laws, are their number-one concern. U.S. privacy pros also place much more emphasis than their EU counterparts on meeting the expectations of business clients and partners, with 19% in the U.S. saying it's a high priority, versus just 3% in the EU. While 12% of U.S. privacy pros also considered CCPA compliance a top issue, it has not become a top concern for any EU privacy pros yet.

Across the board, we can see GDPR compliance is up year over year. Nearly half (47%) of privacy pros said their organizations were fully compliant or very compliant with the GDPR this year, compared to 39% in 2019. EU firms also appear to have made more progress with GDPR compliance than their U.S. counterparts, as 57% of EU firms are fully/very compliant, versus 45% of U.S. firms.

GDPR compliance status




On the GDPR front, the so-called "Schrems II" decision handed down by the CJEU in mid-2020 has had significant consequences for how data is transferred outside of the EU. The decision has had direct or indirect effects on a broad array of companies, with 65% of respondents reporting their organizations transfer data outside of the EU. The EU-U.S. Privacy Shield, which was invalidated as an EU-approved transfer mechanism by the court's decision, was reported to be used by more than half

(55%) of these organizations. Moreover, of those firms that transfer data outside the EU, 88% said they use SCCs as the mechanism for doing so, a number which will surely increase as firms reliant on Privacy Shield are forced to use other mechanisms to enable these transfers. Indeed, of those firms that had planned to switch data transfer mechanisms in light of the decision, 75% indicated they would switch to SCCs. Meanwhile, between 45% and 53% indicated they would add contract-based, technical-based or policy-based additional safeguards.

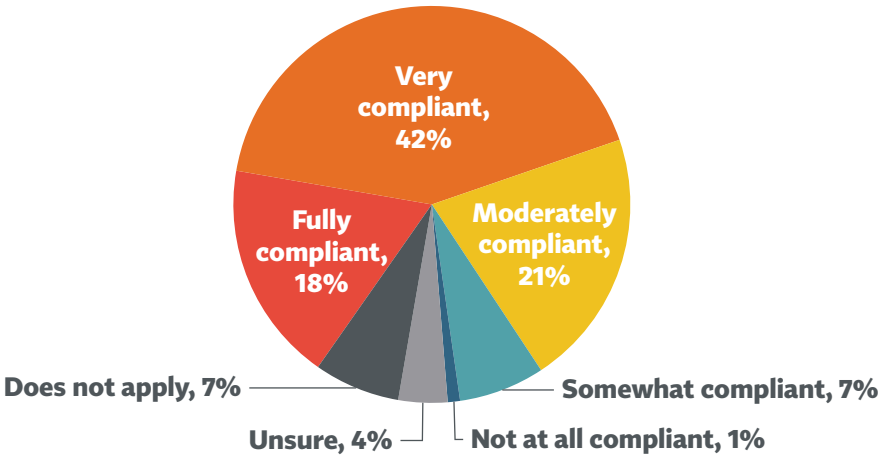
## CCPA compliance in the first year of enforcement

The approval and passage of the CCPA was a watershed moment in the world of privacy. A groundbreaking piece of state privacy legislation, it applies to organizations that handle personal information about California residents and meet a series of other criteria.

Organizations may be subject to the CCPA as a "business," "service provider" or "third party" (or some combination of the three). Indeed, of those organizations doing business in California, 82% considered themselves to be a "business" within the definition of the law, 48% saw themselves as a "service provider," and 22% classified themselves as a "third party." Yet, while only 18% of organizations doing business in California said they sell data under the CCPA, 32% of them have websites containing a "Do Not Sell My Personal Information" link. Thus, it would seem organizations are exercising excess caution in complying with this provision of the CCPA, at the very least.

Furthermore, organizations have also sought to comply with the CCPA by modifying their business practices to avoid "selling" data under the definition of the law. Indeed, 38% of organizations doing business in California reported having done this.

### Level of compliance with CCPA




What has been the most difficult requirement of the CCPA for organizations to comply with? Overall, the largest group of respondents (32%) said the law's data-mapping requirements were the hardest to meet. Enabling the right to delete came in second in terms of difficulty level, with 23% of respondents giving this a very difficult rating. Another 22% said updating vendor contracts has given them the most difficulties.

Of organizations that do business in California, 60% said they are fully or very compliant with the CCPA. Another 28% considered themselves to be moderately or somewhat compliant, and only 1% said they are not at all compliant. These levels are somewhat higher than GDPR compliance levels, which may be due to a couple of factors. First, the GDPR is a more expansive, stricter law, making CCPA compliance relatively easier by comparison. Another important factor is that many organizations that have already worked toward GDPR compliance in previous years have been able to successfully leverage these efforts toward compliance with the CCPA.

At the time the survey was conducted, a majority (63%) of organizations doing business in California and largely subject to the CCPA indicated they were considering the CPRA ballot initiative in their CCPA compliance program. For those who began doing so, this has proved to be a fortuitous strategy, given the resulting passage of the ballot proposal and expected entry into force of the CPRA in 2023, with a look-back provision to 2022.

## Benchmarking privacy metrics

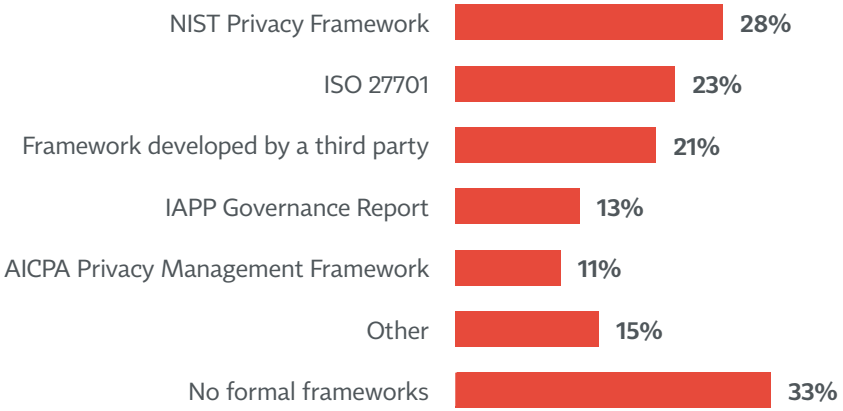
Benchmarking privacy programs has also become increasingly important for privacy pros to demonstrate the value, impact and return on investment that their programs generate. Numerous benchmarks have emerged to provide an overarching structure for year-to-year changes and developments. The most commonly used benchmark is the NIST Privacy Framework, which 28% of privacy pros reported using to measure or benchmark their programs. The ISO 27701 standard is the next most popular framework, with 23% reporting they rely on it. Other frameworks developed by third parties are also used by 21% of privacy pros, and the IAPP "Governance Report" itself is used by 13% to measure/ benchmark privacy program effectiveness (if you're reading this, that probably means you!). One in 10 privacy pros also use the AICPA Privacy Management Framework.

Concerning specific benchmarks that they measure, more than half of privacy pros consider the following:

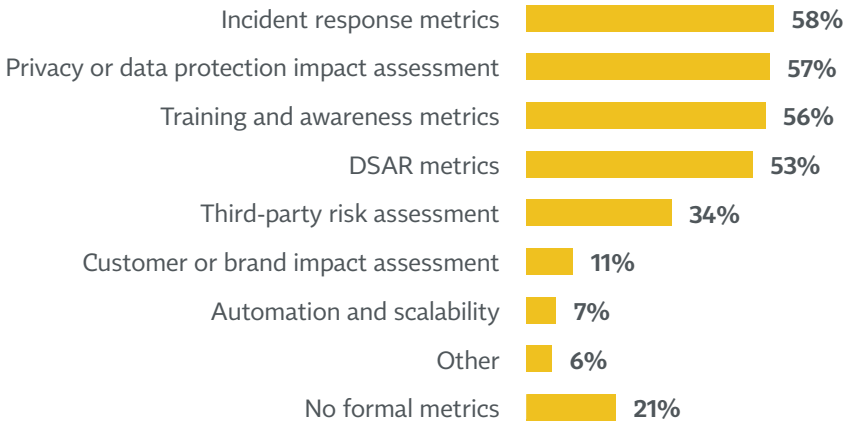
- Incident response metrics (58% use them).
- PIAs or DPIAs (57% use them).
- Training and awareness metrics (56% use them).
- Data subject access request metrics (53% use them).

Third-party risk assessments are also quite popular, being used by about one-third of privacy pros. Some of the lesser-used benchmarks are customer or brand impact assessments (11%) and automation and scalability (7%). Moreover, 21% of privacy pros have no formal metrics in use to measure their program's performance, meaning there is still significant room for formalization in this area.

### Benchmark frameworks used




### Benchmark metrics used



## Accountability and risks

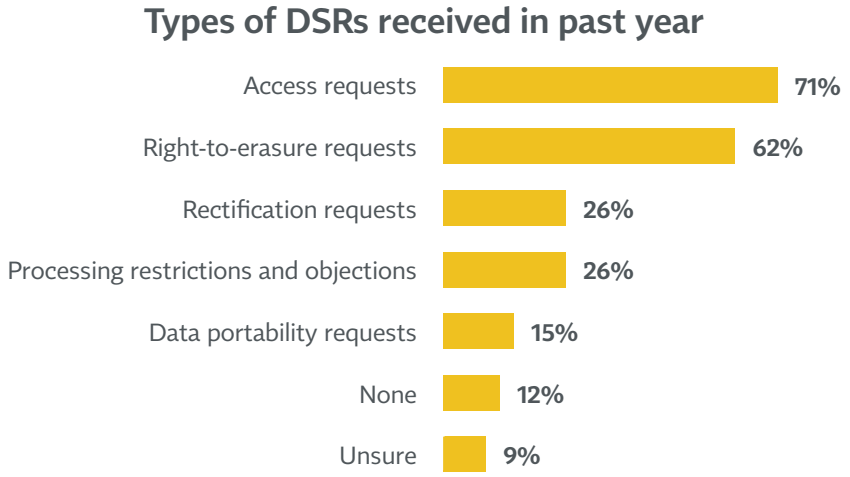
As an accountability mechanism, reporting privacy topics to the board on an annual, quarterly or more frequent basis can be a critical part of linking privacy programs and outcomes to an organization's overall performance. Privacy pros indicated the topics they report most frequently to their boards are data breaches, with more than two-thirds doing so. Other top issues that get reported to the board include privacy program key performance indicators (57%), GDPR compliance status (56%) and progress on various privacy initiatives (55%).

Relatedly, privacy professionals have been increasingly diligent about their communication of privacy issues to stakeholders beyond their boards and other internal teams. Given that nearly half (44%) of privacy pros work for a publicly traded company, disclosing privacy-related risks within financial notices, disclosures, shareholder communications or annual reports has become an important task for many of them. About half of privacy pros who work for a publicly traded company disclosed such risks in financial statements, and these usually contain information about both risks related to compliance and risks related to data breaches.

## Data subject requests

The most common types of DSRs organizations reported receiving were access requests (71%) and right-to-erasure requests (62%). In a distant third and fourth place were rectification requests (26%) and processing restrictions and objections (26%).

In terms of how long they typically take to process DSRs, about 12% make up the fastest responders, being able to address DSRs usually within a few hours. Another 17% were also relatively speedy, responding usually within a day or two. The majority, however, fell into one of two groups: those who responded anywhere from a few days to a week (20%) or about a week or two (31%). The slowest responders, who take anywhere from a month to longer to respond to most DSRs, made up about 13% of the sample. Also, about 62% of organizations reported having a dedicated team to handle DSRs.




The most difficult types of DSRs to respond to are those that involve locating unstructured personal data. Monitoring the practices of third parties that an organization does business with is another top difficulty involved in handling DSRs, as is the verification of the data subject's identity. Ensuring data minimization and developing an opt-out tool that is easy to use and centralized are other key challenges in the DSR process.

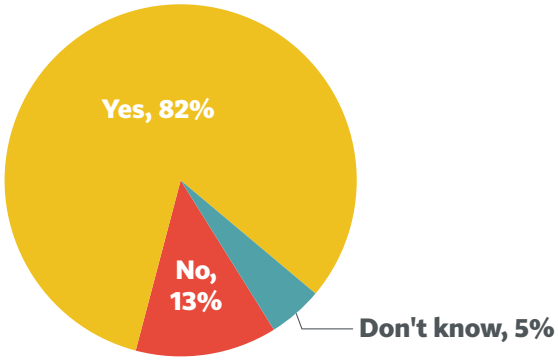
The most common tools privacy pros use to conduct data inventory and mapping are manual/informal ones, such as email, spreadsheets and in-person communication, which 32% of respondents reported using. A similar amount (28%) said they use a commercial software tool designed

specifically for data inventory/mapping, while another 22% said they employ governance, risk management and compliance software that is customized to the task of inventory/mapping. Indeed, only 2% of privacy pros reported their DSR process is fully automated. The rest rely on a mixture of partial automation (42%), entirely manual but mature processes (30%) or a process that is entirely manual and ad hoc (23%).

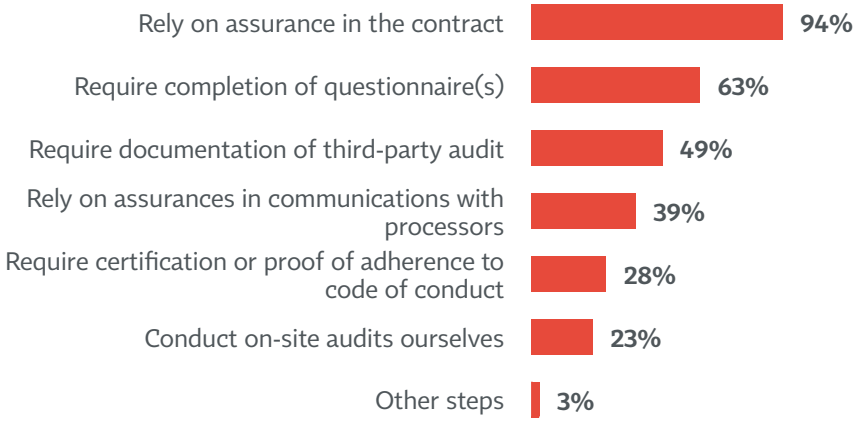
Regarding automation more generally, more than three-quarters of privacy pros reported having either purchased or built in-house some form of privacy technology to automate a part of their privacy program. Indeed, most privacy pros used privacy technologies to conduct DPIAs (55%) or do data mapping/inventory (54%).

Third-party service providers are used by about half (49%) of privacy pros to manage their cookie consent/website-scanning activities. Third-party service providers are also popular choices for data inventory/mapping (32%), consent management (28%) and risk management (26%).

### Use of other companies to process data




### Steps taken to ensure processor responsibilities




## Certifications, audits and vendor management

As data-processing chains become more complex, vendor management is an increasingly important task for privacy professionals. Overall, 83% of organizations used some kind of "processor" or outside firm to process data on their behalf. To ensure these processors fulfill their responsibilities, about 94% of organization relied on assurances in the contract. In addition, a majority (63%) required completion of a questionnaire, whereas about half (49%) required documentation from a third-party audit.

Regarding audits organizations require of their data processors, the most common one, used by 35%, is an assessment that they have developed internally and that their vendors must "pass." A sizeable number of organizations also required PCI (27%) and ISO 27001 (25%).

Internally, a popular certification required by 13% of respondents is the CIPP/CIPM/CIPT credentials. The NIST Privacy Framework is also required within 10% of organizations, with ISO 27002 and SOC 2 HIPAA both being required internally by 9% of organizations. Overall, U.S. firms are more likely than EU firms to require specific certifications internally or of their data processors.

## METHODOLOGY

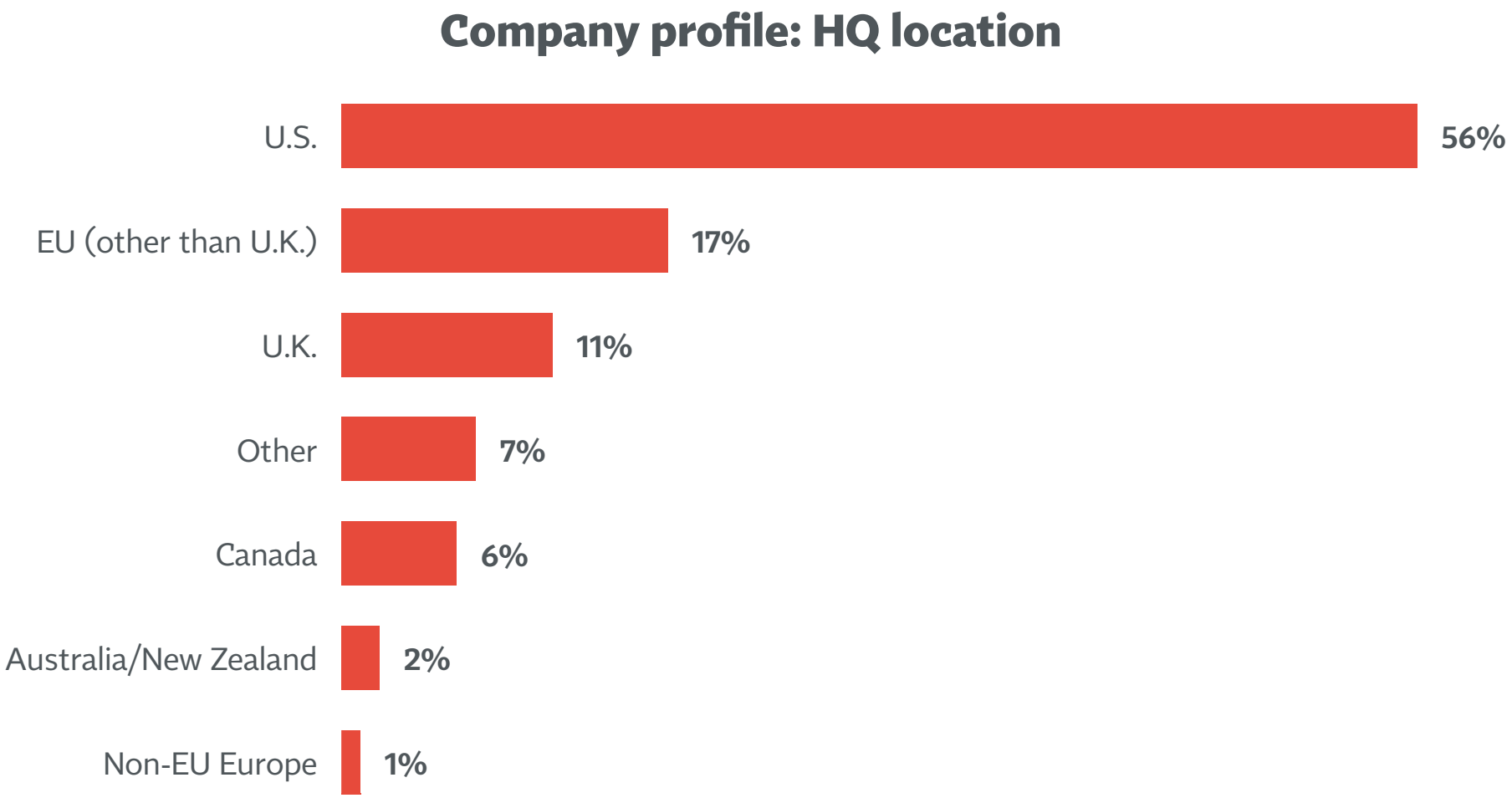
A total of **473 respondents** completed the survey this year. Email invitations to take the survey were sent, along with several reminders, to subscribers of the IAPP's Daily Dashboard. The survey was fielded in August and September of 2020 by Fondulas Strategic Research.

As with any survey iterated on an annual basis using different pools of respondents, variations in the sample from year to year may affect the results. One factor this year is that there were significantly **more respondents based in the U.S.** and **significantly fewer based in the EU** who took the survey compared to last year. Given there are significant differences in U.S. versus EU firms in terms of staff, budget, privacy leadership, tasks, priorities and compliance, this can affect year-to-year comparisons.

# Contents



# More than half of respondents work for an organization based in the U.S.

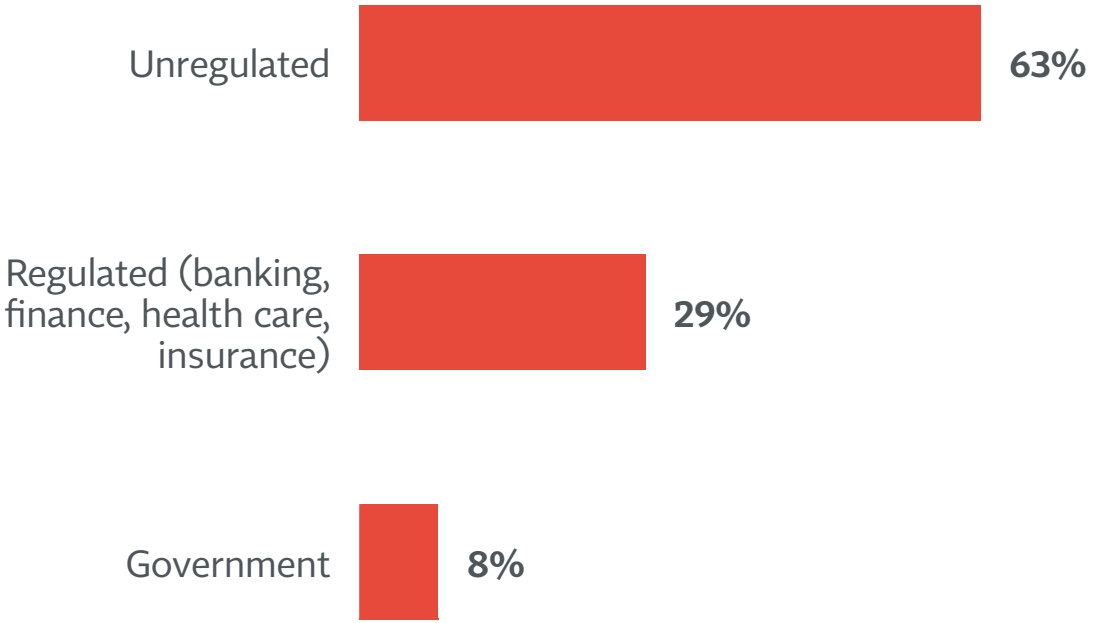



A4: What is the primary location of your company's headquarters?

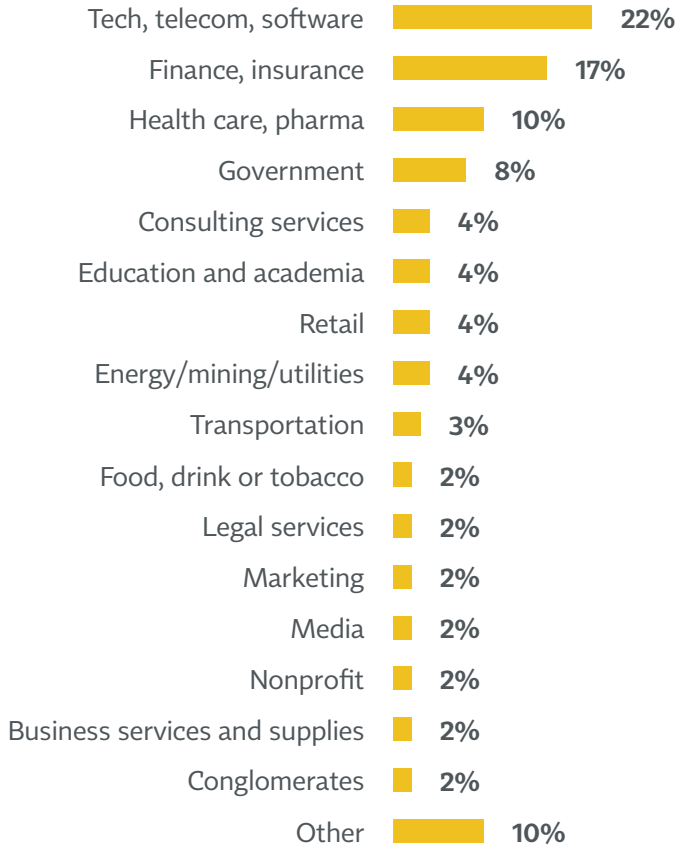
# The largest group of respondents in the survey work in the tech/telecom/software industry

## Company profile: Industry

### Major category




### Specific industry sector

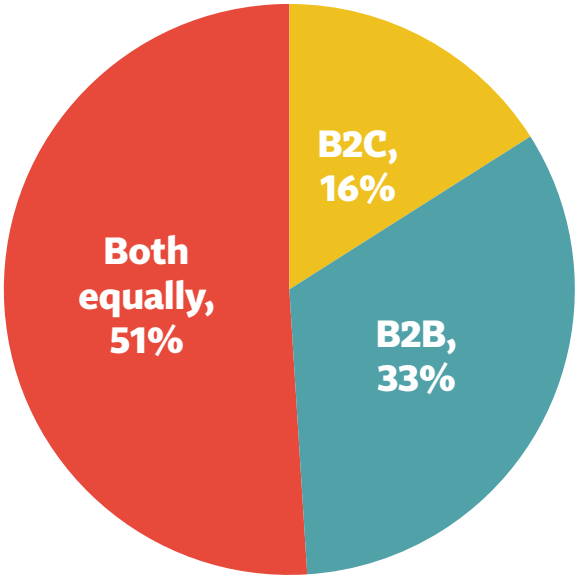



A1: Which sector listed below best describes how your company would be classified?

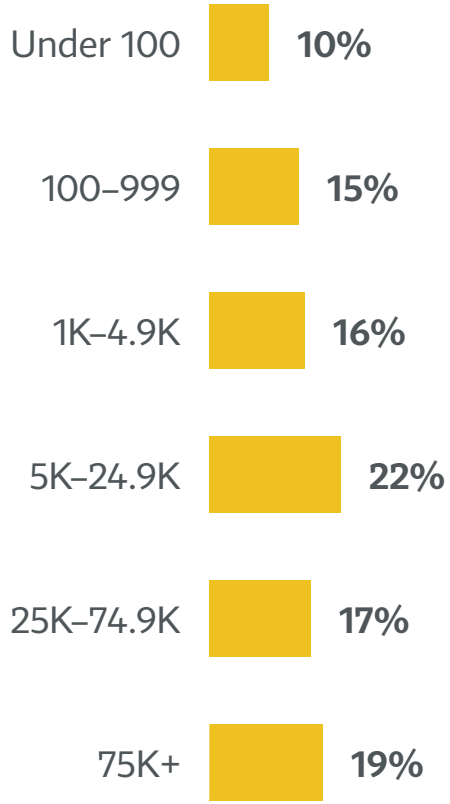
# Respondents were evenly distributed across organizations of various sizes and budgets

## Company profiles

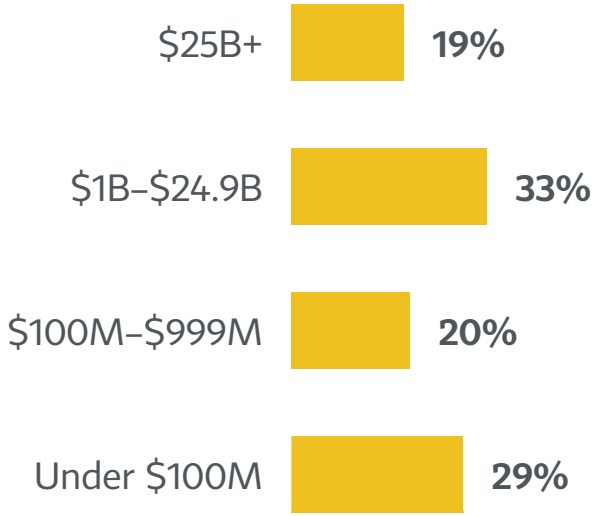
### Business type




### Employees

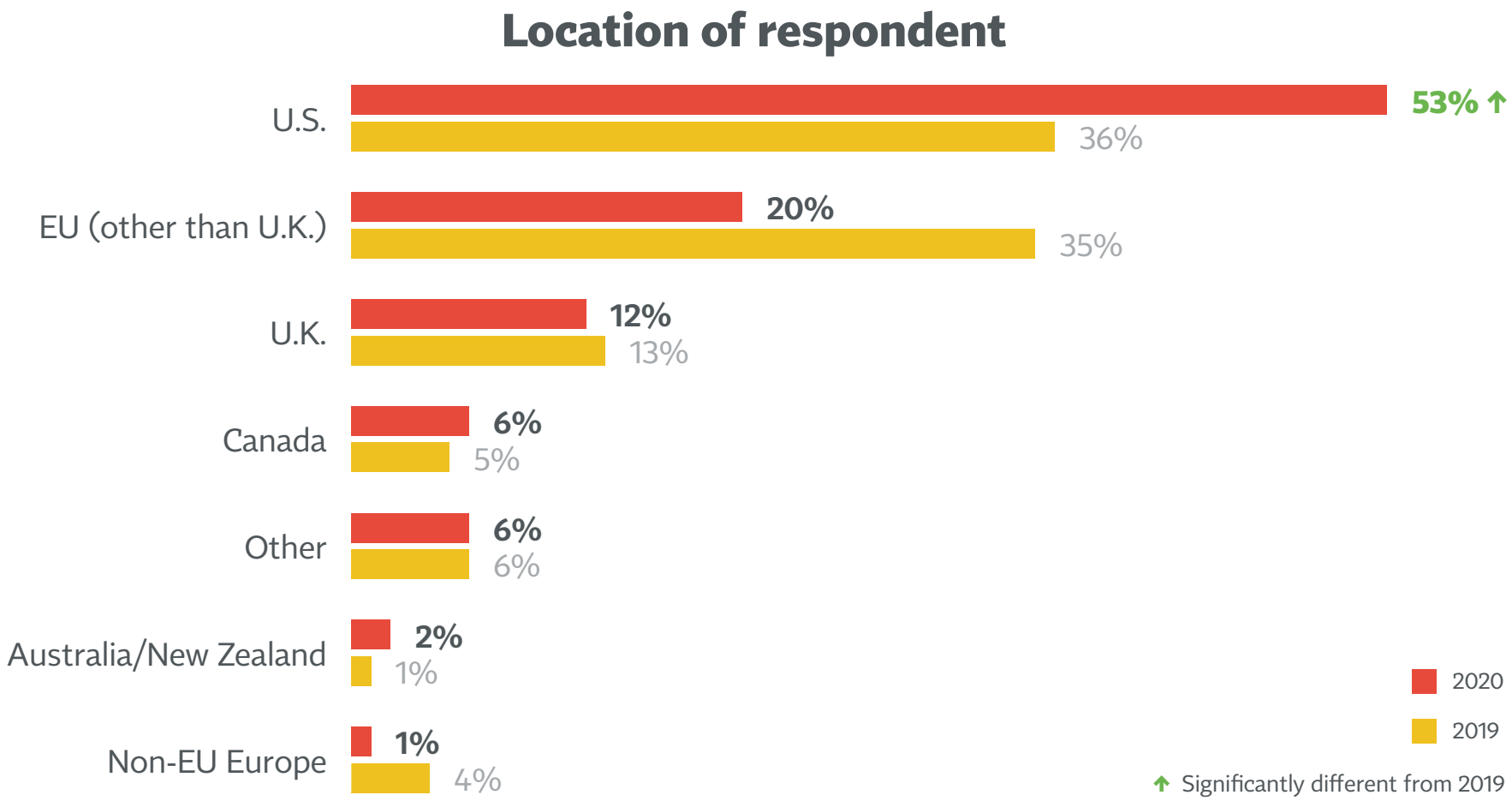



### Revenue




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.

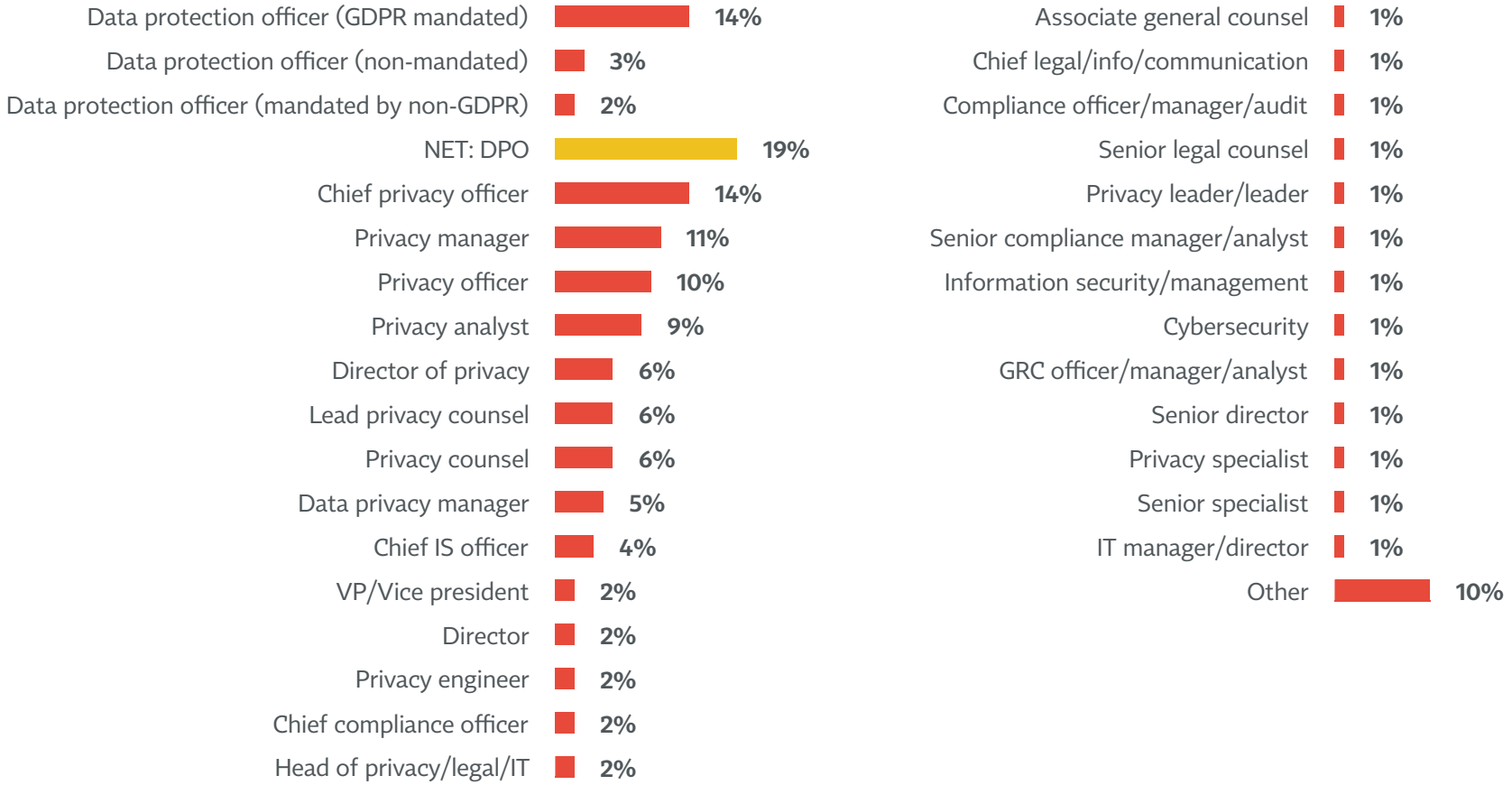
# A greater number of respondents this year are U.S.-based, and fewer EU-based, compared to last year




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

# DPO was the most common title, followed by CPO

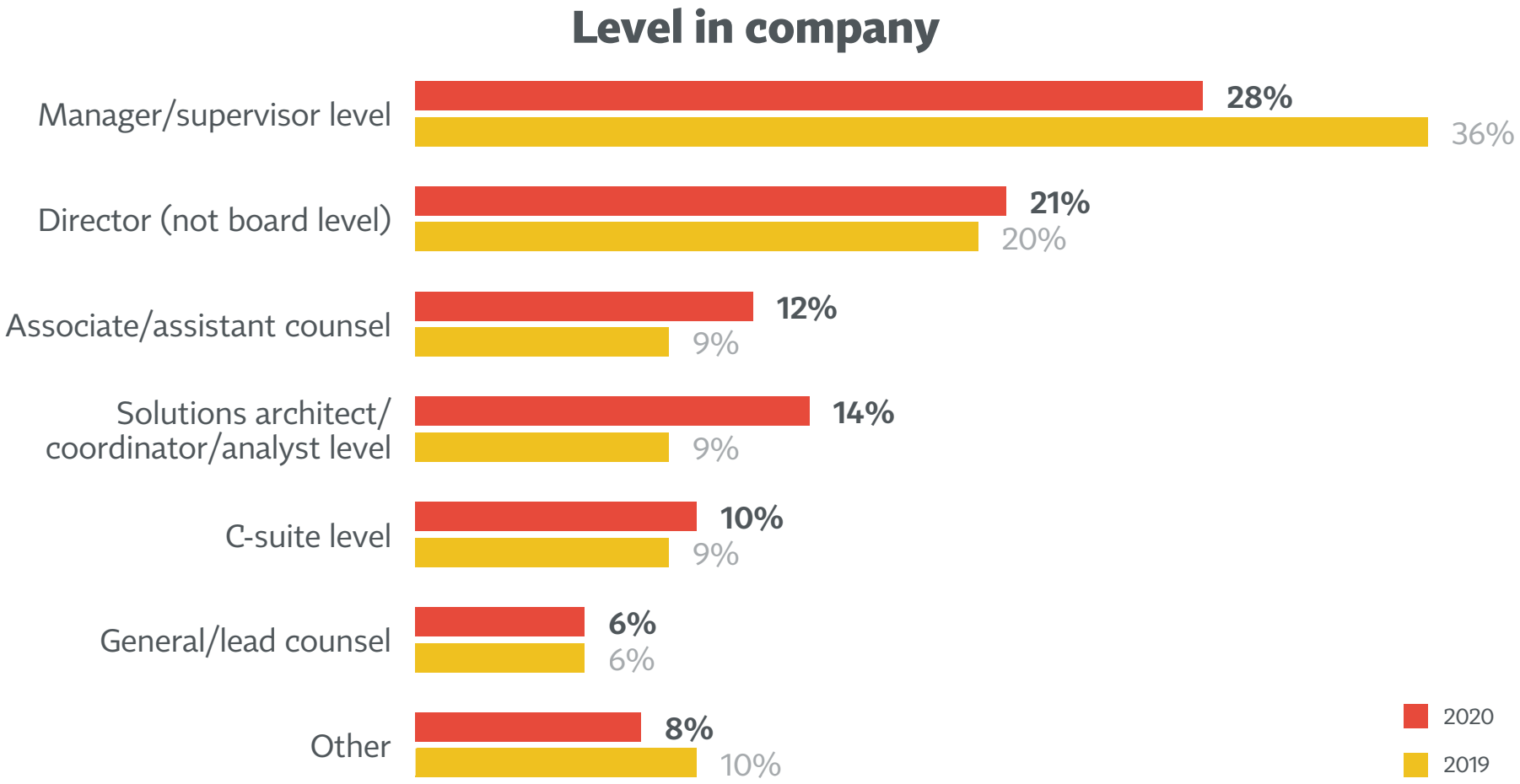
## Respondent title*




***Given that some respondents held more than one job title, the total adds to more than 100%.***

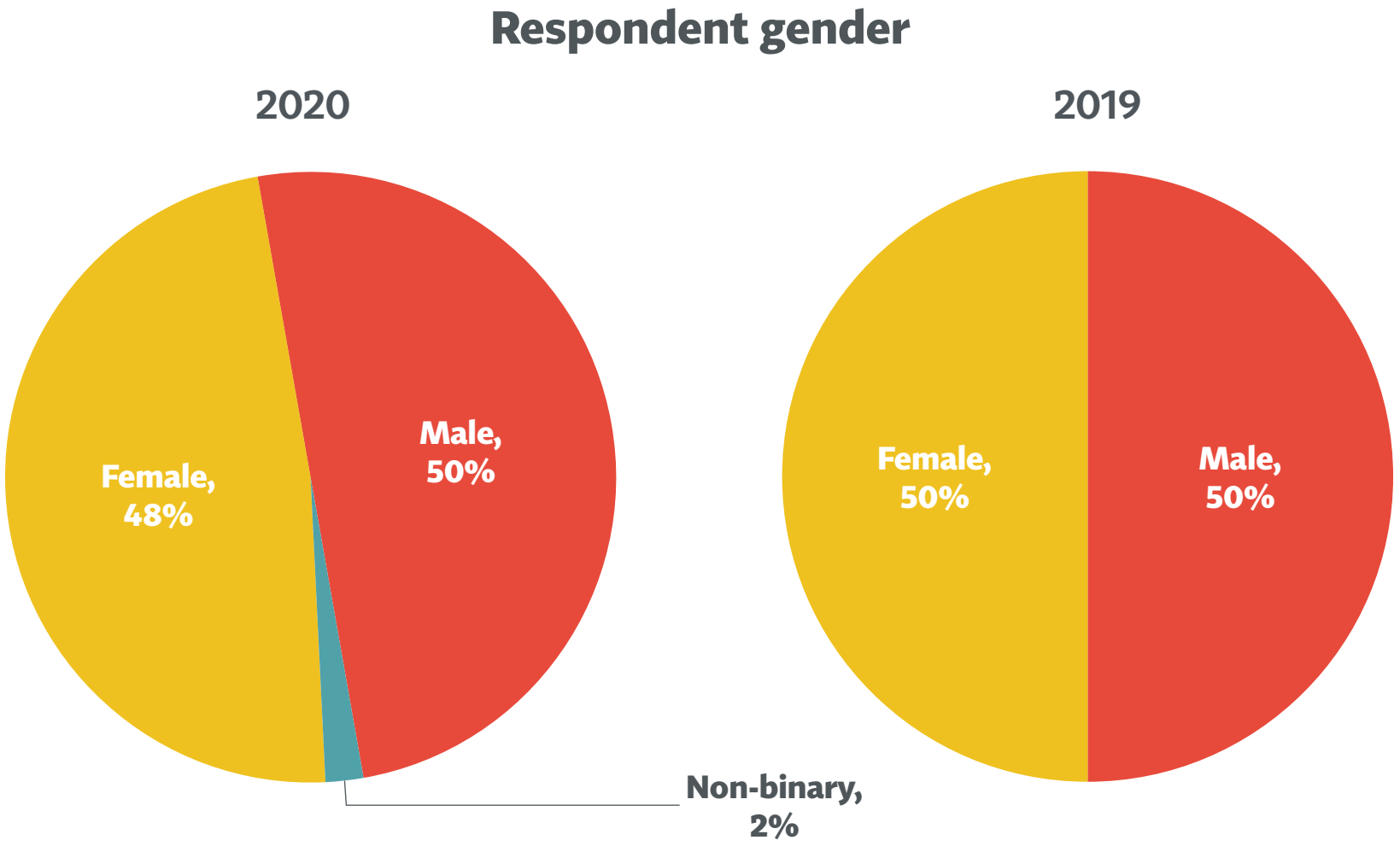
D2A: What is your job title?

# About half of respondents were at the manager, supervisor or director (non-board) level




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

# Respondents were evenly split by gender, similar to 2019



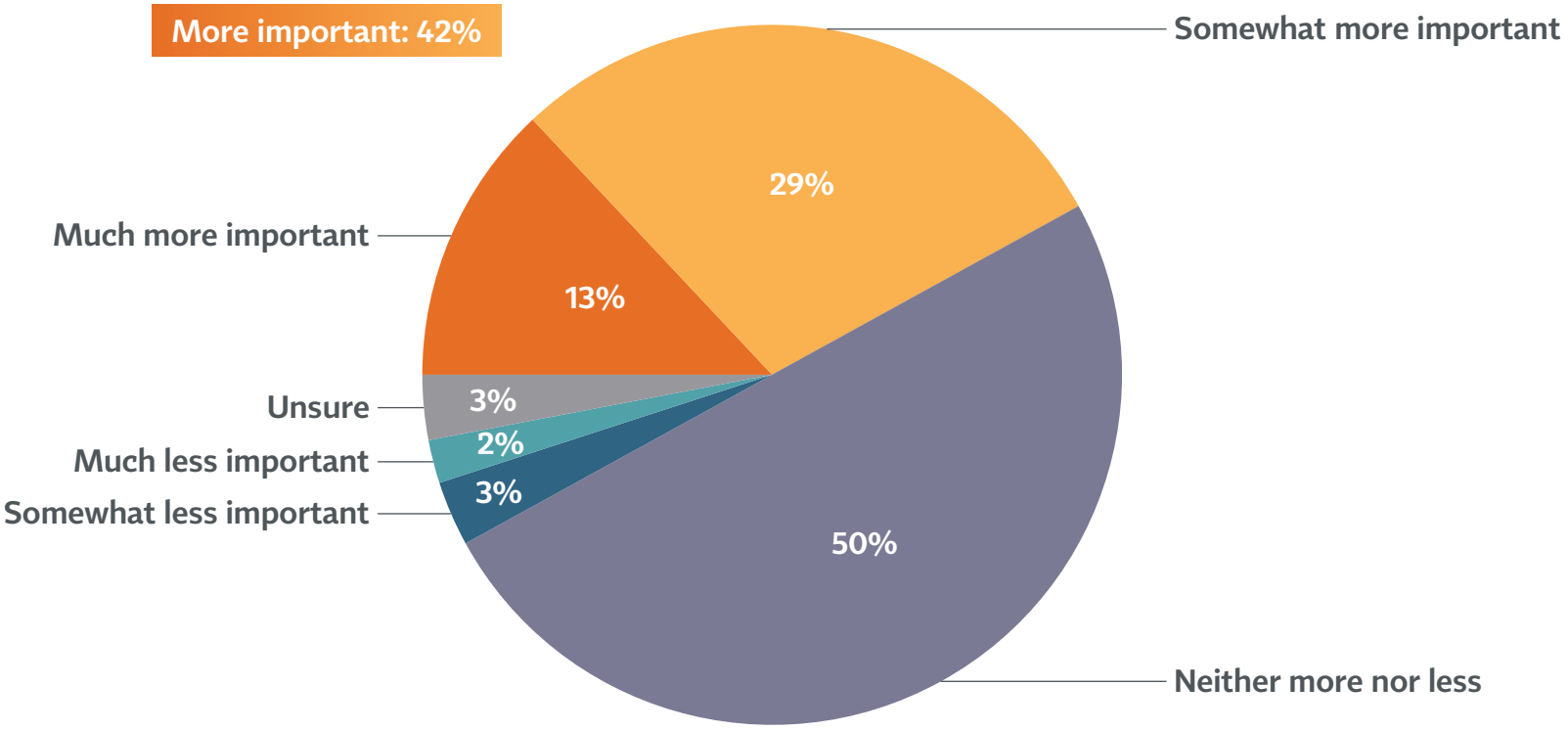

I12: Are you…

# Contents



# 4 in 10 firms said privacy has become more important within their organization during the COVID-19 pandemic

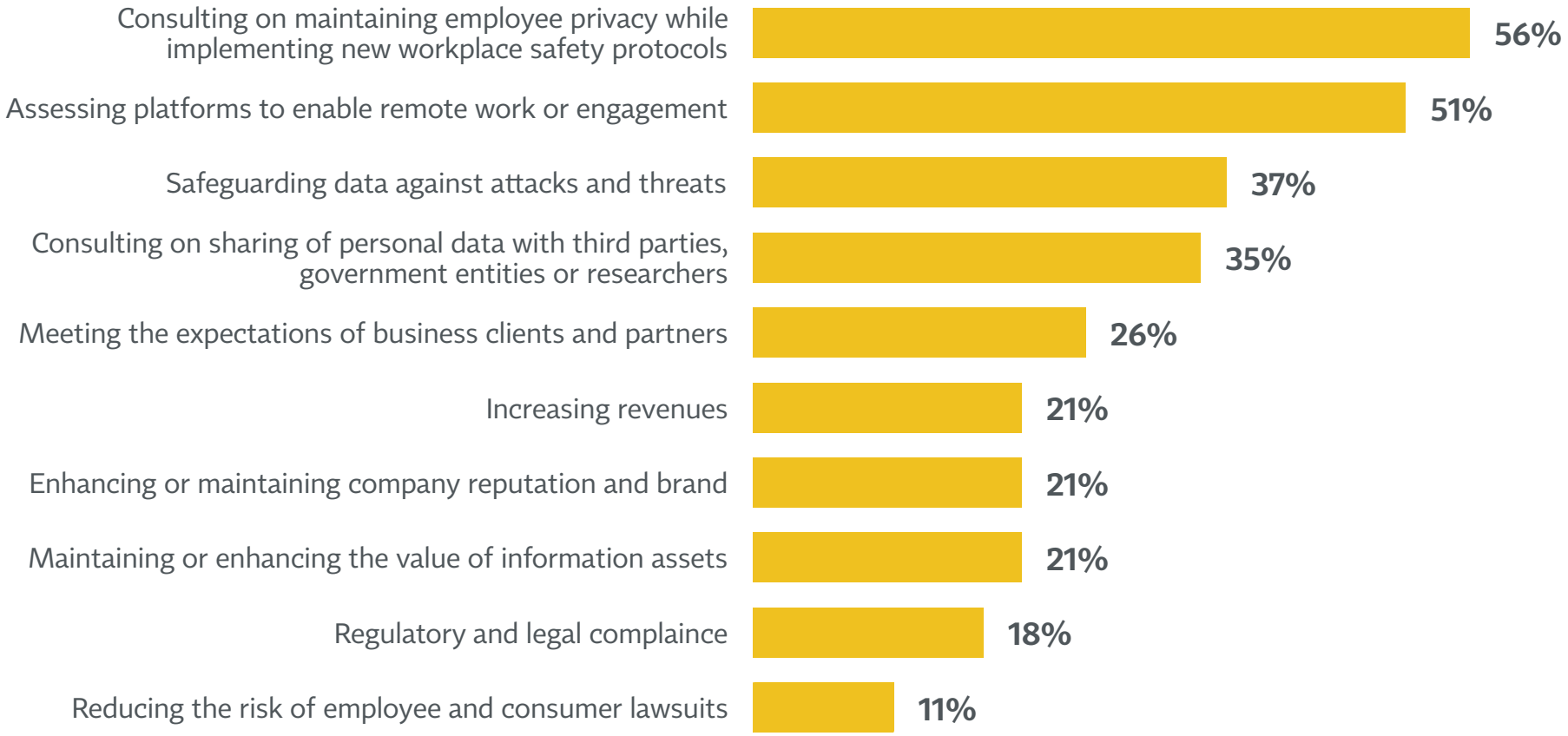
## Impact of COVID-19 on privacy importance




CV1: How has the importance of privacy changed within your organization, if it has at all, in the wake of COVID-19?

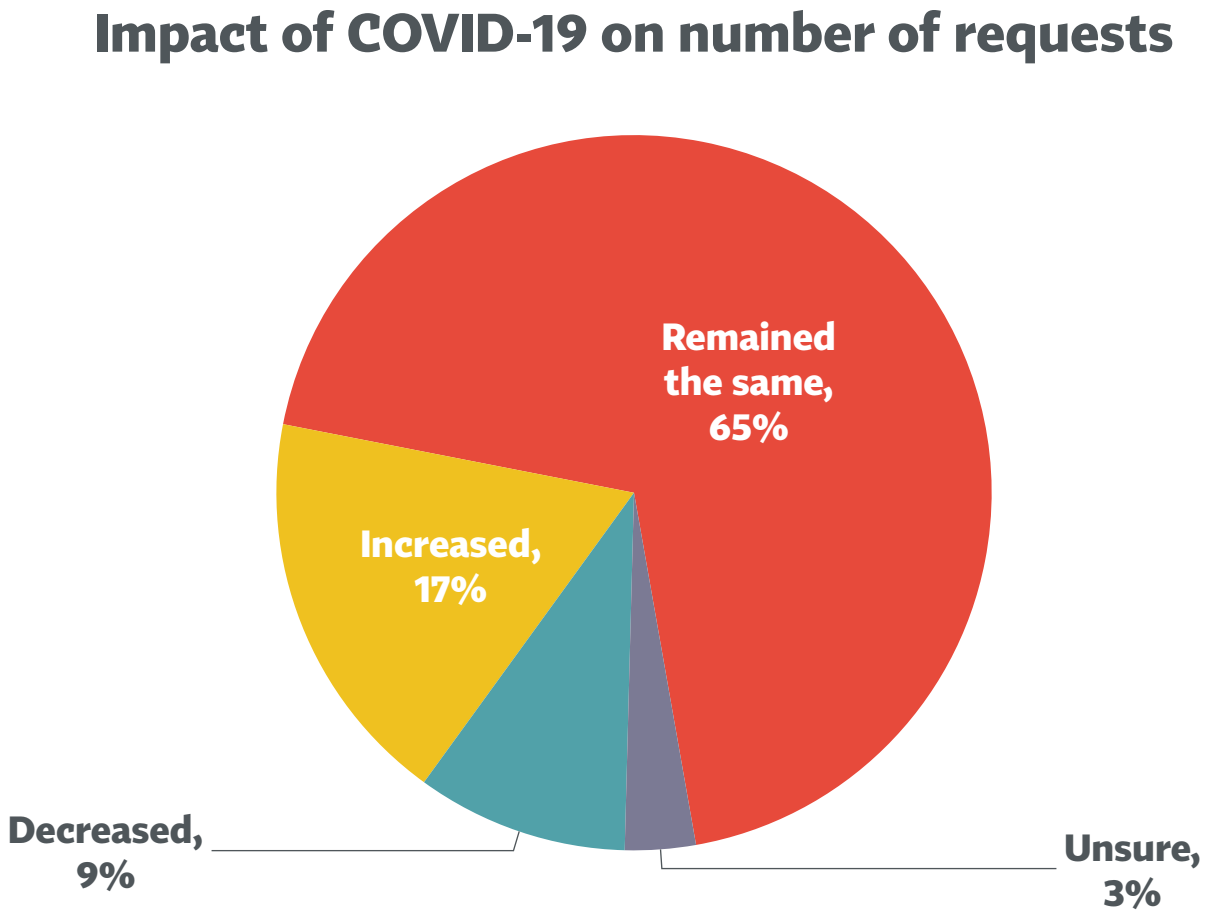
# Dealing with remote working and new workplace safety protocols have become top priorities during COVID-19

## Tasks 'more' of a priority since COVID-19



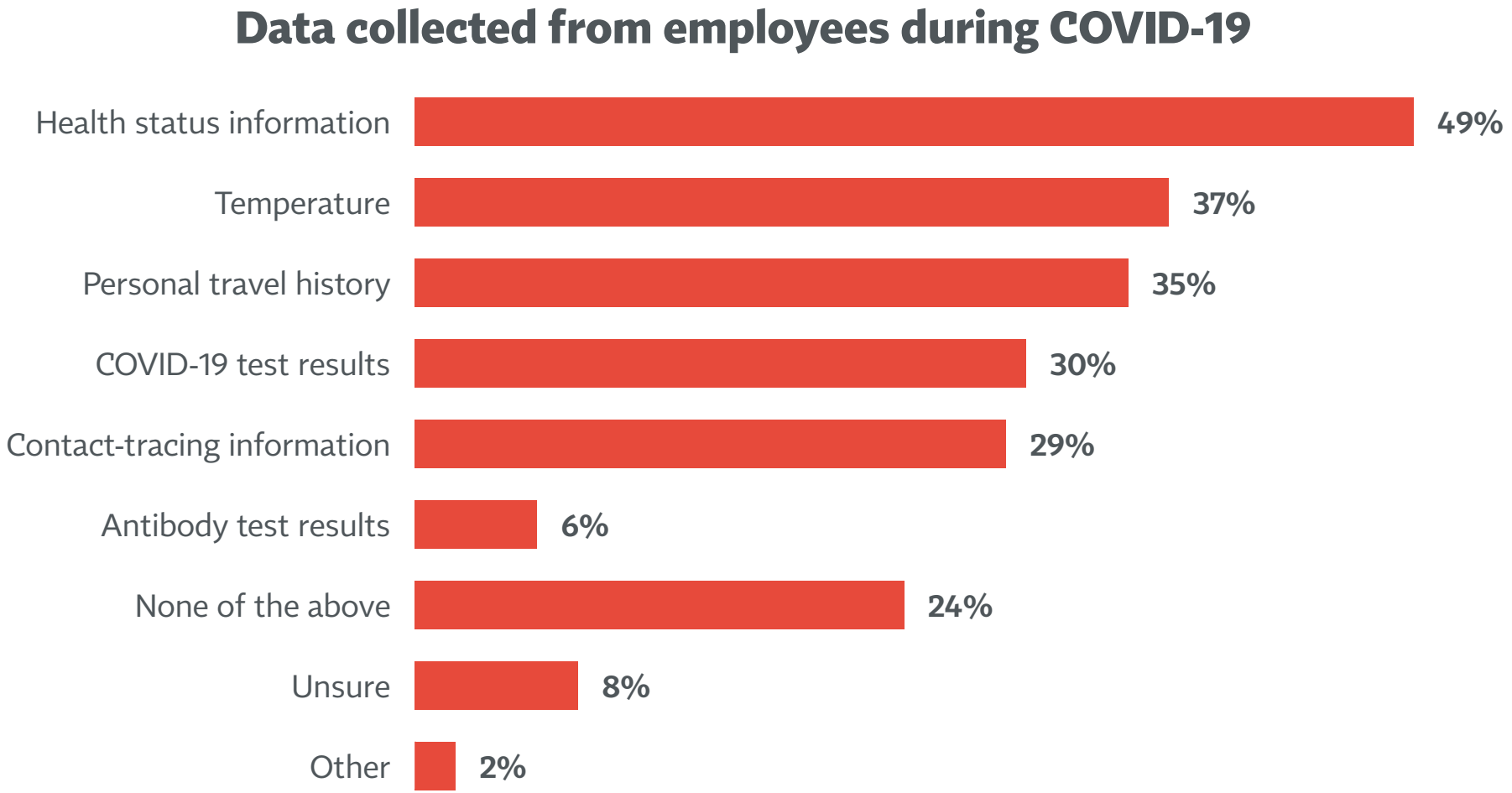

CV2: Since the COVID-19 pandemic began, how have your privacy tasks and responsibilities changed, if they have at all?

# Although two-thirds have seen no change in DSRs, 17% said requests have increased




CV3: Since the COVID-19 pandemic began, has the number of data subject access, correction, deletion or restriction requests your organization receives increased, decreased or remained about the same?

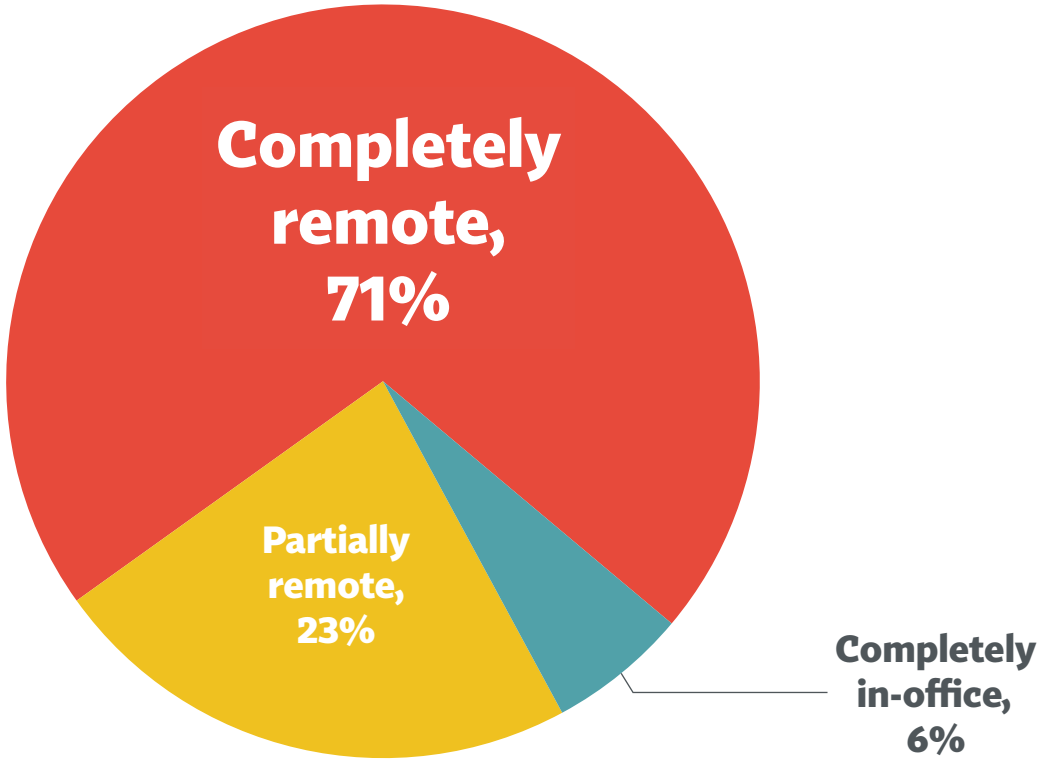
# Firms are most likely to collect health status, temperature and travel history from employees due to COVID-19




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

# 7 in 10 survey respondents said they are currently working completely remotely

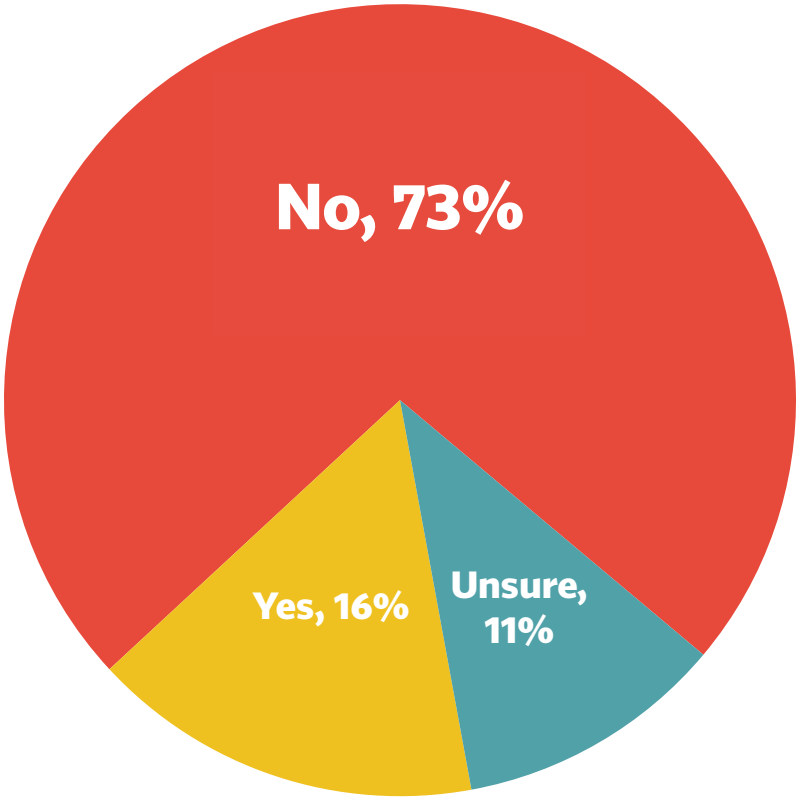
## Current working arrangement
(Base: Have collected data or employees working from home)




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

# While firms have many more remote employees, the vast majority have not changed how they monitor their activity

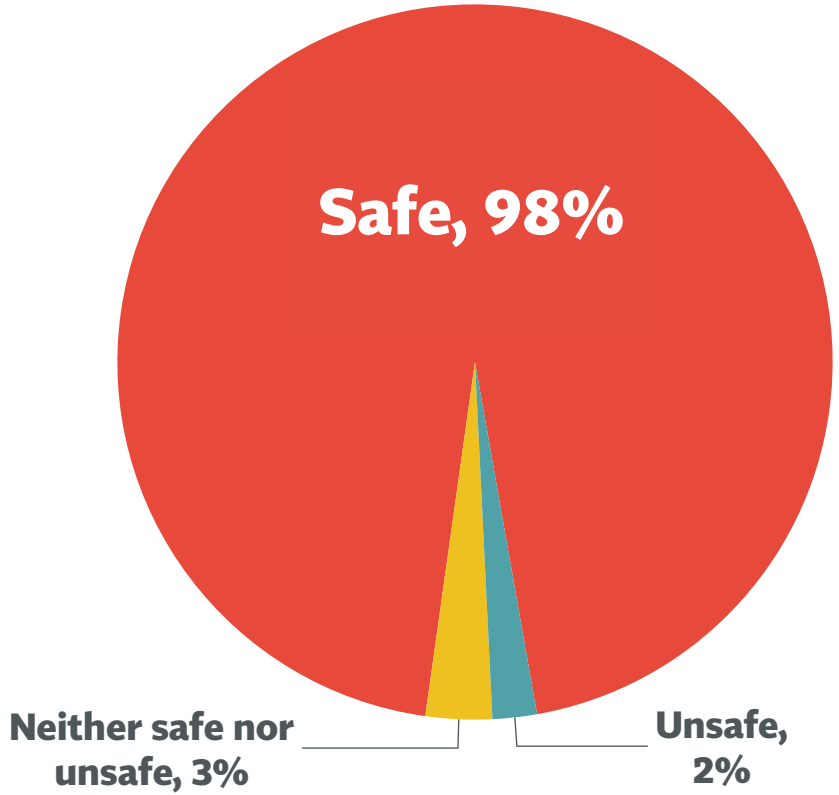
## Begun or increased monitoring of remote employees




CV5: Has your organization begun to monitor or increased monitoring of employees working remotely during the pandemic (e.g., to monitor productivity or protect information assets)?

# Nearly all feel safe in their current working arrangement, although the percent is a bit lower for those on-site

## Feelings about current working arrangement
(Base: Have collected data or employees working from home)

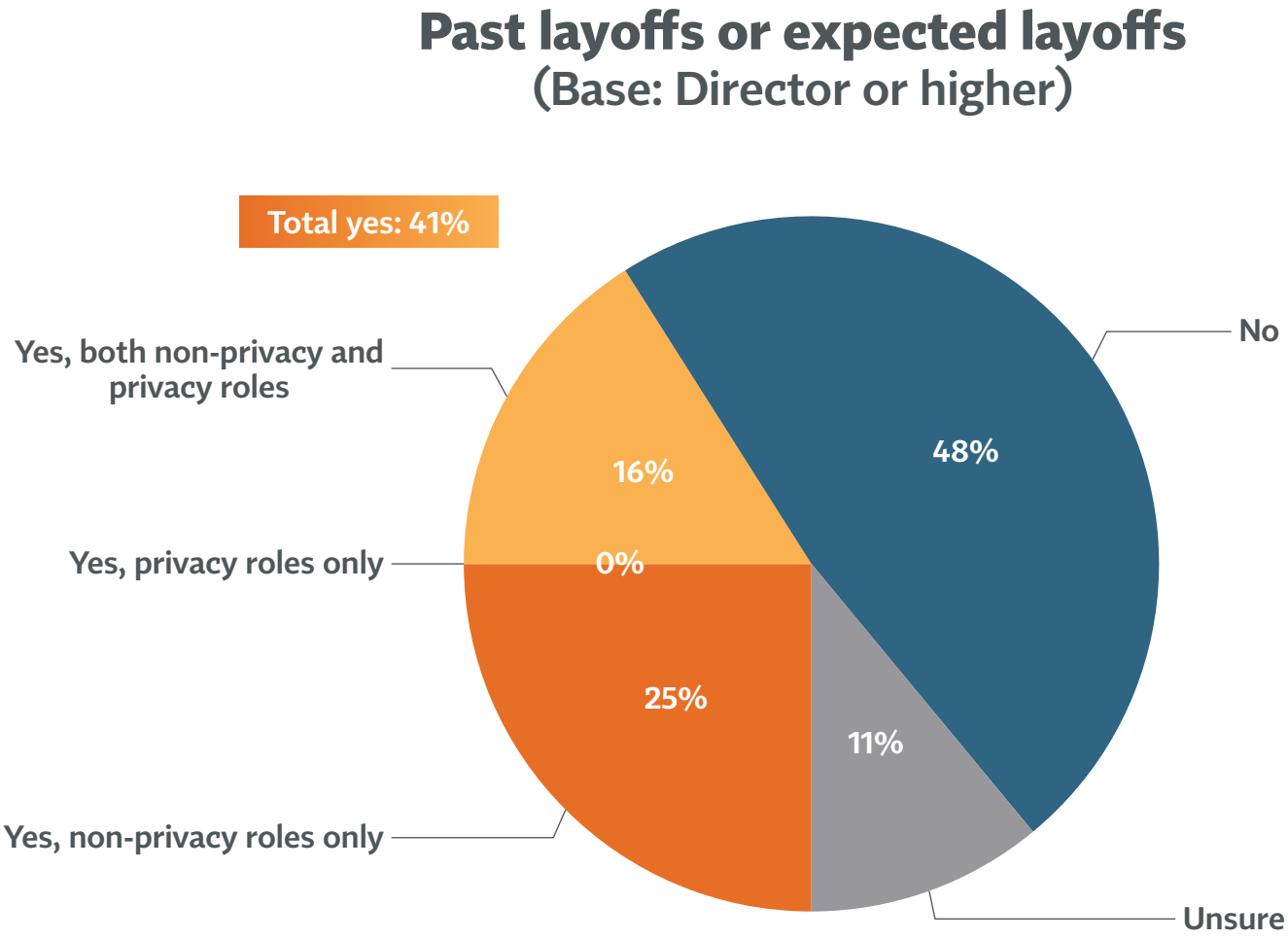



### BY WORK ARRANGEMENT

| | Completely remote | Partially remote | Completely in office/ work site |
|---|---|---|---|
| **Feelings re: work arrangement** | | | |
| Safe | 98% | 91% | 80% |
| Unsafe | 1% | 5% | 8% |
| Neither | 2% | 4% | 12% |

CV8: In light of the health risks posed by the COVID-19 pandemic, how safe or unsafe do you feel with your current working arrangement?

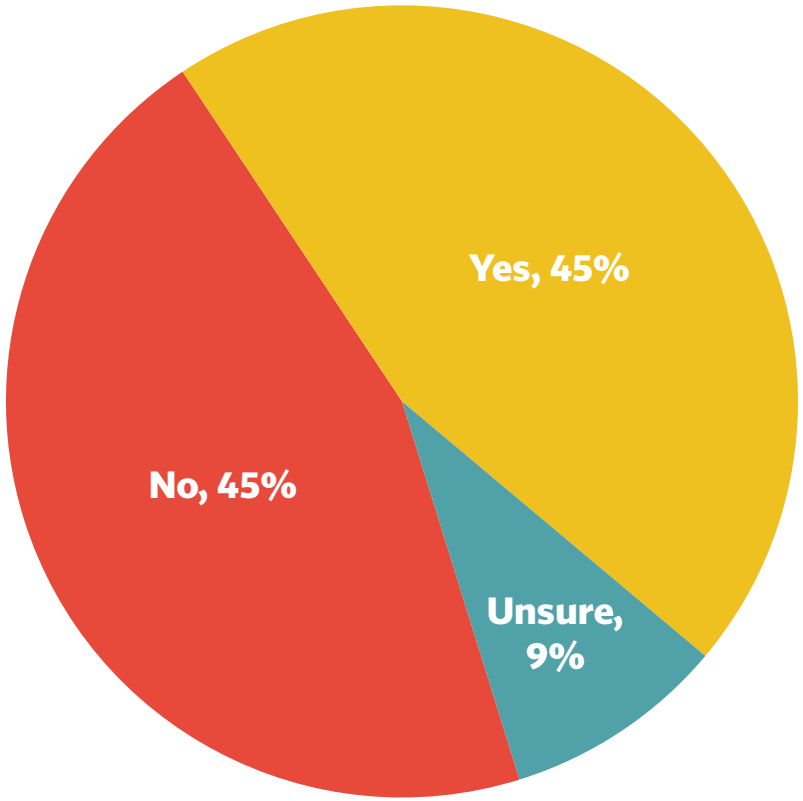
# For companies that saw or expect to see layoffs, almost 2 in 3 affected non-privacy roles alone




F2a: In the past six months or over the next 12 months, has your organization laid off or do you expect it to lay off workers, either in general or specifically in your privacy program?

# Only half of the firms collecting employee data related to COVID-19 have conducted a privacy risk assessment

## Assessment done since COVID-19?
(Base: Have collected data or employees working from home)



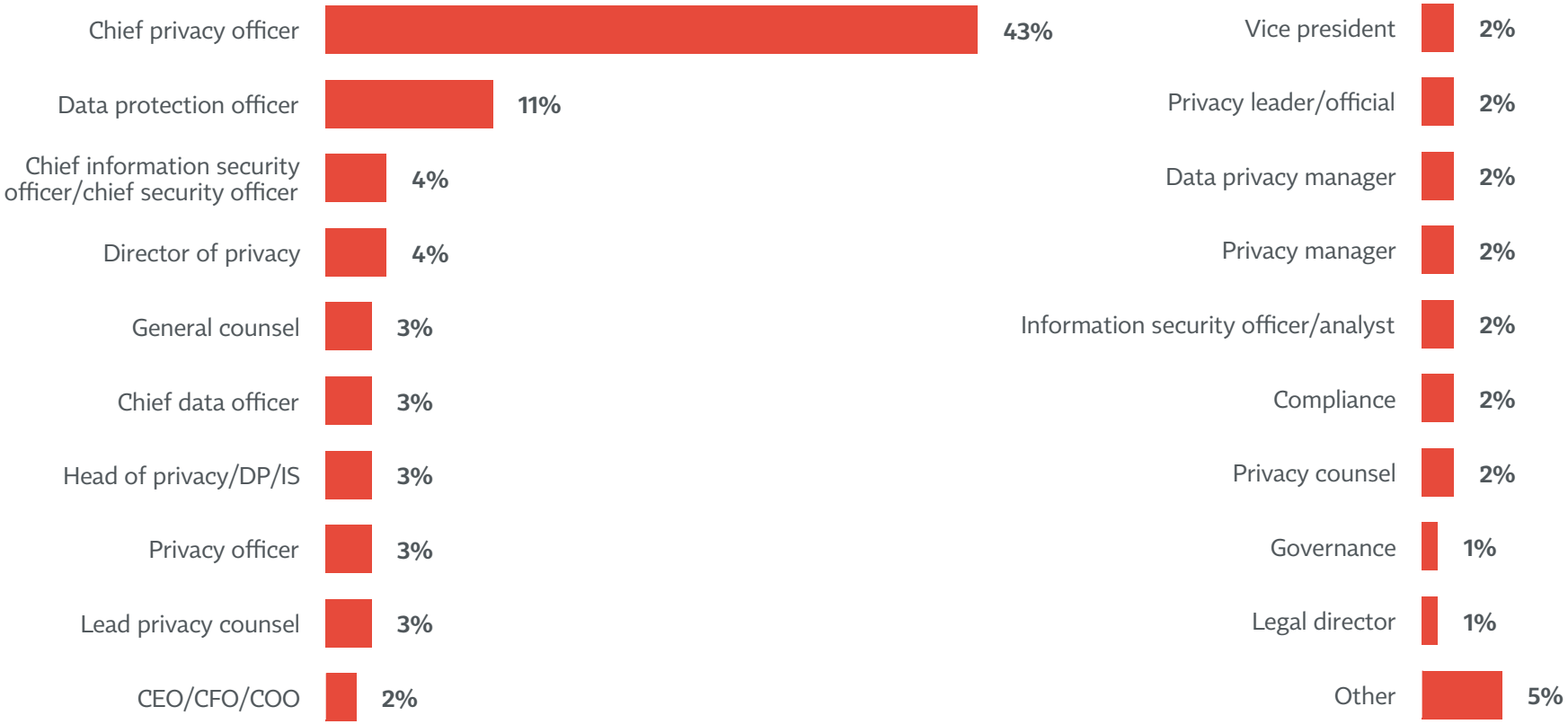

CV6: Has your organization conducted a privacy risk assessment or data protection impact assessment specifically with regards to the data collected from employees in the context of COVID-19?

# Contents



# About half of privacy leaders hold the title of CPO or DPO

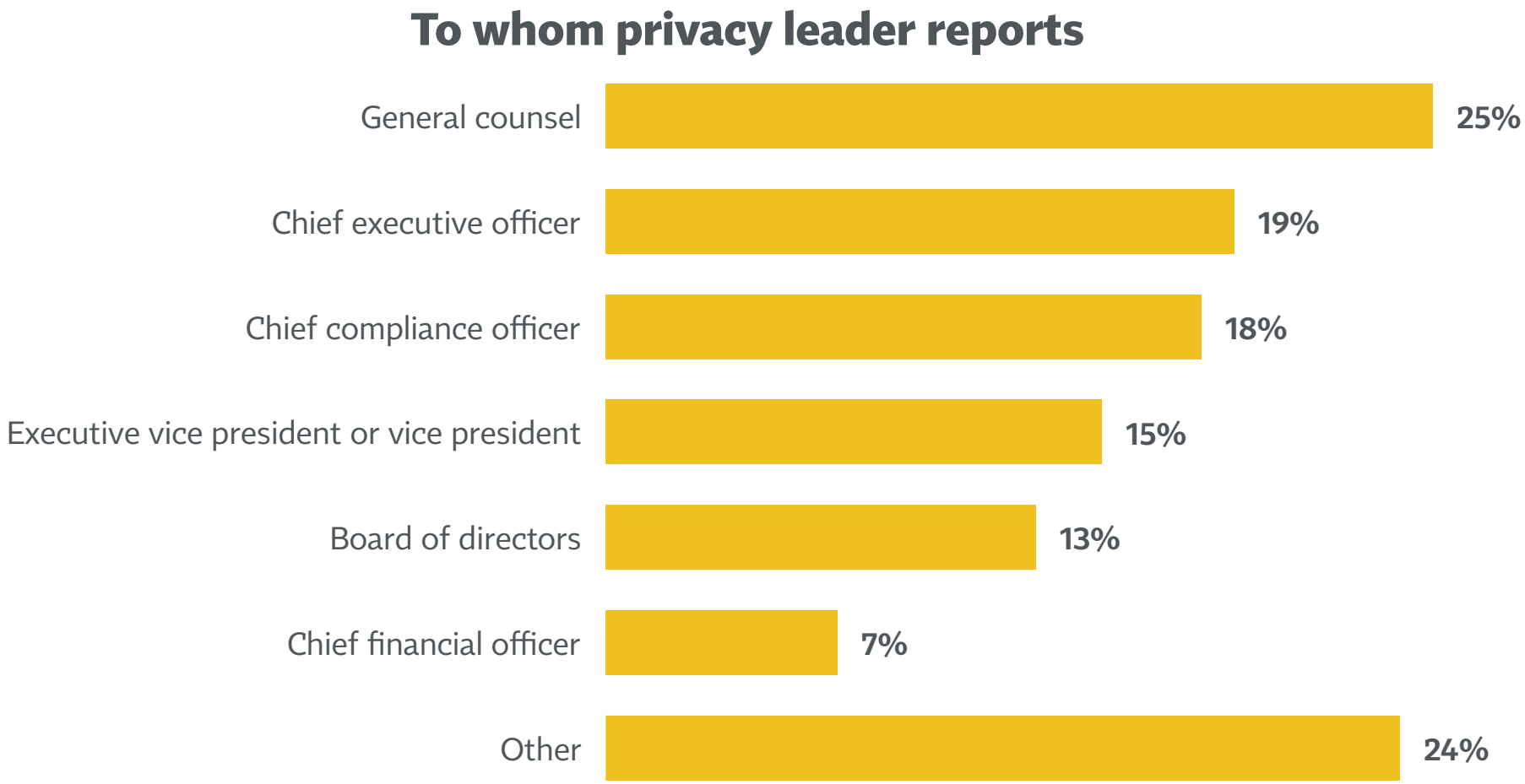
## Job title of the privacy leader*
(Base: Director or higher, have internal privacy position)




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

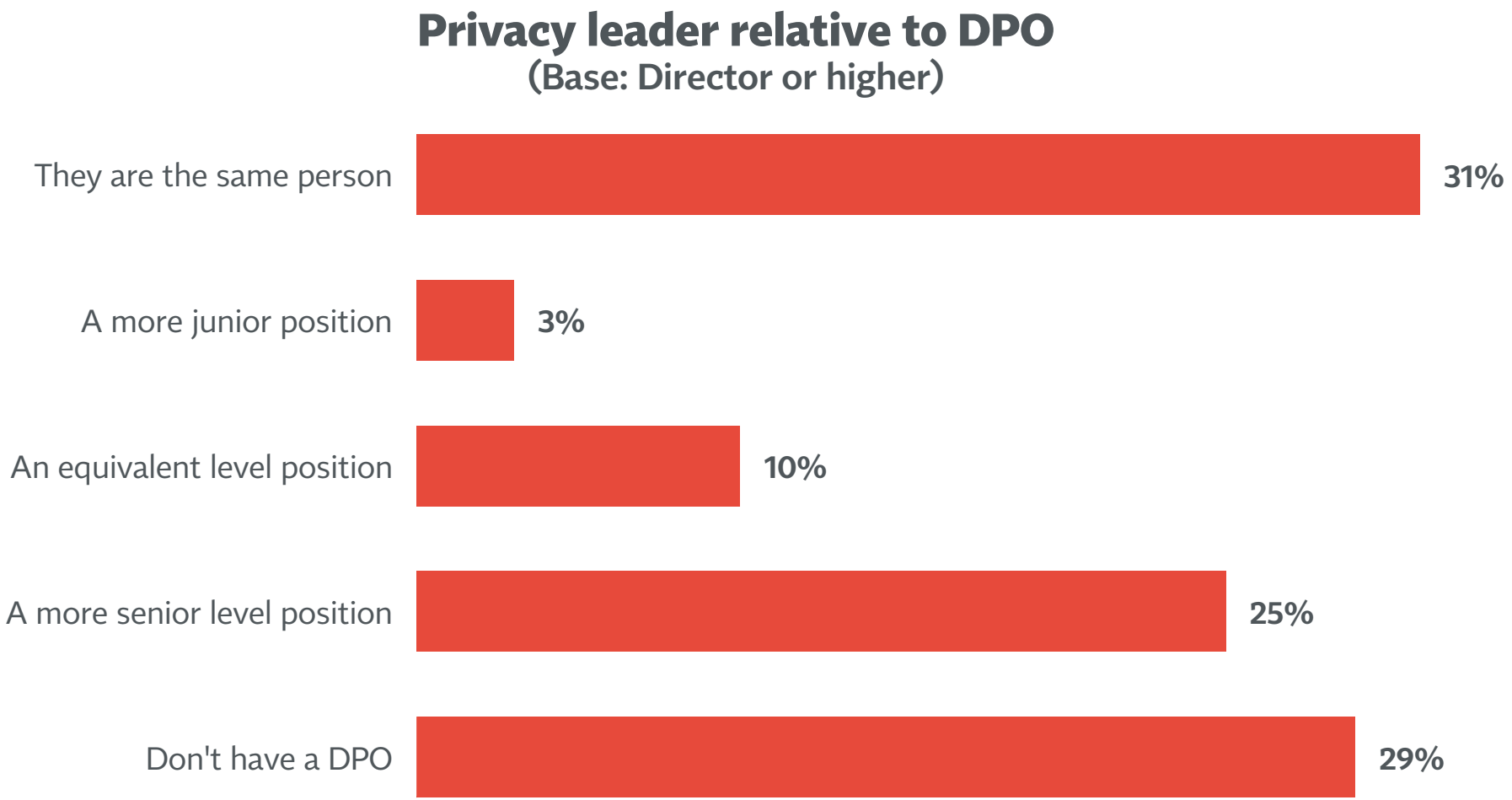
F21: What is the job title of the privacy leader in your company?

# Most privacy leaders report to the general counsel, CEO or chief compliance officer



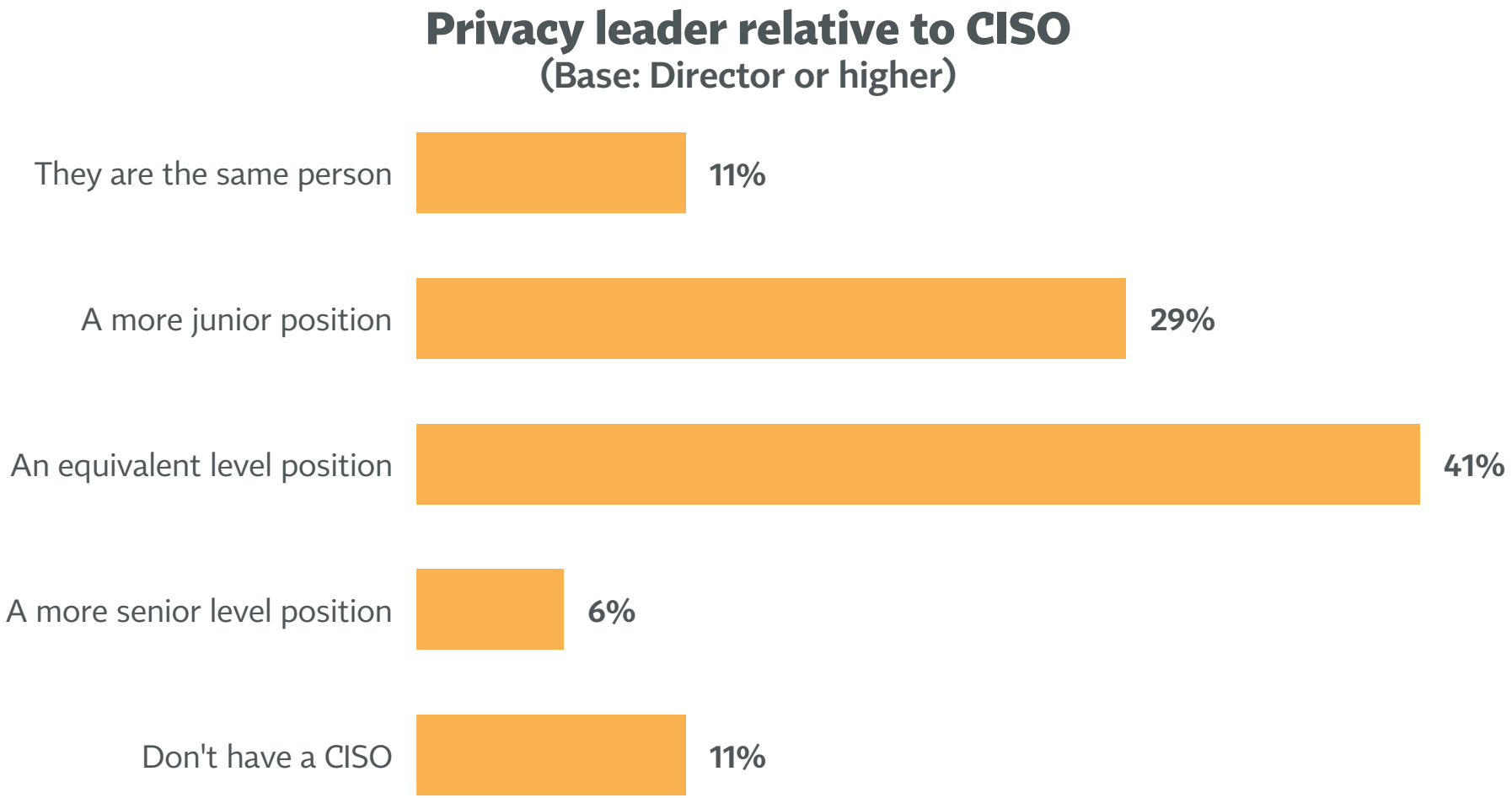

F25: To whom in your company does the privacy leader report?

# Within about 1 in 3 organizations, the DPO is also the privacy leader




F31: How does the position of privacy leader compare with your company's data protection officer, if any?

# In half of firms, the CISO and privacy leader are at the same level or are the same person; for most others, CISO is higher




F22: How does the position of the privacy leader compare with your company's chief information security officer (CISO) or the highest level information security person in the company?

# Privacy leaders at smaller firms are more likely to report directly to the board of directors

## BY COMPANY REVENUE

| | Under $100M | $100M-$999M | $1B-$24.9B | $25B+* |
|---|---|---|---|---|
| **Privacy leader reports to:** | | | | |
| General counsel | 15% | 29% | 38% | 24% |
| Chief compliance officer | 12% | 15% | 22% | 26% |
| Board of directors | 20% | 12% | 7% | 11% |

## BY EMPLOYEE SIZE

| | <5K | 5-24.9K | 25K-74.9K | 75K+* |
|---|---|---|---|---|
| **Privacy leader reports to:** | | | | |
| General counsel | 20% | 35% | 25% | 20% |
| Chief compliance officer | 9% | 22% | 27% | 25% |
| Board of directors | 17% | 13% | 11% | 8% |

* Small sample size

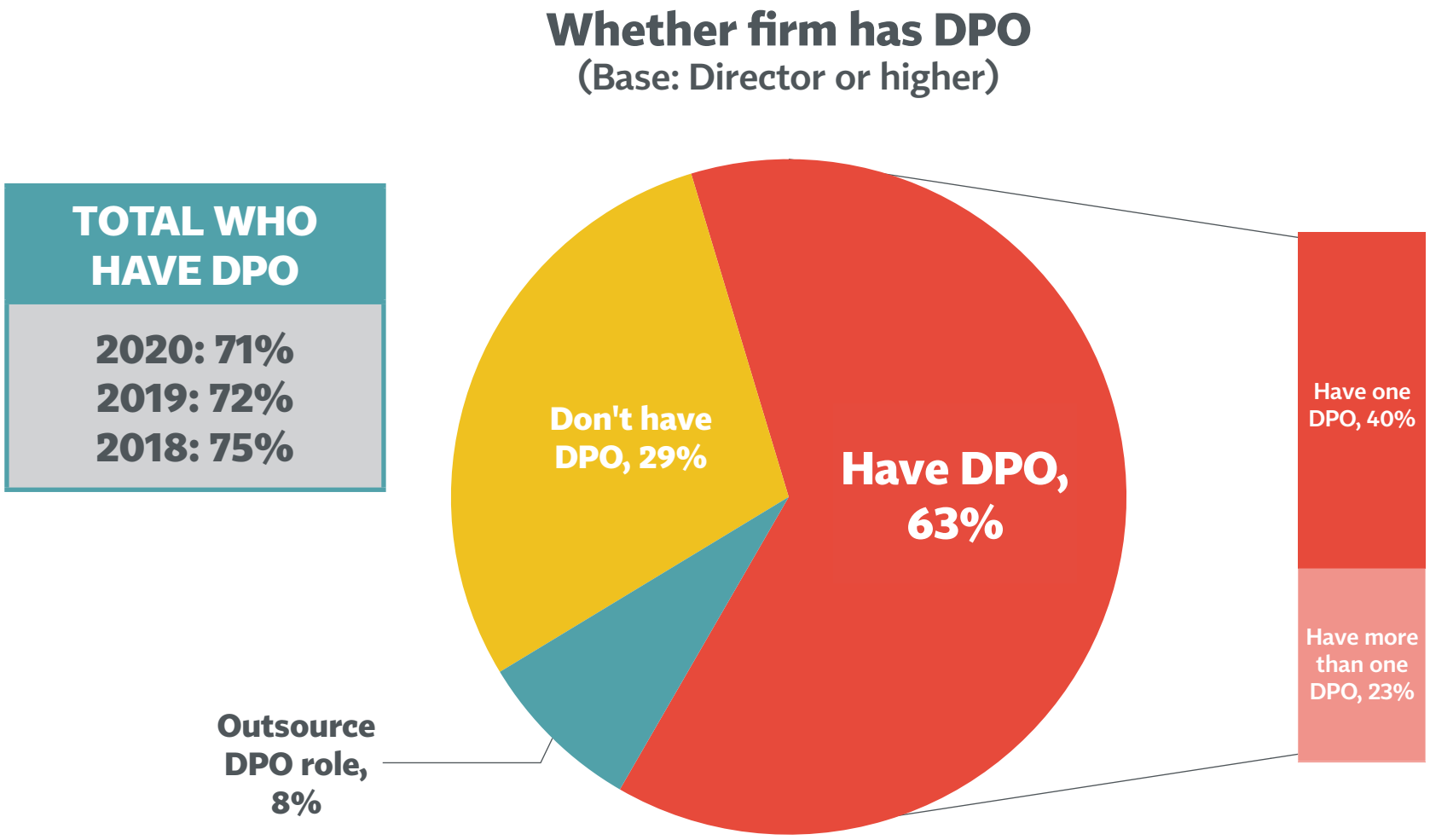
# U.S. privacy leaders are more likely to report to general counsel, less likely to report to the board

**BY HQ LOCATION**

| | U.S. | EU |
|---|---|---|
| **Privacy leader reports to:** | | |
| CEO | **13%** | 24% |
| General counsel | **32%** | 19% |
| Board of directors | **5%** | 30% |

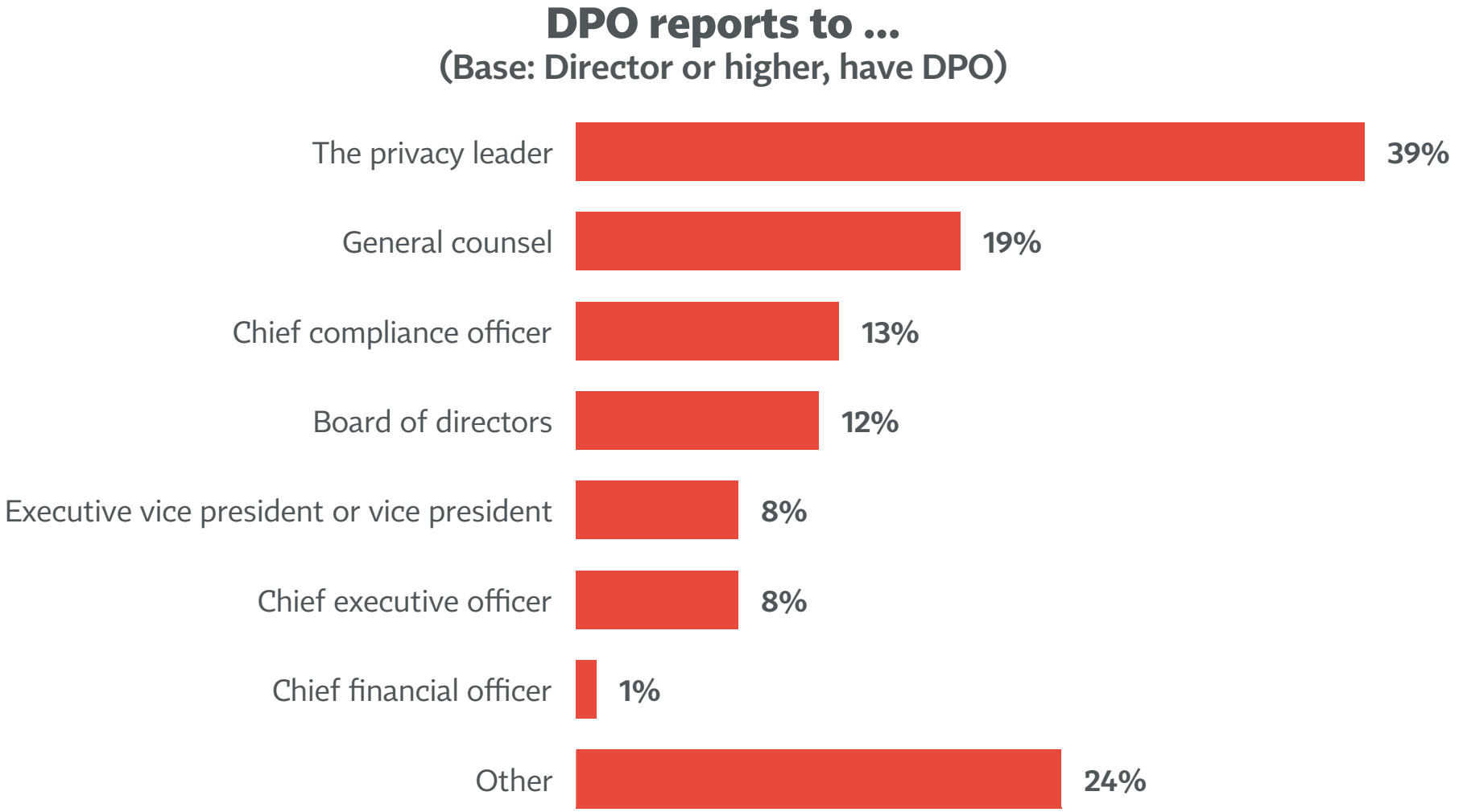
Significantly different than other segments

# About 7 in 10 firms have a DPO, with almost 1 in 10 outsourcing the role




F28: Are you the data protection officer, or is that someone else?
F30: Does your company have only one data protection officer or does it have more than one?

# Most DPOs report to the privacy leader, general counsel or CCO




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

# Almost half of privacy pros in the EU serve as their organization's DPO, compared to just 1 in 5 in the U.S.

## BY HQ LOCATION

| | U.S. | EU |
|---|---|---|
| Respondent is DPO | **20%** | 45% |

## BY EMPLOYEE SIZE

| | <5K | 5K–24.9K | 25K–74.9K | 75K+* |
|---|---|---|---|---|
| Respondent is DPO | 36% | 28% | 23% | 11% |

## BY COMPANY REVENUE

| | Under $100M | $100M–$999M | $1B–$24.9B | $25B+* |
|---|---|---|---|---|
| Respondent is DPO | 33% | **45%** | 19% | 18% |

Significantly different than other segments

* Small sample size

# DPOs tend to be the privacy leader at smaller organizations based elsewhere than the U.S.

**BY DPO STATUS**

| | DPO IS PRIVACY LEAD | DPO IS NOT PRIVACY LEAD |
|---|---|---|
| Mean company revenue | $7.3B | $14.4B |
| Mean company employees | 10,788 | 29,113 |
| Mean total privacy employees | 25 | 16 |
| HQ in U.S. | 31% | 72% |
| Respondent is in U.S. | 30% | 71% |
| Privacy team responsible for GDPR compliance | 95% | 69% |
| Privacy team responsible for CCPA compliance | 50% | 69% |

# Contents



# EU firms have more full-time privacy staff; U.S. firms have more working on privacy part-time

## Privacy staff: Mean

| | Overall |
|---|---|
| Full-time privacy staff | 15 |
| Part-time privacy staff | 18 |

## Mean privacy staff size by HQ location

| | U.S. | EU |
|---|---|---|
| Full-time privacy staff | 9 | 13 |
| Part-time privacy staff | 21 | 15 |

***NOTE: Outliers over 999 removed.***

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

# The biggest privacy staffs are found at organizations with many employees and high revenues

## Mean privacy staff size by total employee size and company revenue

| | <5K | 5K–24.9K | 25K–74.9K | 75K+* |
|---|---|---|---|---|
| Full-time privacy staff | 4 | 9 | 12 | 53 |
| Part-time privacy staff | 8 | 14 | 48 | 18 |

| | Under $100M | $100M–$999M | $1B–$24.9B | $25B+* |
|---|---|---|---|---|
| Full-time privacy staff | 5 | 8 | 9 | 21 |
| Part-time privacy staff | 14 | 13 | 19 | 33 |

* Small sample size

***NOTE: Outliers over 999 removed.***

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

# Hybrid (B2B/B2C) firms have the largest privacy staffs; government agencies the smallest

## Mean privacy staff by industry category and consumer target

| | Regulated | Unregulated | Gov't* |
|---|---|---|---|
| Full-time privacy staff | 14 | 16 | 3 |
| Part-time privacy staff | 17 | 20 | 9 |

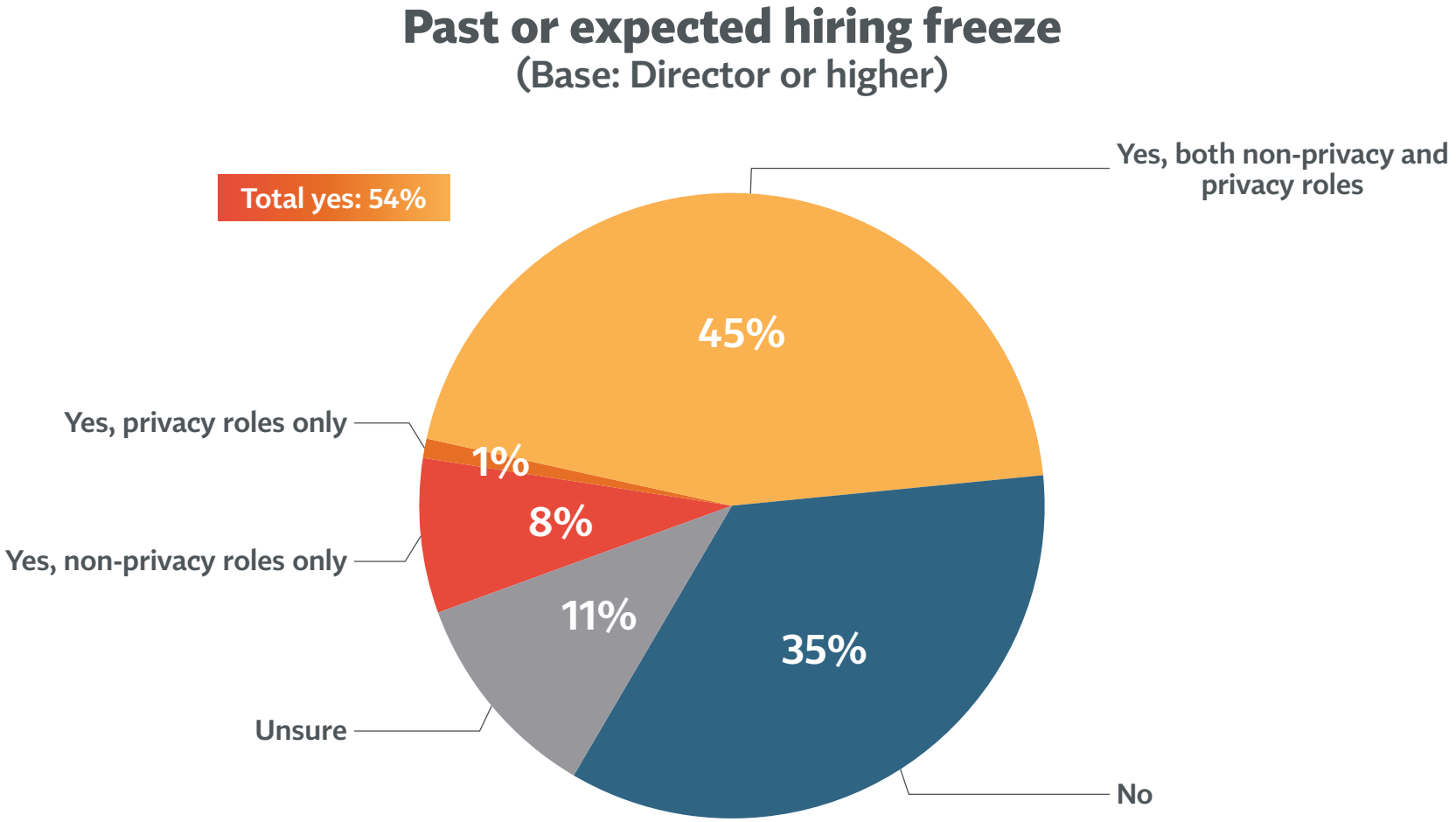
| | B2B | B2C | Both |
|---|---|---|---|
| Full-time privacy staff | 7 | 6 | 24 |
| Part-time privacy staff | 30 | 9 | 13 |

* Small sample size

***NOTE: Outliers over 999 removed.***

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

# More than half of firms have had a hiring freeze or expect one within the next 12 months




F2b: In the past six months or over the next 12 months, has your organization instituted or do you expect it to institute a hiring freeze, either in general or in your privacy program?

# The pandemic has not slowed privacy teams' staffing plans, with hiring in 2020 like 2019

## Expected employee change in coming year

| | % saying increase | | % saying decrease | | % saying stay the same | | Net % change expected (mean) | |
|---|---|---|---|---|---|---|---|---|
| | 2020 | 2019 | 2020 | 2019 | 2020 | 2019 | 2020 | 2019 |
| Full-time privacy staff | 27% | 30% | 3% | 4% | 71% | 66% | +11% | +12% |
| Part-time privacy staff | 12% | 19% | 2% | 2% | 86% | 79% | +4% | +6% |

***NOTE: Outliers over 999 removed.***

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

# Average privacy spending has increased since 2019

## Estimated privacy spend (000)^
(Base: Director or higher)

| TOTAL PRIVACY SPEND |
| --- |
| 2020 MEAN: $676K<br>2019 MEAN: $622K<br><br>2020 MEDIAN: $300K<br>2019 MEDIAN: $200K |

*^This question was changed in 2020 to ask only for total spending, versus last year when the question asked respondents for a breakdown of spending by category. Trend should be interpreted with caution.*

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

# Average privacy spend is significantly higher at companies with higher revenues

## Median estimated privacy spend (000)^
(Base: Director or higher)

### BY EMPLOYEE SIZE

| | <5K | 5K–24.9K | 25K–74.9K | 75K+* |
|---|---|---|---|---|
| Total privacy spend | $269 | $294 | $1,192 | $2,155 |

### BY COMPANY REVENUE

| | Under $100M | $100M–$999M | $1B–$24.9B | $25B or more* |
|---|---|---|---|---|
| Total privacy spend | $343 | $213 | $815 | **$1,850** |

Significantly different than other segments

* Small sample size

# Firms in regulated industries and hybrid (B2B/B2C) spend the most on privacy

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

### BY INDUSTRY CATEGORY

| | Regulated | Unregulated | Gov't* |
|---|---|---|---|
| Total privacy spend | $1,751 | **$454** | $768 |

### BY BUSINESS TYPE

| | B2B | B2C* | Both |
|---|---|---|---|
| Total privacy spend | $431 | $374 | $973 |

Significantly different than other segments

* Small sample size

# U.S. firms spend more on privacy than EU firms

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

| | BY HQ LOCATION | |
|---|---|---|
| | U.S. | EU |
| Total privacy spend | $733 | $284 |

## Median estimated privacy spend (000)^
(Base: Director or higher)

| | BY HQ LOCATION | |
|---|---|---|
| | U.S. | EU |
| Total privacy spend | $250 | $232 |

# Despite the pandemic, total privacy spend increased among the very largest firms since last year

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

### BY EMPLOYEE SIZE

| | <5K | | 5K–24.9K | | 25K–74.9K | | 75K+ | |
|---|---|---|---|---|---|---|---|---|
| | 2020 | 2019 | 2020 | 2019 | 2020 | 2019* | 2020 | 2019 |
| Total privacy spend (000) | $269 | $258 | $294 | $744 | $1,192 | $923 | $2,155 | $1,883 |

### BY COMPANY REVENUE

| | Under $100M | | $100M–$999M | | $1B–$24.9B | | $25B or more | |
|---|---|---|---|---|---|---|---|---|
| | 2020 | 2019* | 2020 | 2019* | 2020 | 2019 | 2020* | 2019* |
| Total privacy spend (000) | $343 | $357 | $213 | $254 | $815 | $1,038 | $1,850 | $1,556 |

* Small sample size

*^This question was changed in 2020 to ask only for total spending, versus last year when the question asked respondents for a breakdown of spending by category. Trend should be interpreted with caution.*

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

# Median privacy spend also shows higher spending at larger organizations

## Median estimated privacy spend (000)^
(Base: Director or higher)

### BY EMPLOYEE SIZE

| | <5K | 5K–24.9K | 25K–74.9K | 75K+* |
|---|---|---|---|---|
| Total privacy spend | $200 | $250 | $870 | $750 |

### BY COMPANY REVENUE

| | Under $100M* | $100M–$999M* | $1B–$24.9B | $25B or more* |
|---|---|---|---|---|
| Total privacy spend | $343 | $254 | $1,038 | $1,556 |

* Small sample size

# The median privacy budget tended to be lowest among less regulated and strictly B2C firms

## Median estimated privacy spend (000)^
(Base: Director or higher)

### BY INDUSTRY CATEGORY

| | Regulated | Unregulated | Gov't* |
|---|---|---|---|
| Total privacy spend | $750 | $250 | $854 |

### BY BUSINESS TYPE

| | B2B | B2C | Both |
|---|---|---|---|
| Total privacy spend | $300 | $200 | $300 |

* Small sample size

# As with average spend, the biggest median spending jump occurred among the largest firms

## Median estimated privacy spend (000)^
(Base: Director or higher)

### BY EMPLOYEE SIZE

| | <5K | | 5K–24.9K | | 25K–74.9K | | 75K+ | |
|---|---|---|---|---|---|---|---|---|
| | 2020 | 2019 | 2020 | 2019 | 2020 | 2019* | 2020* | 2019* |
| Total privacy spend | $200 | $150 | $250 | $400 | $870 | $403 | $750 | $506 |

### BY COMPANY REVENUE

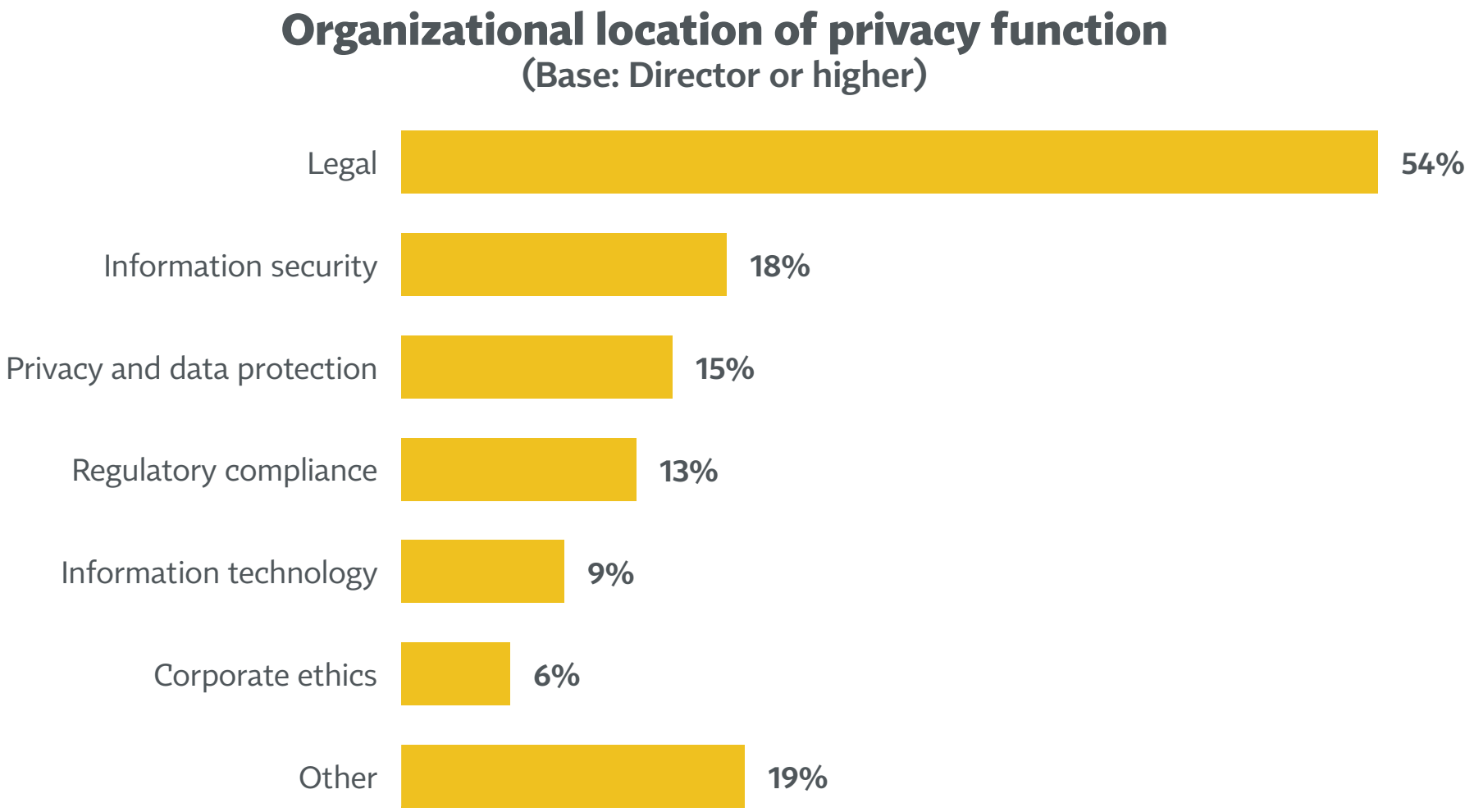
| | Under $100M | | $100M–$999M | | $1B–$24.9B | | $25B or more | |
|---|---|---|---|---|---|---|---|---|
| | 2020 | 2019* | 2020 | 2019* | 2020 | 2019 | 2020* | 2019* |
| Total privacy spend | $250 | $150 | $200 | $162 | $476 | $448 | $750 | $224 |

* Small sample size

*^This question was changed in 2020 to ask only for total spending, versus last year when the question asked respondents for a breakdown of spending by category. Trend should be interpreted with caution.*

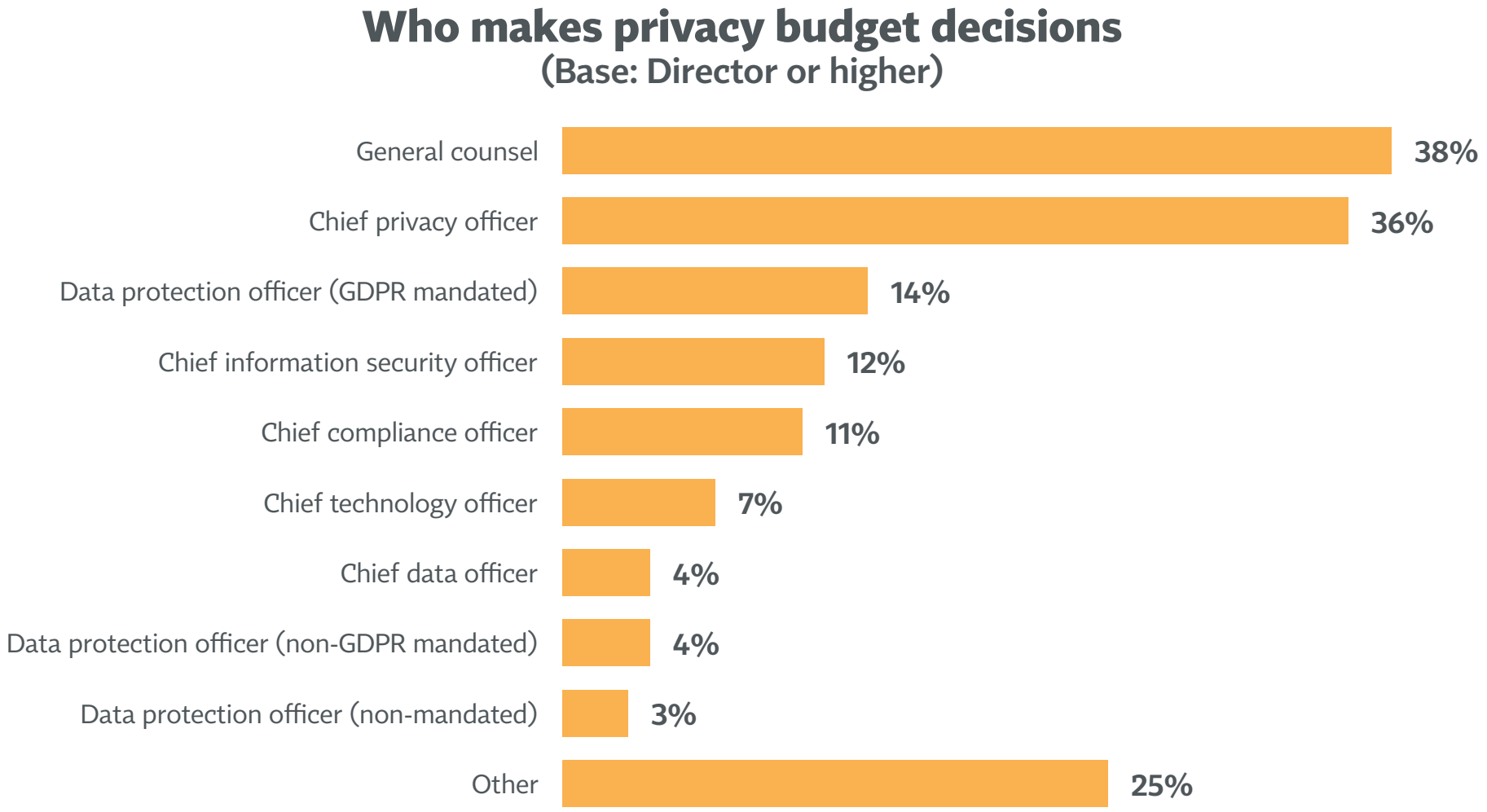
F4a: What was your organization's total privacy spend last year?

# Privacy teams are most often located within the legal department




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

# The general counsel or CPO most frequently make the privacy budget decisions

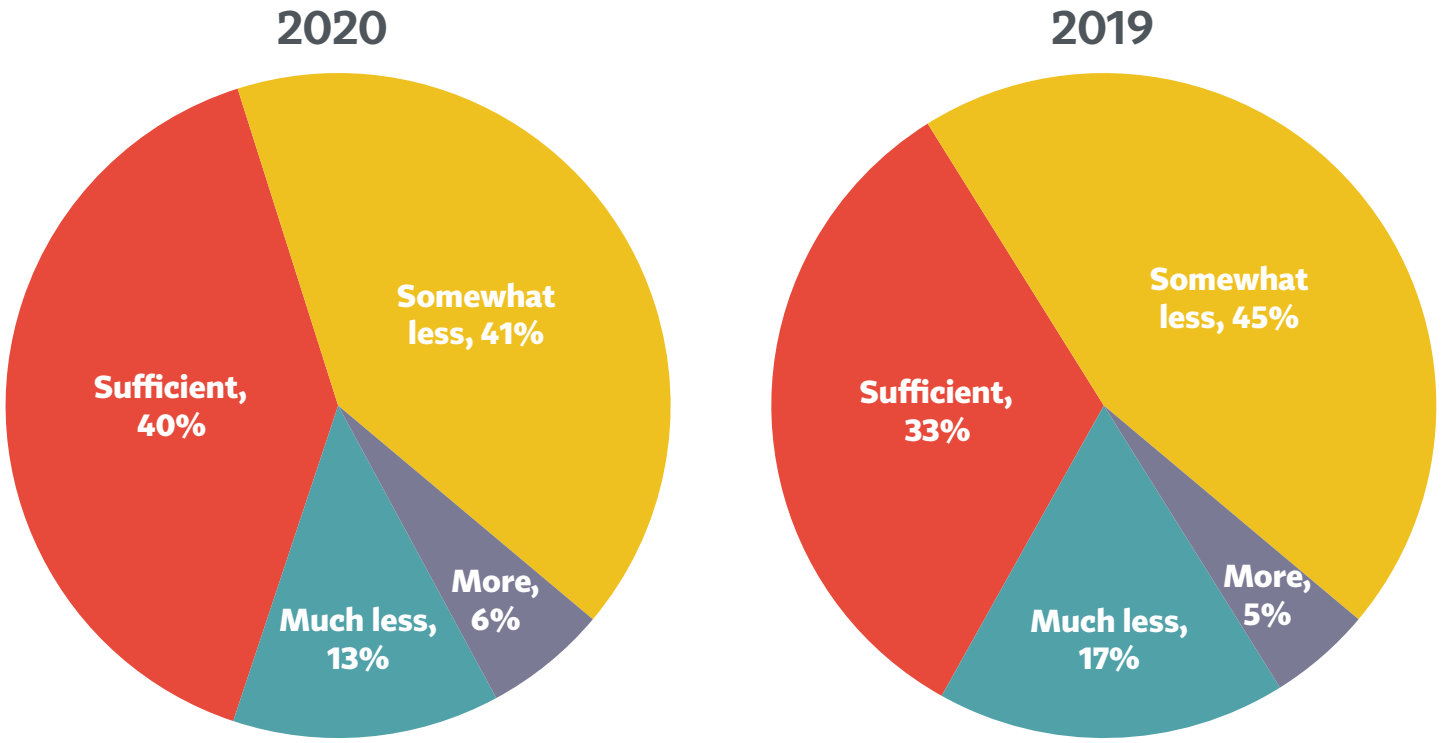



F3b: Who makes privacy budgeting/purchasing decisions at your organization?

# Better budgets: The proportion of privacy pros saying budgets are sufficient has increased in recent years

## How sufficient is privacy budget versus obligations?

(Base: Director or higher)

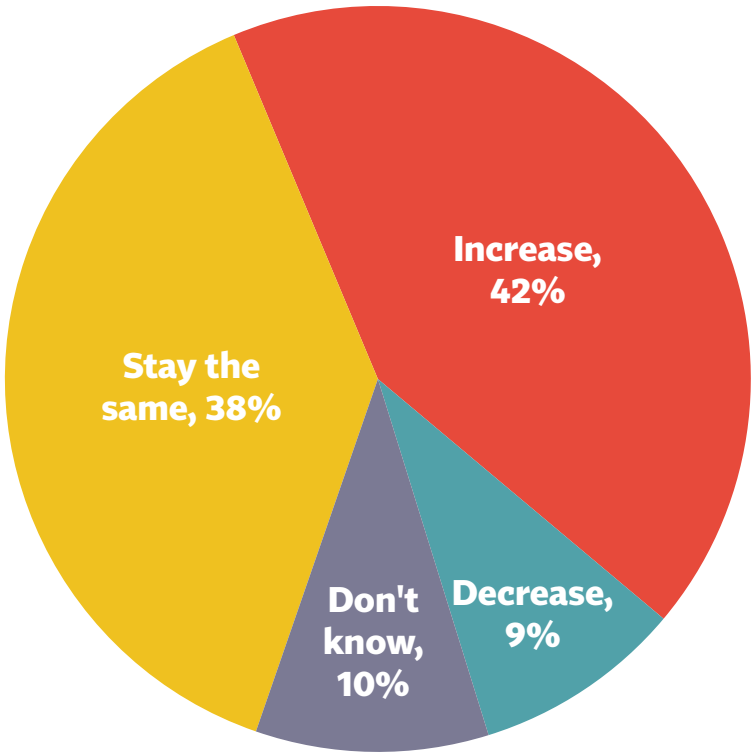



| TOTAL WHO SAY LESS THAN SUFFICIENT |
|---|
| 2020: 54% |
| 2019: 62% |
| 2018: 65% |

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

# Among those expecting a budget change, more believe they will see an increase than a decrease

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



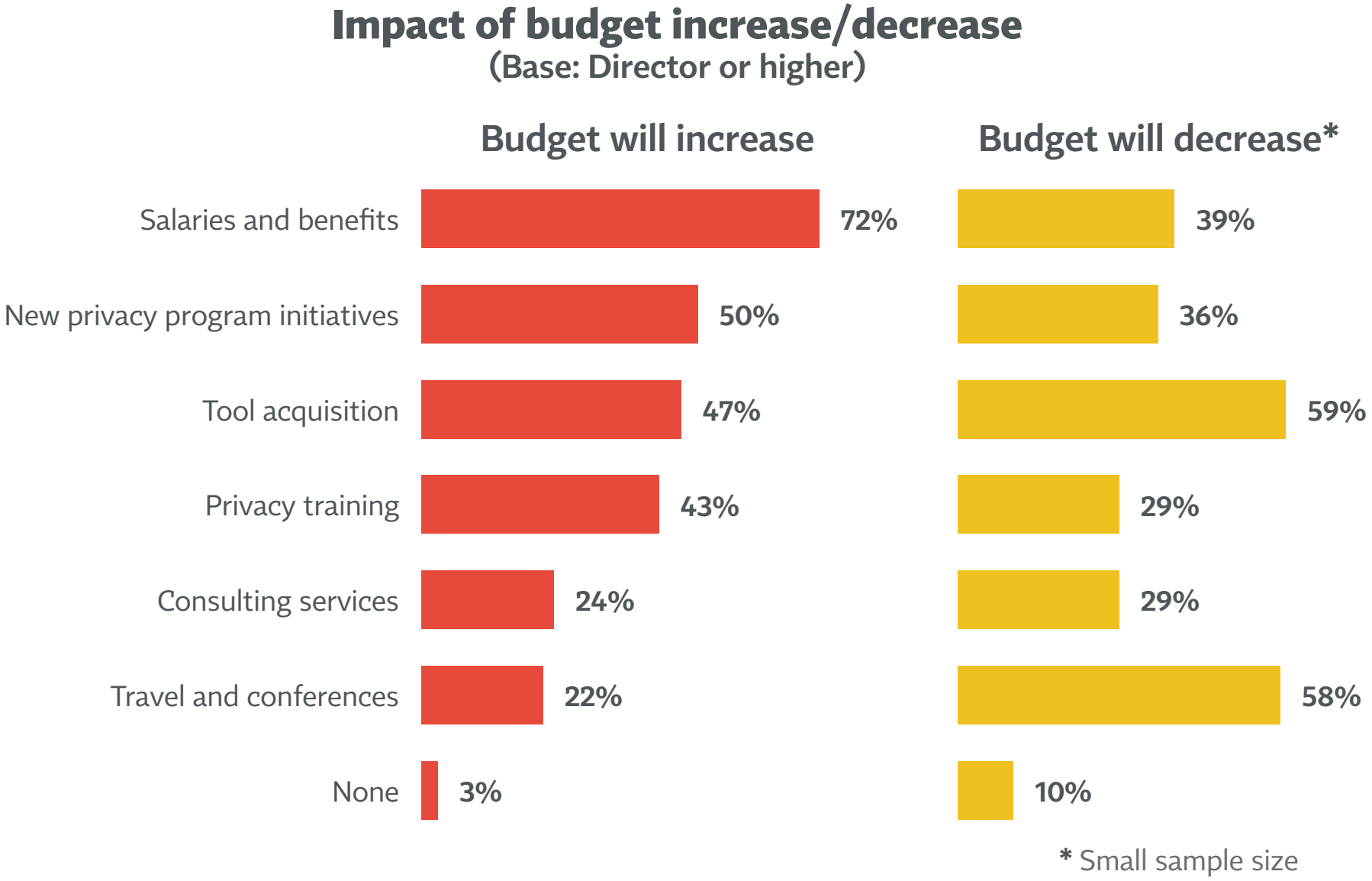

## % privacy budget increase/decrease
(Base: Director or higher)

| | Budget will increase | Budget will decrease* |
|---|---|---|
| Median % expected change | 15% | 25% |

* Small sample size

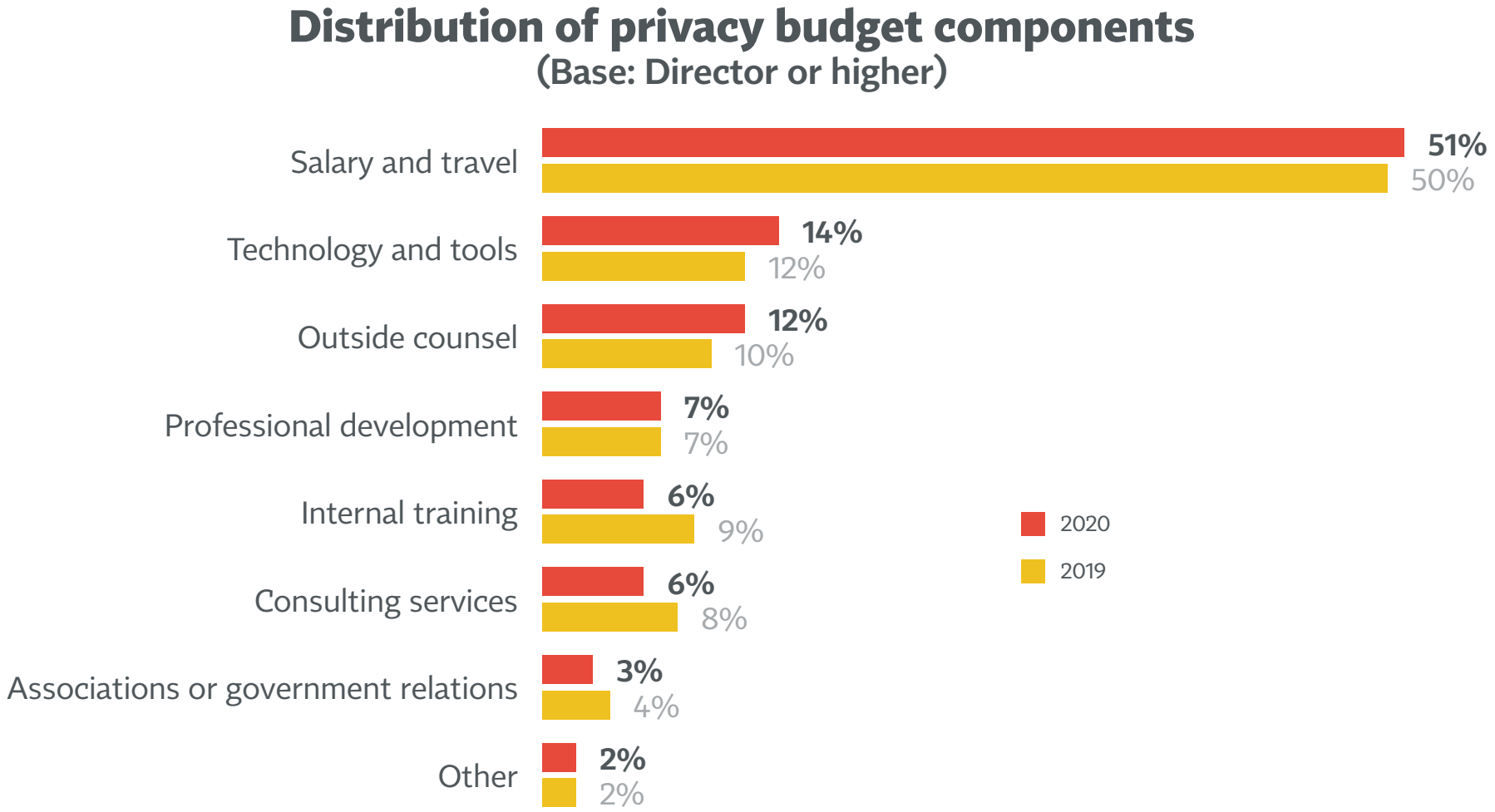
F5: In the next 12 months, you expect your company's privacy budget will …

# Those predicting a budget increase believe the boost will mostly impact salaries



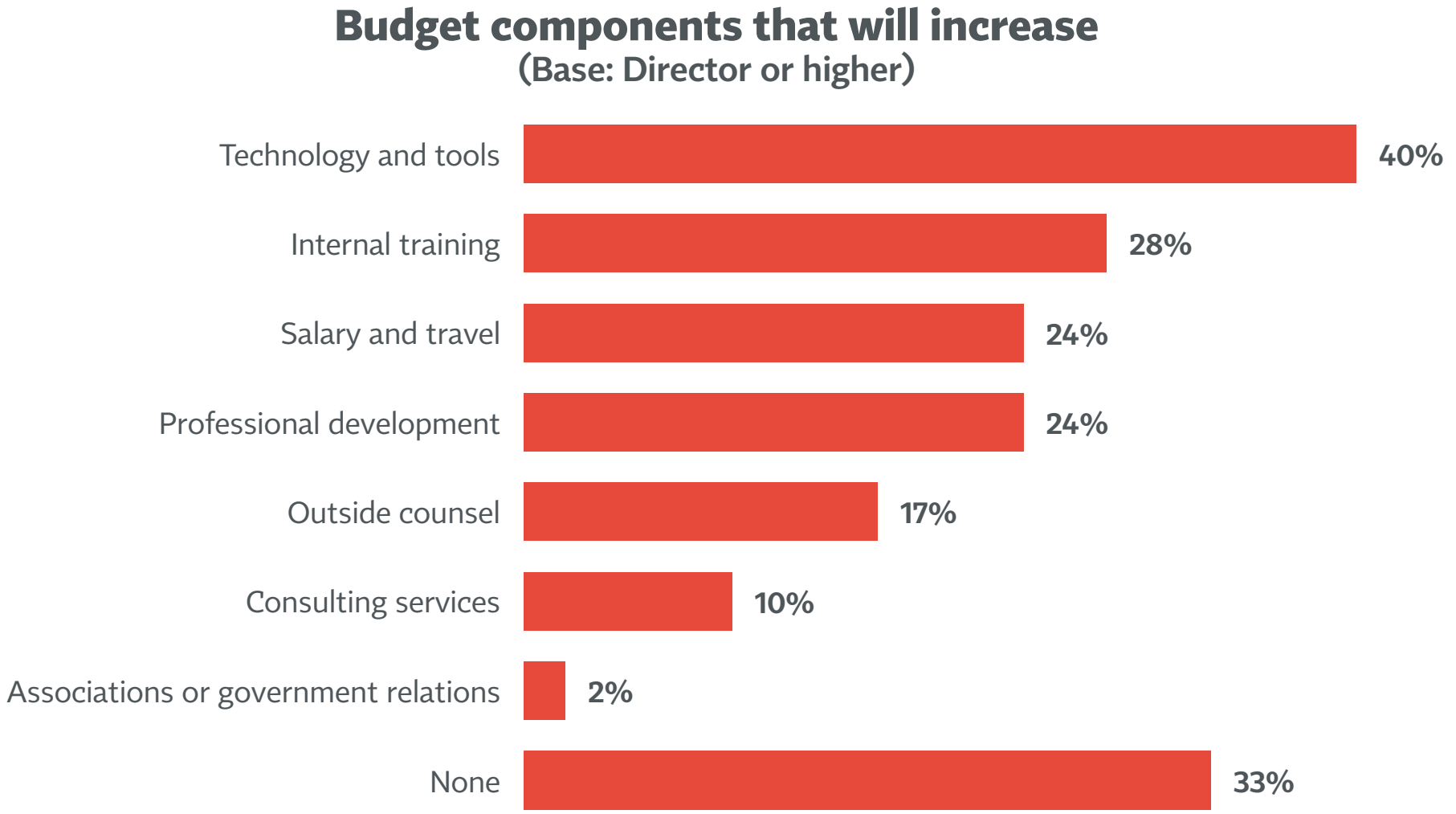

F5b: Will the change in spend affect any of the following?

# Little change since last year, however, in how privacy budget is spent, with salary and tech still the top items




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

# Privacy tech/tools are at top of the list of items expected to see more spending in the next 12 months




F3a: And in which areas to you plan to increase spending (if any) over the next 12 months?

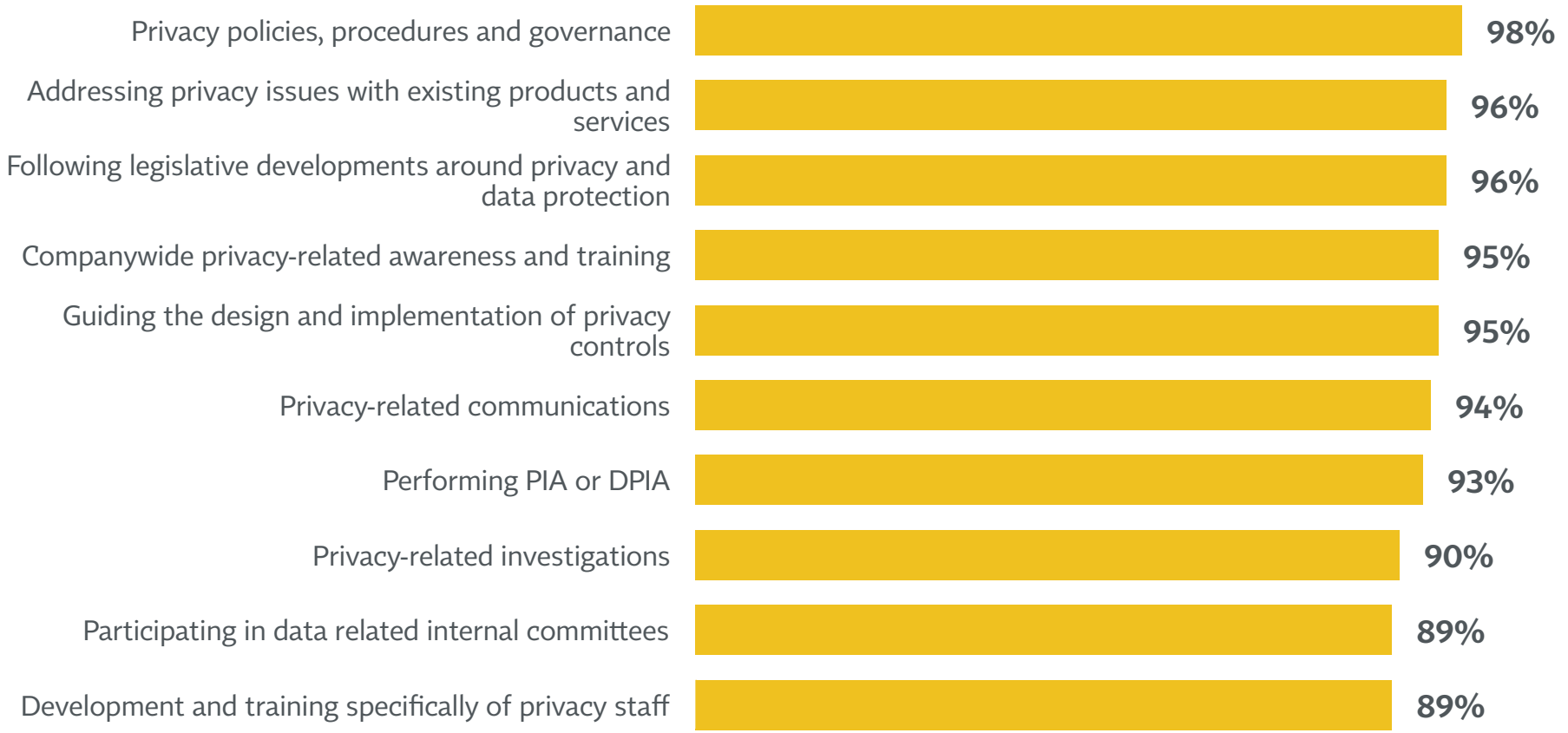
# Contents



# Privacy policies, privacy issues with products/services, and monitoring privacy laws are top responsibilities

## Privacy team responsibilities

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

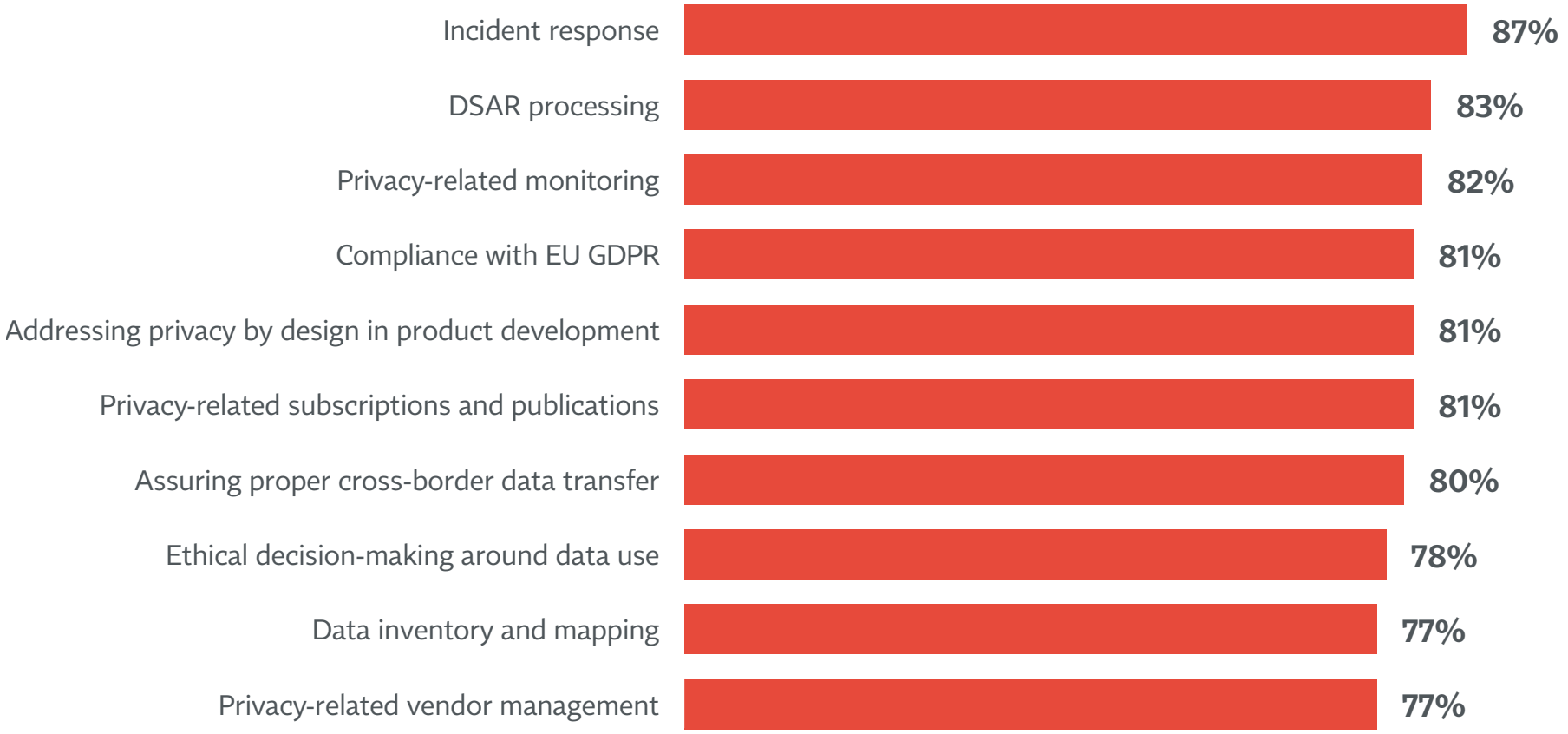



D4c/d: Which of the following are you, the privacy team or someone outside the privacy team responsible for accomplishing on an annual basis?

# Incident response, DSARs and GDPR compliance rank near the middle of the pyramid of responsibilities

## Privacy team responsibilities

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

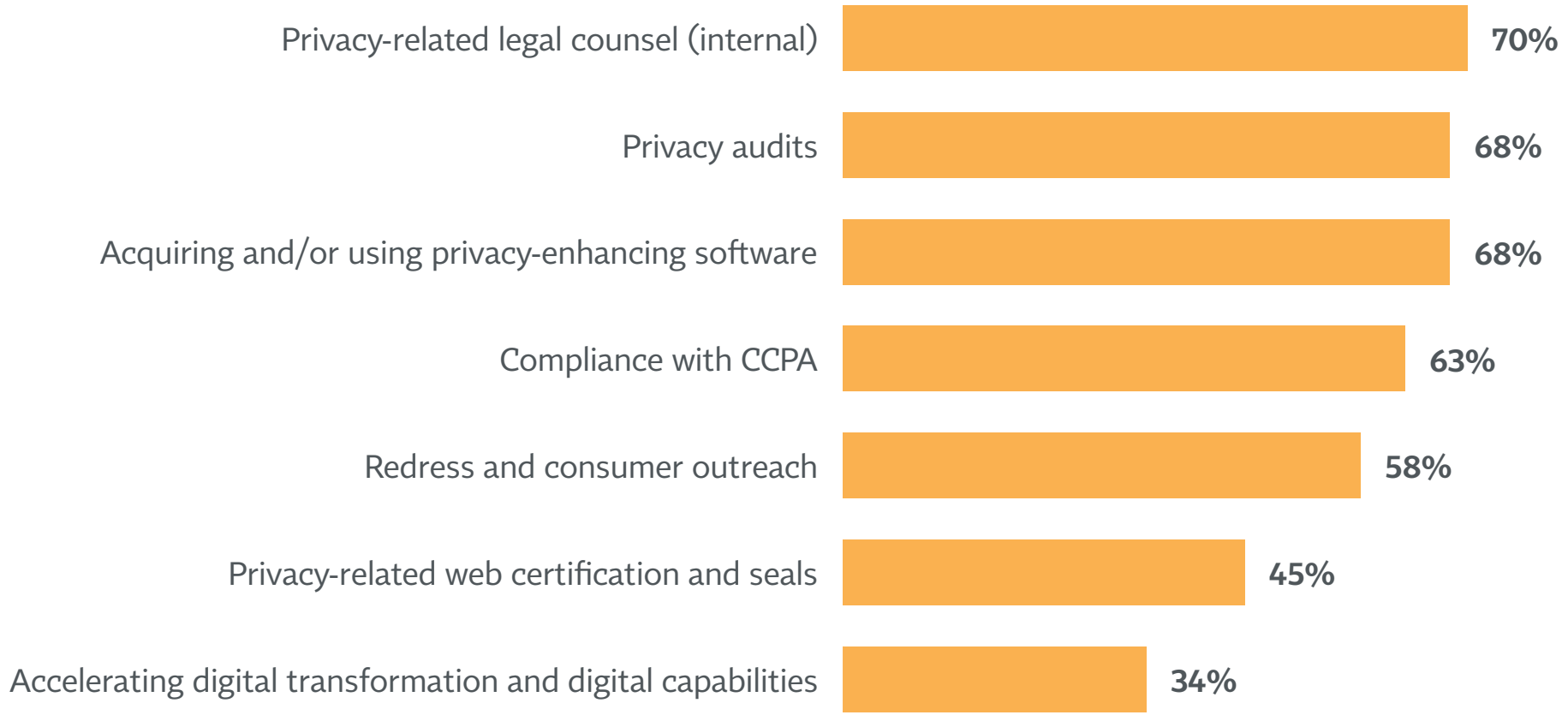



D4c/d: Which of the following are you, the privacy team or someone outside the privacy team responsible for accomplishing on an annual basis?

# Responsibilities regarding outreach, certification/seals, and digital transformation rank near the bottom

## 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, the privacy team or someone outside the privacy team responsible for accomplishing on an annual basis?

# Privacy-related monitoring, GDPR and cross-border data transfers are more pressing for EU privacy pros

## BY RESPONDENT LOCATION

| | U.S. | EU |
|---|---|---|
| **Privacy responsibilities** | | |
| Privacy-related monitoring | 80% | **91%** |
| Compliance with EU GDPR | 76% | **99%** |
| Assuring proper cross-border data transfer | 74% | **89%** |
| Ethical decision-making around data use | **84%** | 70% |
| Compliance with CCPA | **84%** | 41% |

Significantly different than other segments

# Firms with higher revenues tend to be responsible for more tasks, such as CCPA compliance

## BY COMPANY REVENUE

| | Under $100M | $100M–$999M | $1B–$24.9B | $25B+* |
|---|---|---|---|---|
| **Privacy responsibilities** | | | | |
| Compliance with EU GDPR | **68%** | 90% | 86% | 92% |
| Assuring proper cross-border data transfer | **69%** | 81% | 86% | 88% |
| Ethical decision-making around data use | **67%** | 84% | 86% | 78% |
| Acquiring and/or using privacy-enhancing software | **55%** | 75% | 76% | 75% |
| Compliance with CCPA | **45%** | 60% | **76%** | **90%** |

Significantly different than other segments

* Small sample size

# Respondents with DPO titles tend to differ from others in the range of their personal responsibilities

## BY JOB TITLE

| | CPO | Privacy officer | DPO | Lead privacy counsel | Director of privacy |
|---|---|---|---|---|---|
| **Privacy responsibilities that respondent is responsible for** | | | | | |
| Guiding the design and implementation of privacy controls | 83% | 75% | 75% | 83% | **97%** |
| Participating in data related internal committees | **89%** | 74% | 76% | 85% | 75% |
| Privacy-related communications | 85% | 85% | **83%** | 82% | 82% |
| Development and training specifically of privacy staff | 78% | 75% | 76% | **94%** | 70% |
| Compliance with EU GDPR | 67% | 57% | **82%** | **88%** | 82% |
| Privacy-related investigations | 75% | 73% | **78%** | 77% | 73% |
| Privacy-related subscriptions and publications | 64% | 70% | **72%** | 71% | 75% |

Significantly different than other segments

*Note: Only titles with sample sizes over 20 are shown.*

# DPO respondents are, not surprisingly, more likely to be involved in data-related tasks than others

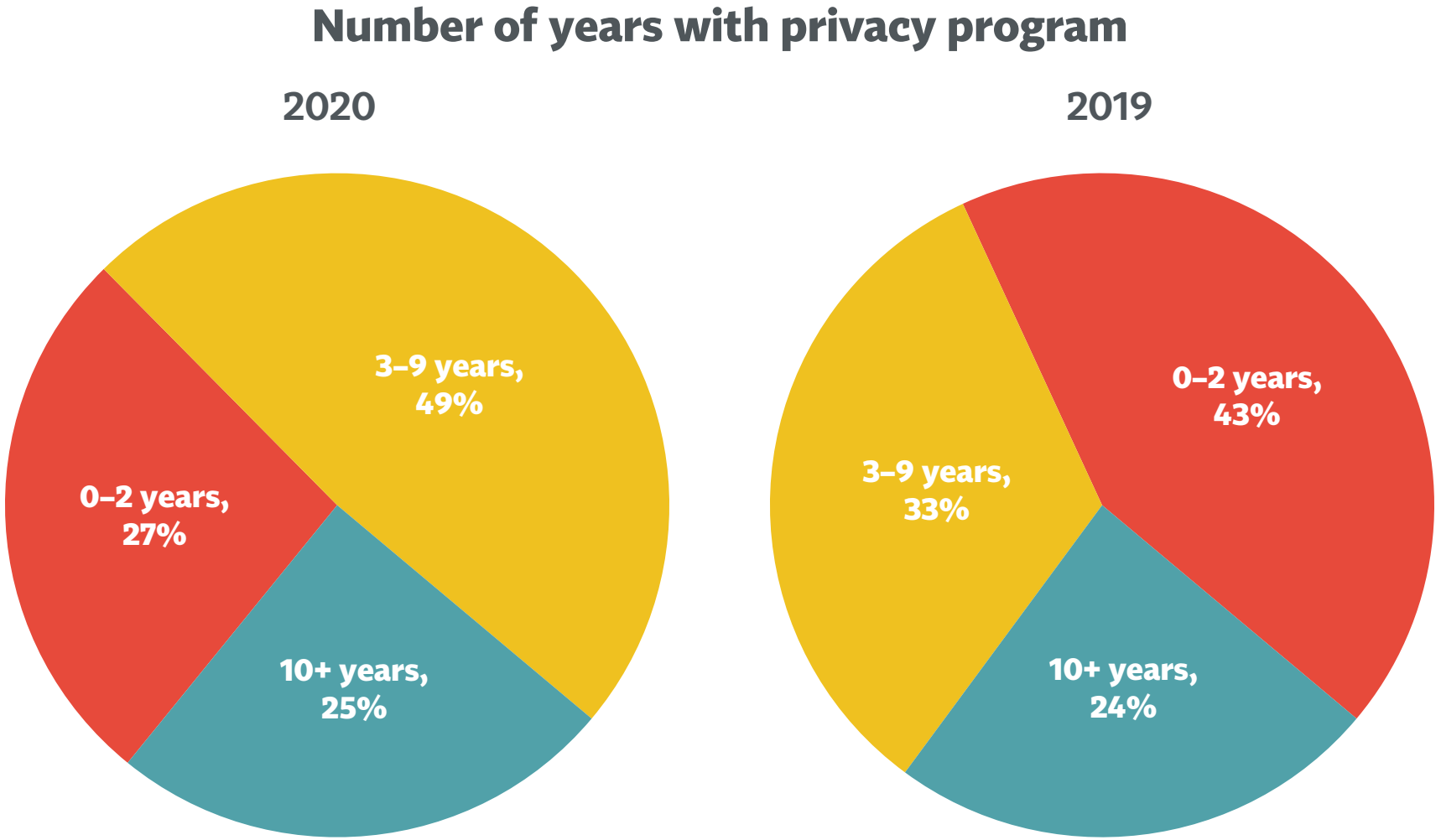
## BY JOB TITLE (cont'd.)

| | CPO | Privacy officer | DPO | Lead privacy counsel | Director of privacy |
|---|---|---|---|---|---|
| **Privacy responsibilities that respondent is responsible for** | | | | | |
| Ethical decision-making around data use | 71% | 49% | 55% | **82%** | **87%** |
| Privacy-related monitoring | 50% | 70% | **72%** | 61% | 75% |
| Assuring proper cross-border data transfer | 60% | 59% | **67%** | **86%** | 68% |
| Data inventory and mapping | 45% | 46% | **69%** | 66% | 63% |
| DSAR processing | 39% | 48% | **67%** | 55% | 64% |
| Compliance with CCPA | 50% | 44% | **29%** | 69% | 62% |
| Privacy audits | 44% | 49% | **59%** | 37% | 62% |
| Privacy-related legal counsel (internal) | **67%** | 27% | 51% | **94%** | 32% |

Significantly different than other segments

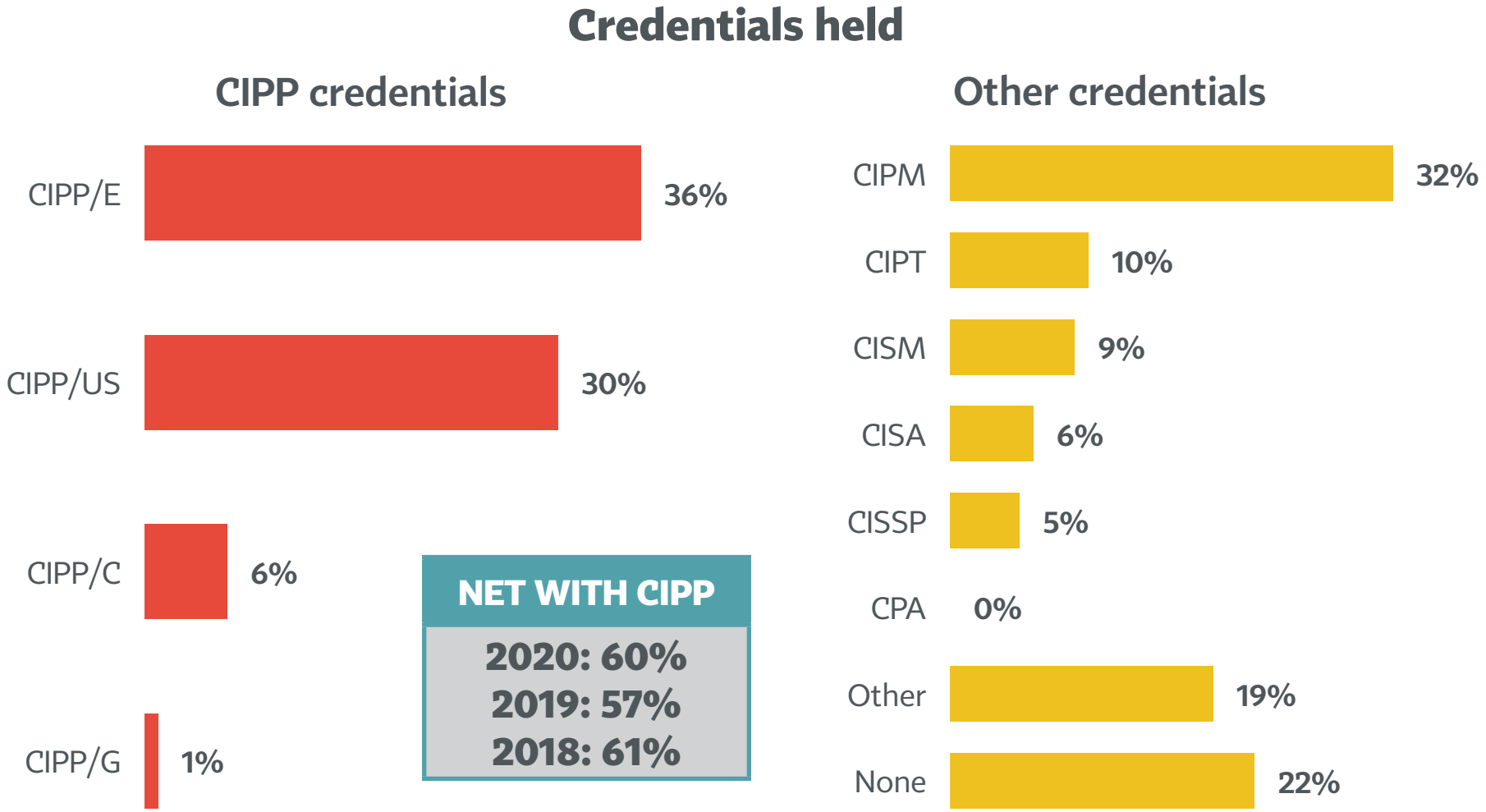
*Note: Only titles with sample sizes over 20 are shown.*

# Compared to 2019, respondents in 2020 are more likely to have had a privacy program at their firms for 3 to 9 years




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

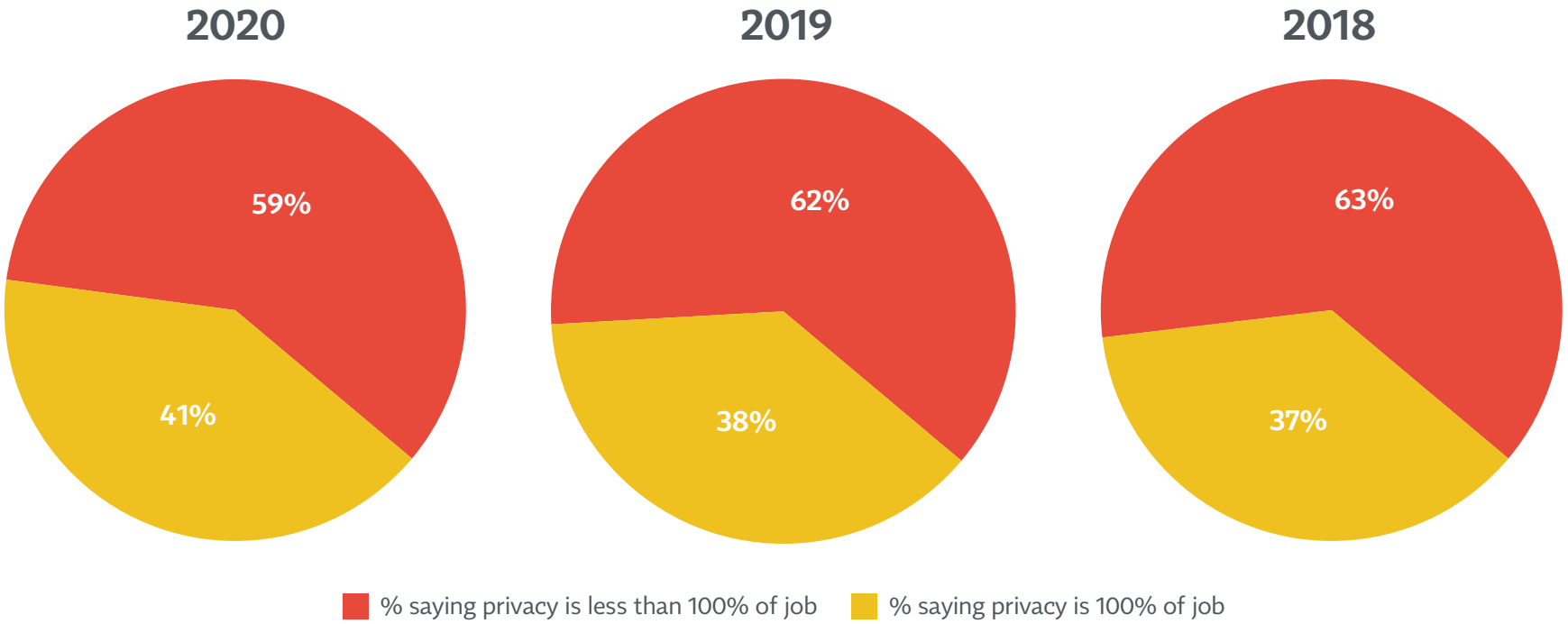
# CIPP/E is the most popular credential, followed by CIPM and CIPP/US




I10: Which certifications do you hold?

# Privacy pros spent 73% of their time on average working on privacy

## Privacy as % of job
(Base: Director or higher)




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

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

# Privacy pros at the largest firms spent more of their time on privacy

## BY EMPLOYEE SIZE

| | <5K | 5K–24.9K | 25K–74.9K | 75K+* |
|---|---|---|---|---|
| **Mean** % of time spent on privacy | **61%** | **84%** | 81% | 77% |

## BY COMPANY REVENUE

| | Under $100M | $100M–$999M | $1B–$24.9B | $25B+* |
|---|---|---|---|---|
| **Mean** % of time spent on privacy | 64% | 70% | **83%** | 79% |

## BY COMPANY REVENUE

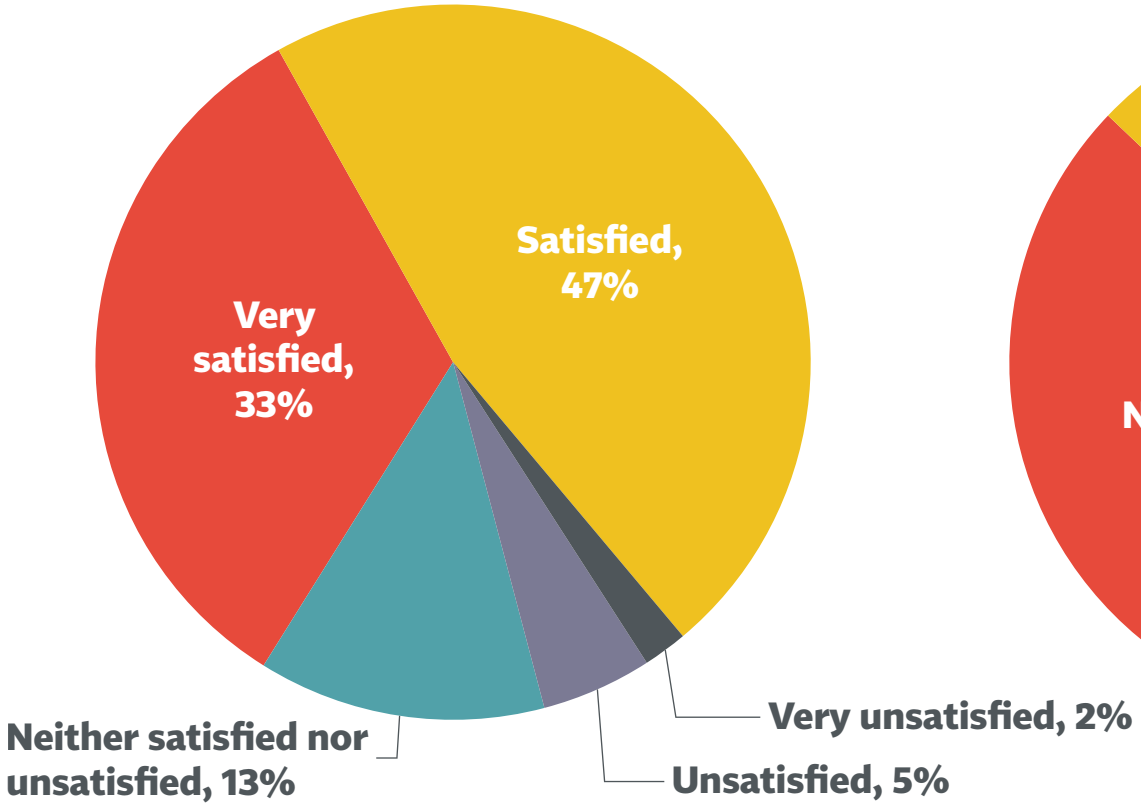
| | Under $100M | $100M–$999M | $1B–$24.9B | $25B+* |
|---|---|---|---|---|
| **Median** % of time spent on privacy | 70% | 80% | 100% | 100% |

Significantly different than other segments

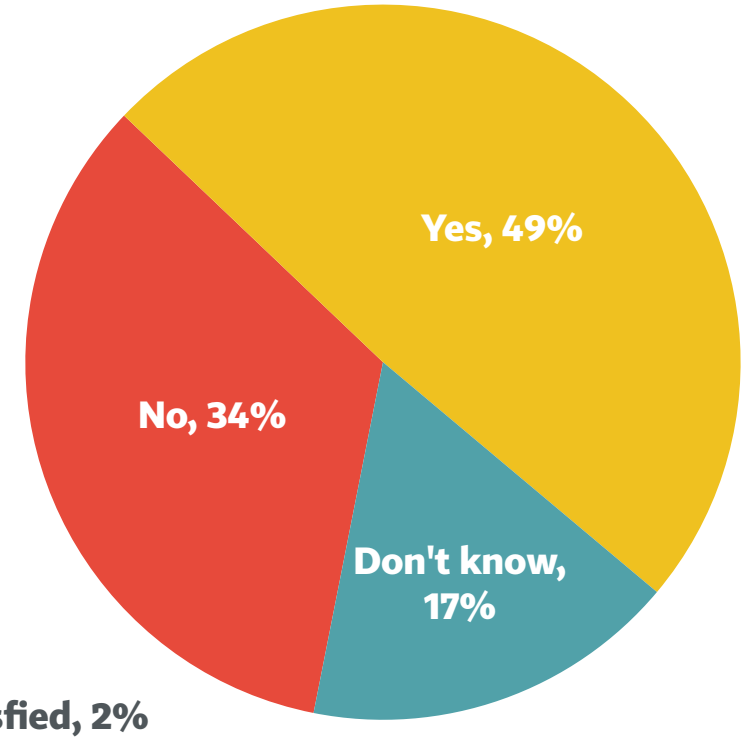
* Small sample size

# 8 in 10 privacy pros are satisfied or very satisfied with their job, and half see an upward career path

## Satisfaction with job?




## Expect upward career path?



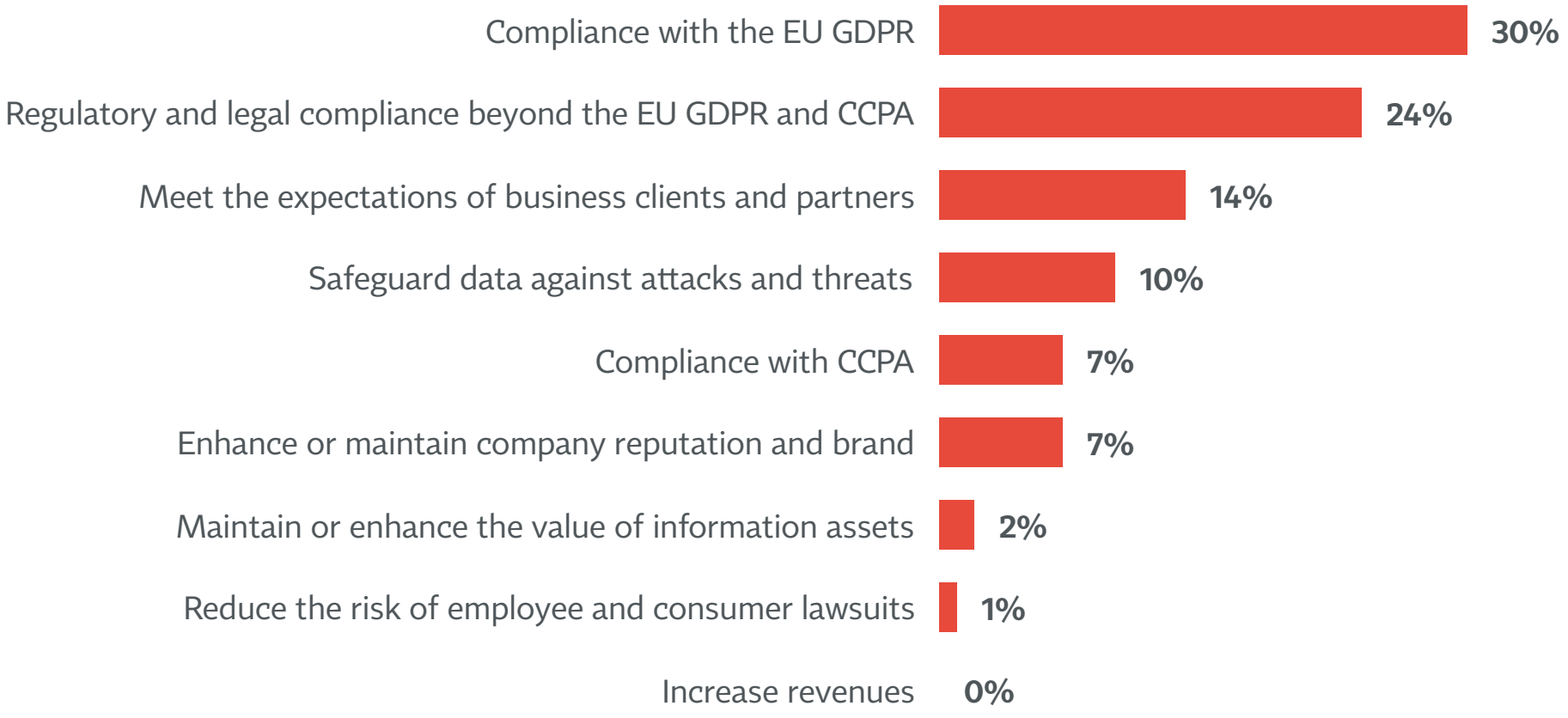

I13: How satisfied are you with your job?
I14: Are you expecting an upwards career trajectory (for example, do you see a track for promotion)?

# Contents



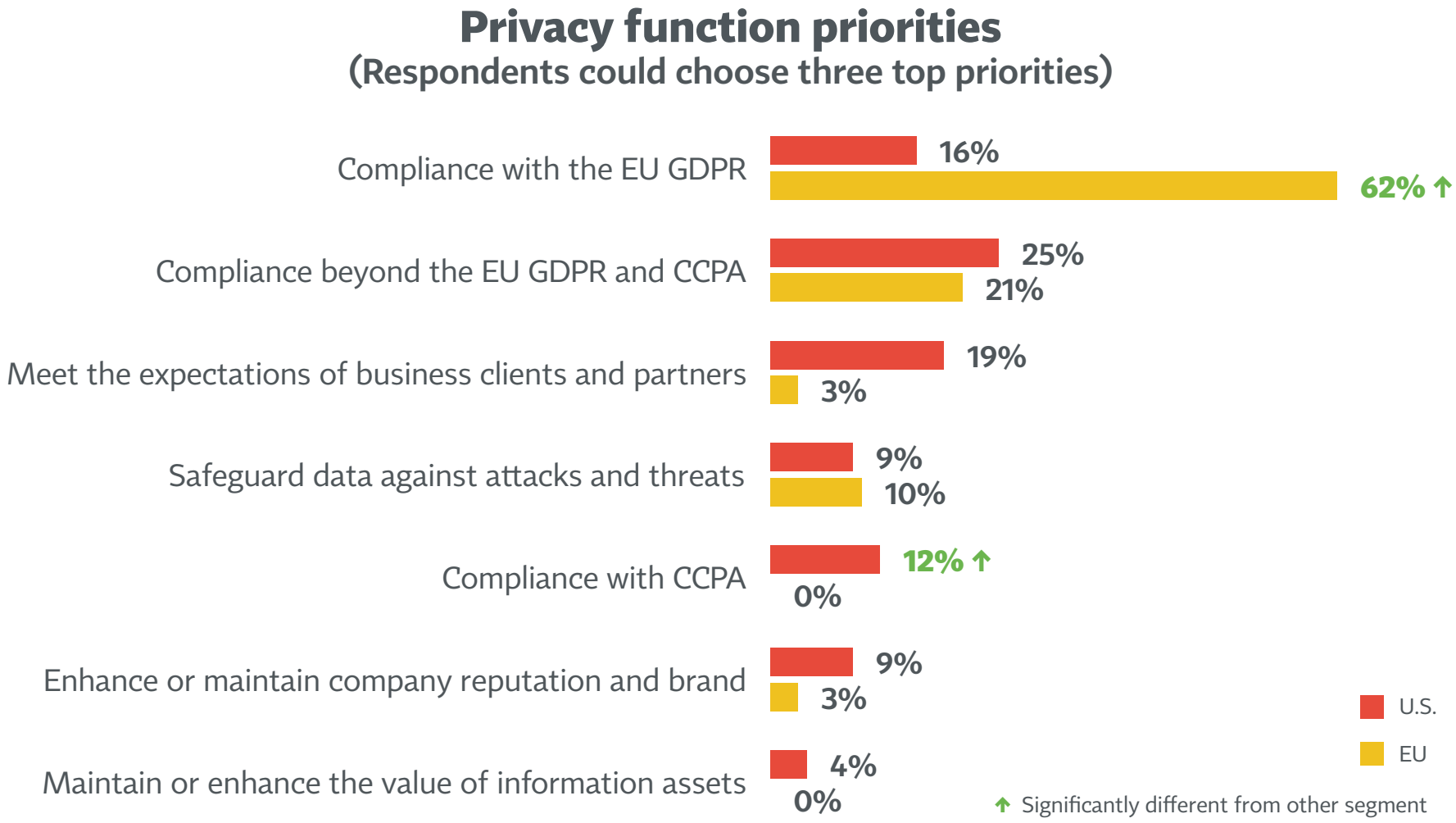
# Compliance issues — GDPR, CCPA and beyond — top the list of privacy priorities

## Privacy function priorities
### (Respondents could choose three top priorities)



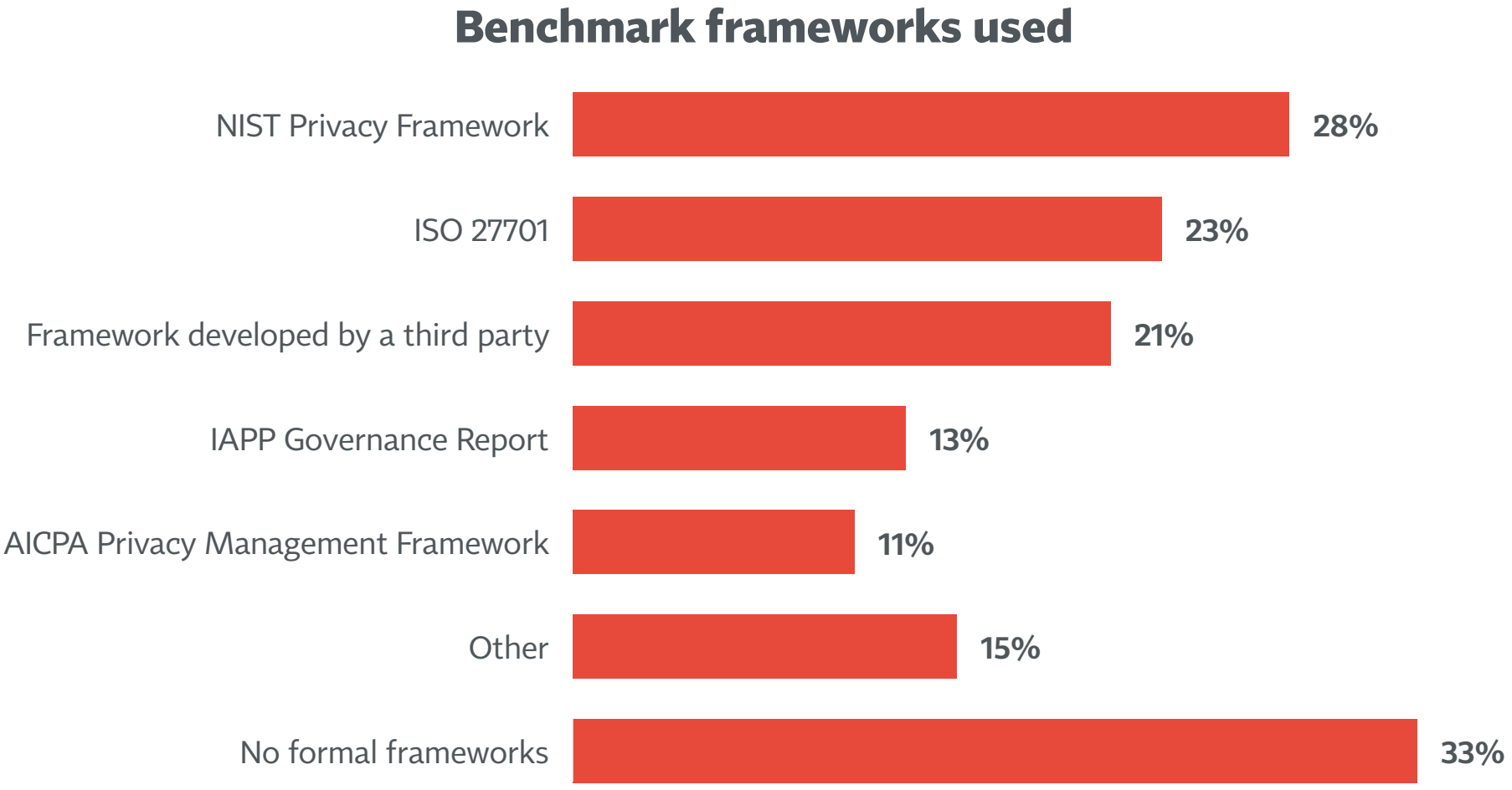

E3: Which of the following is the highest priority within your privacy program?

# While CCPA is more of a priority in the U.S., GDPR remains a much higher priority in the EU



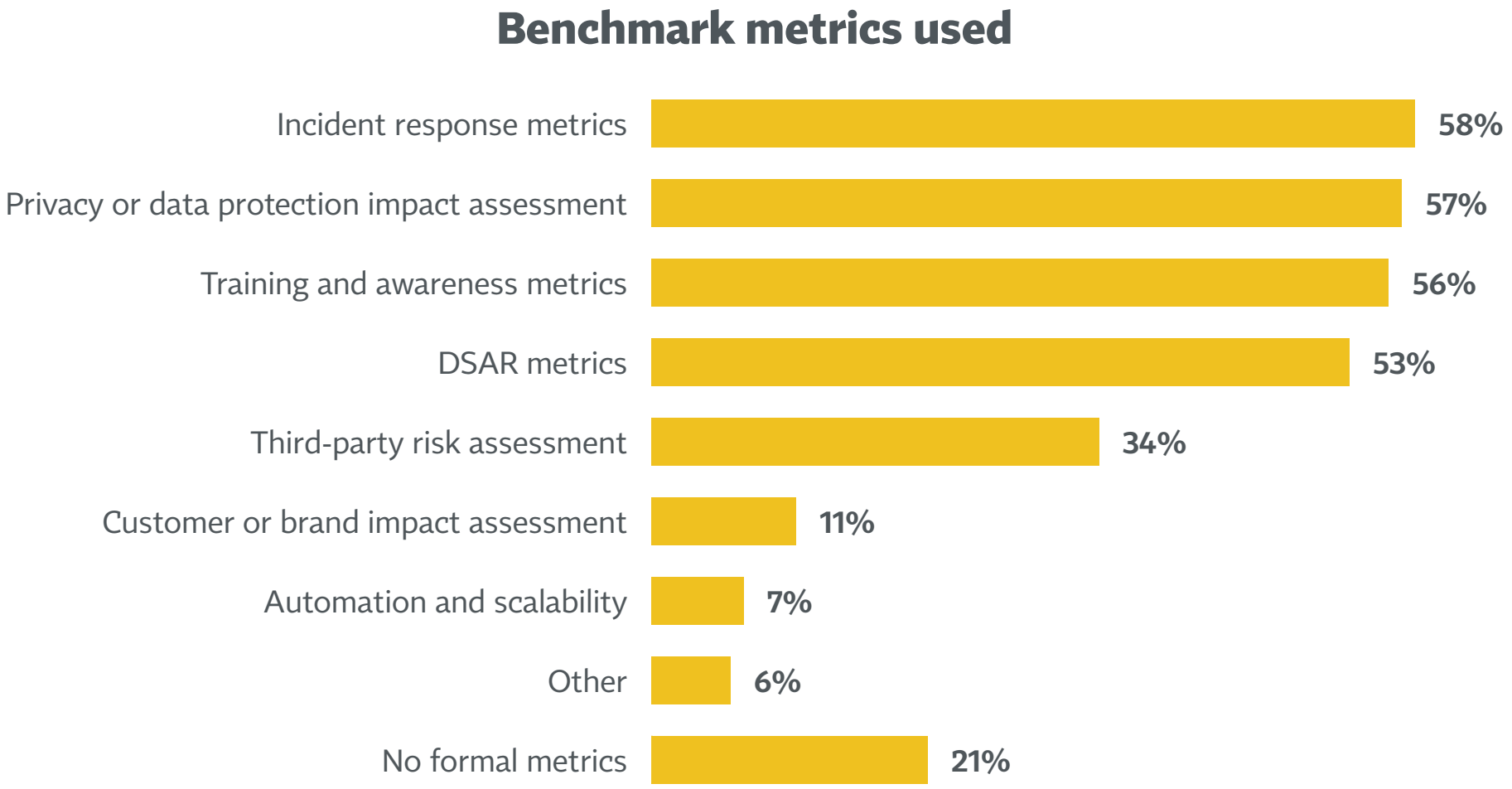

E3: Which of the following is the highest priority within your privacy program?

# NIST, ISO 27701 and third-party frameworks are the most commonly used program benchmarks




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

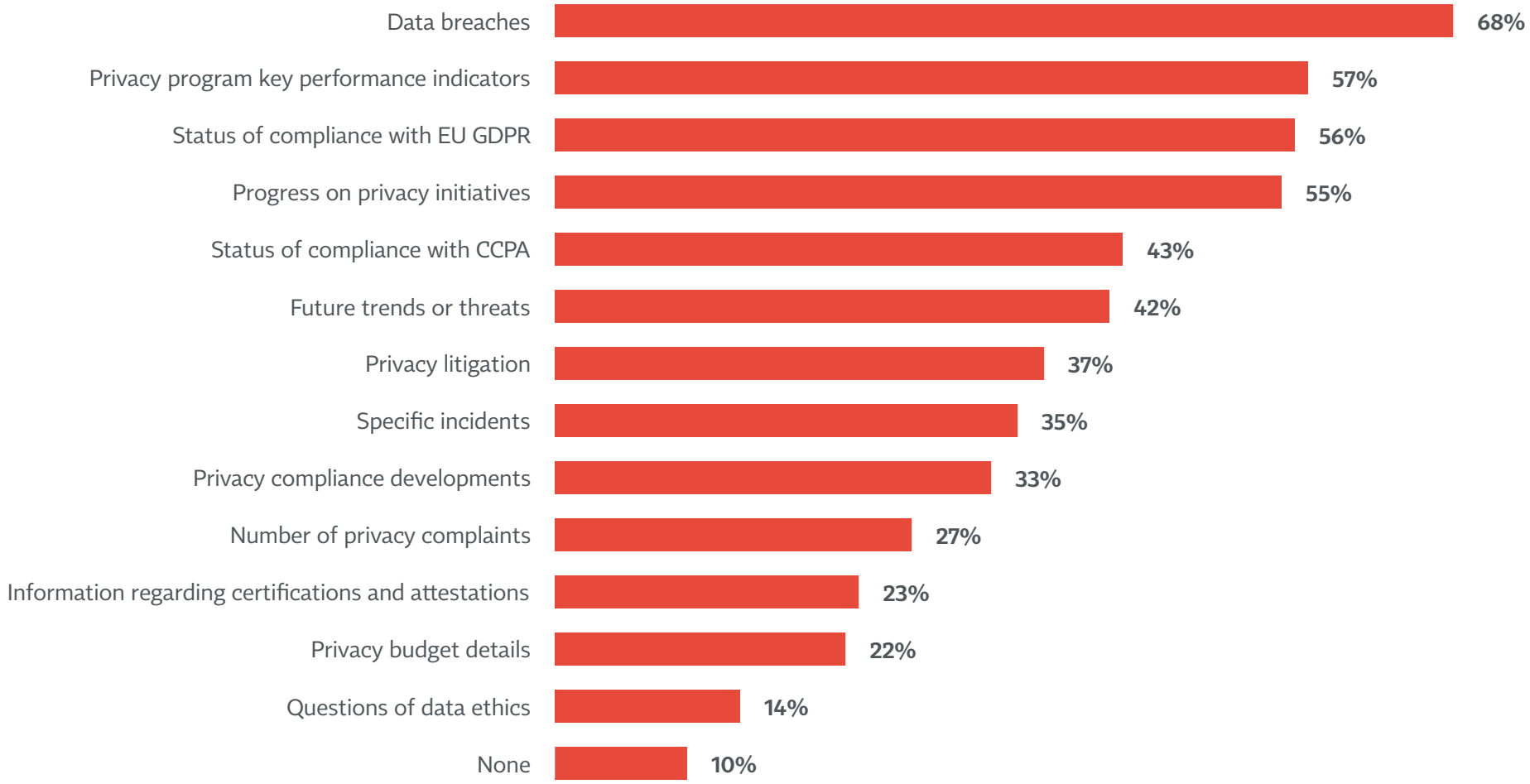
# Incident response, impact assessment and training/awareness are the top performance metrics




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

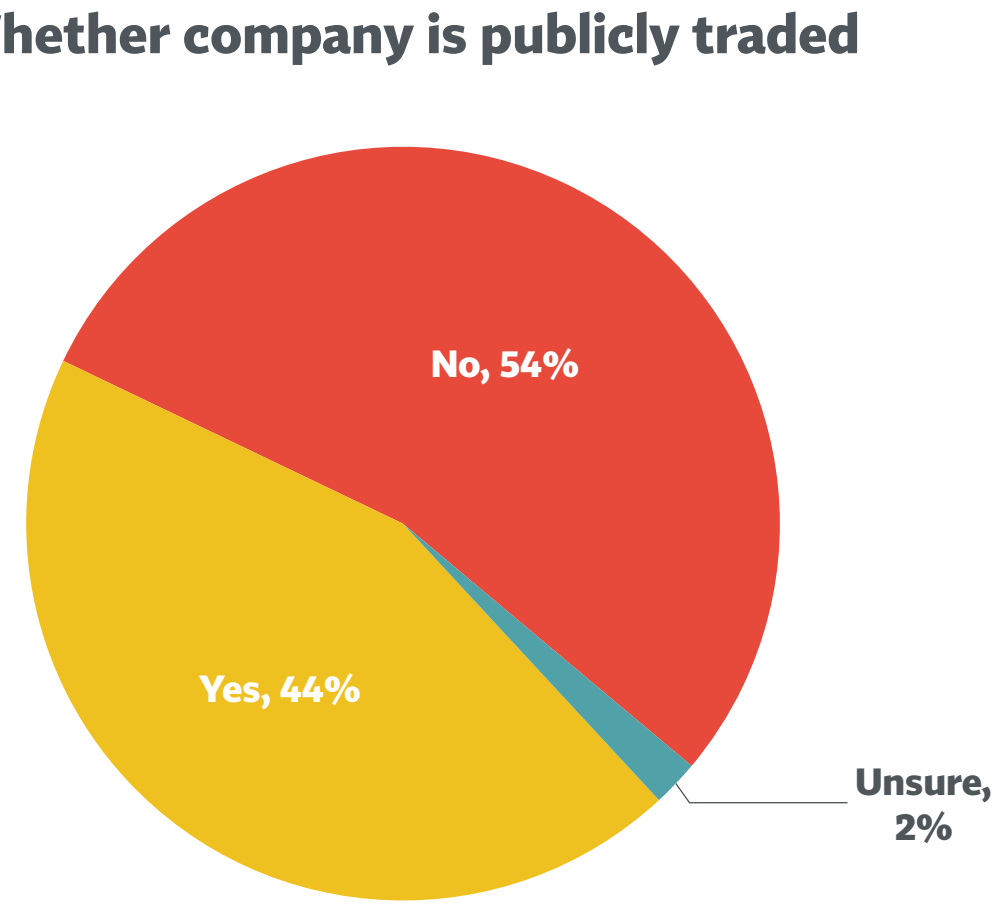
# Data breaches, privacy key performance indicators and GDPR compliance are the most common topics reported to the board

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




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

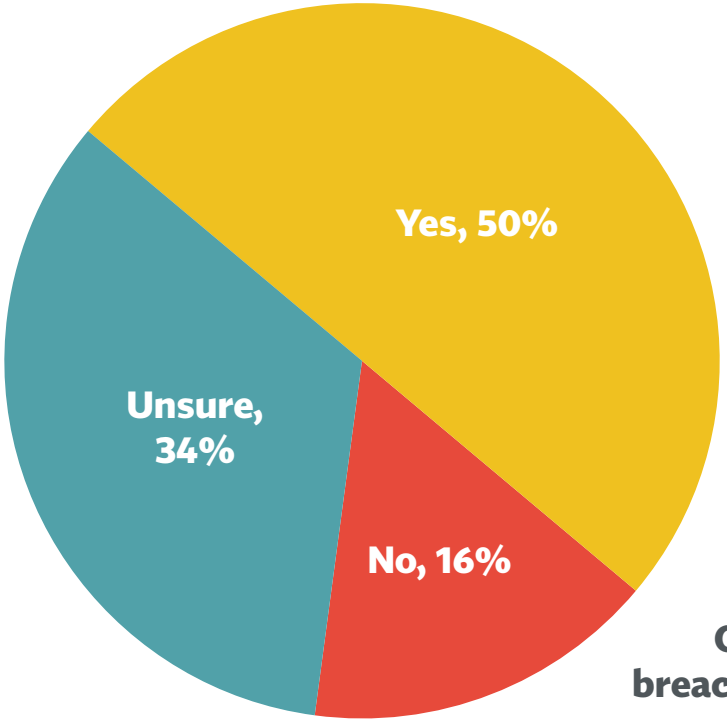
# Almost half of respondents work for a publicly traded firm



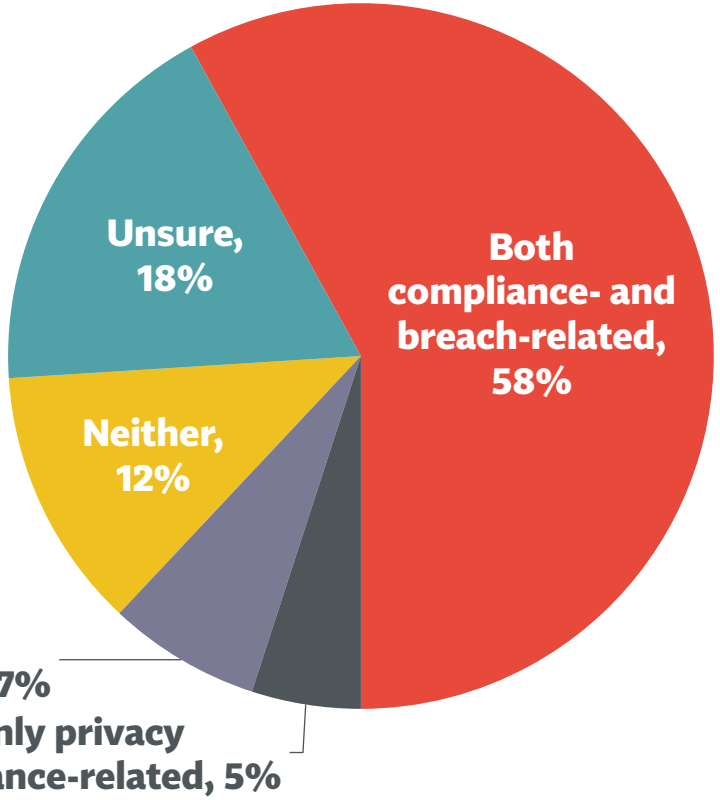

F44: Are shares of your company publicly traded on a stock exchange, such as but not limited to the New York Stock Exchange, Hong Kong Stock Exchange or London Stock Exchange?

# Half of those in public firms said privacy risks are included in annual reports and other communications

## Privacy risks communicated
(Base: Publicly traded)




## What is communicated
(Base: Privacy items disclosed)

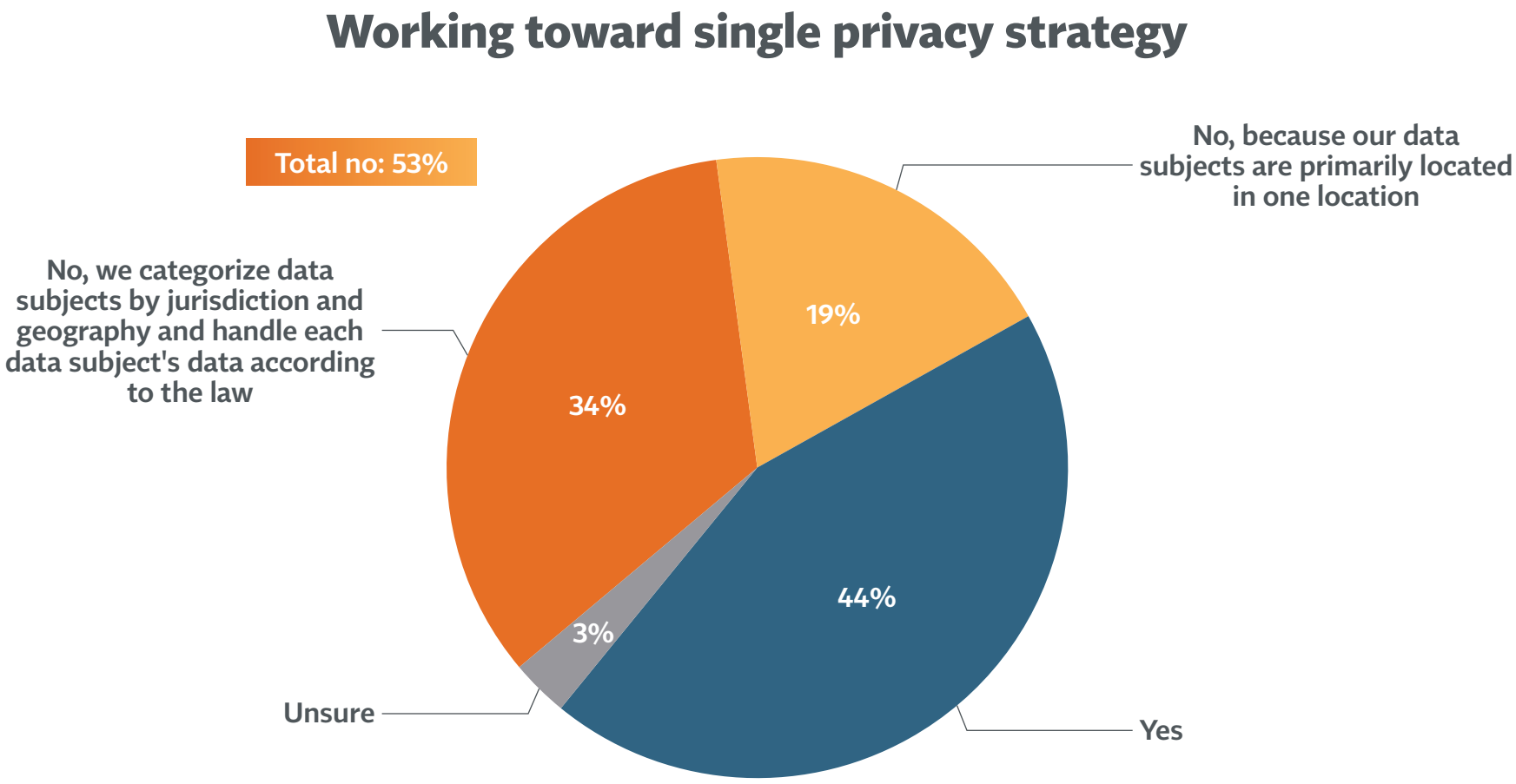



F45: Are your organization's privacy-related risks included in any financial notices, disclosures, shareholder communications or annual reports?
F46: Do these financial notices, disclosures, shareholder communications or annual report mention data breach–related risks or privacy compliance–related risks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

# Contents

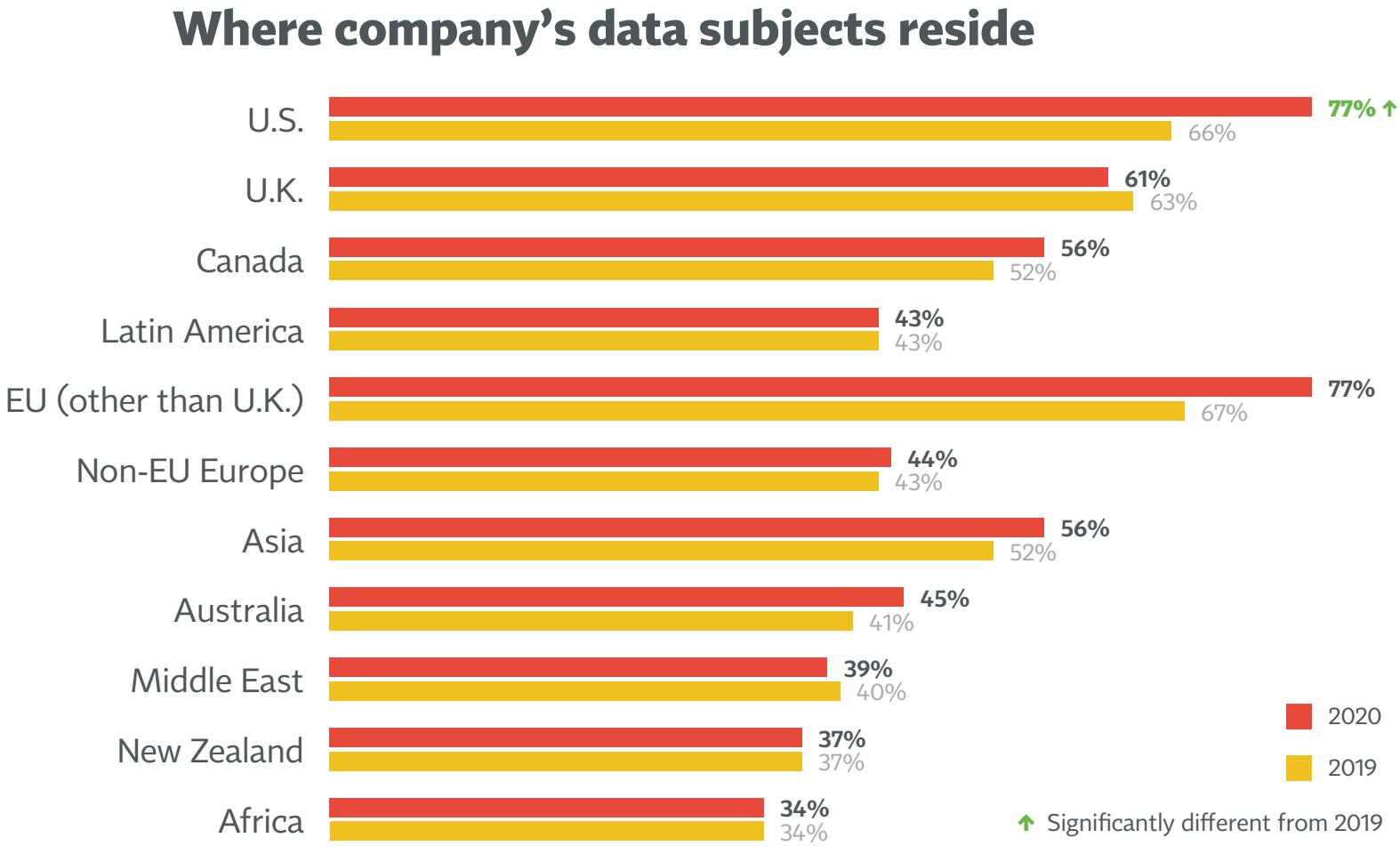


# 4 in 10 are working toward a single global privacy strategy; one-third prefer region-based strategies



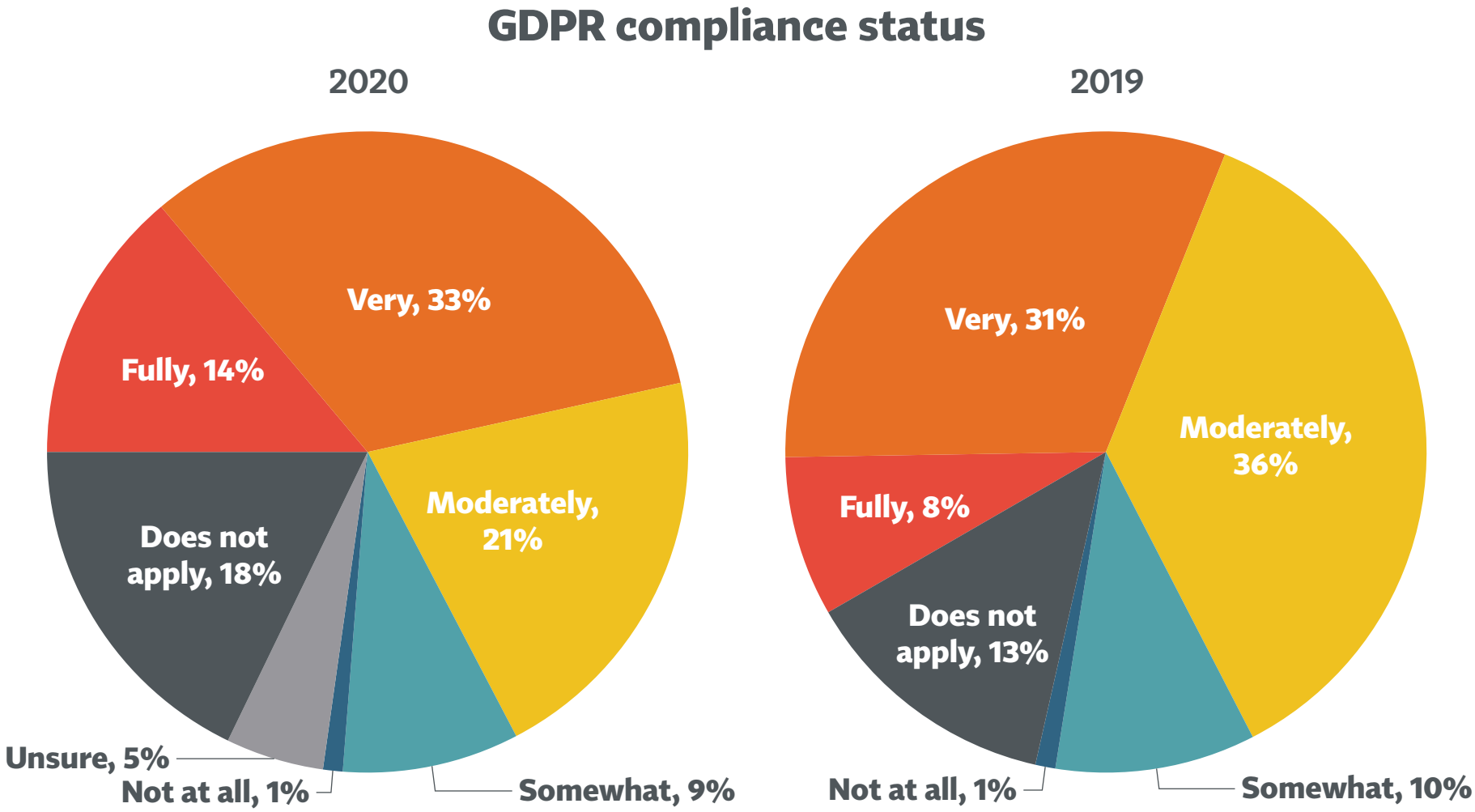

D5: Is your organization working toward a single global data protection/privacy strategy for data subjects' rights?

# Significantly more companies this year have data subjects residing in the U.S. compared to the year prior




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

# GDPR compliance is up: 47% said they are fully or very compliant versus 39% last year




J18: How would you rate your organization's current level of EU General Data Protection Regulation compliance?

# More EU companies are very/fully compliant with GDPR than U.S. ones, although not all U.S. businesses are subject to it

**BY HQ LOCATION**

| | U.S. | EU |
|---|---|---|
| **Level of GDPR compliance** | | |
| Fully compliant | 16% | 12% |
| Very compliant | 29% | **45%** |
| Moderately compliant | 19% | 27% |
| Somewhat compliant | 6% | 15% |
| Not at all compliant | 1% | 0% |
| GDPR doesn't apply | **23%** | 0% |

Significantly different than other segment

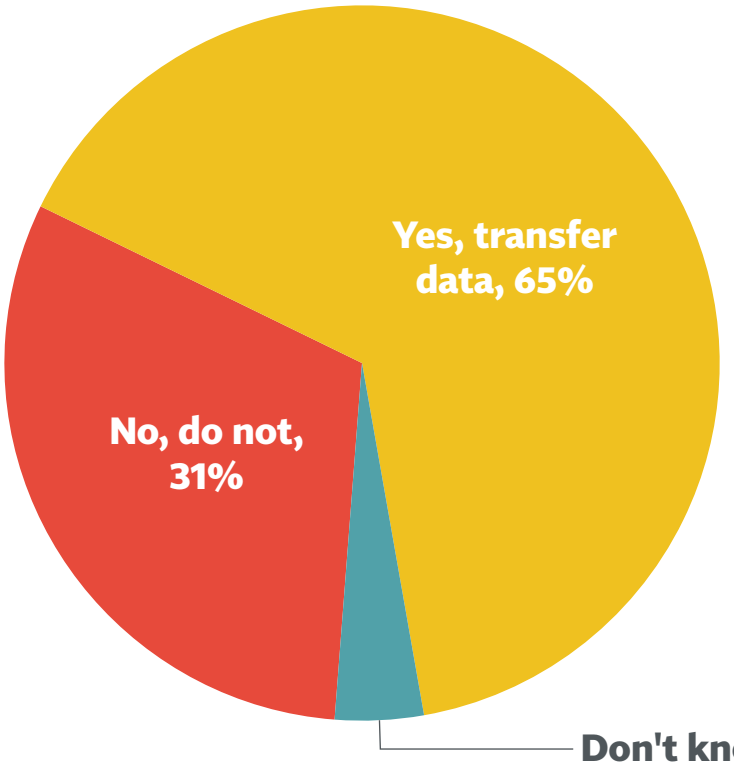
**NET "FULLY/VERY" COMPLIENT**

**U.S.: 45%**
**EU: 57%**

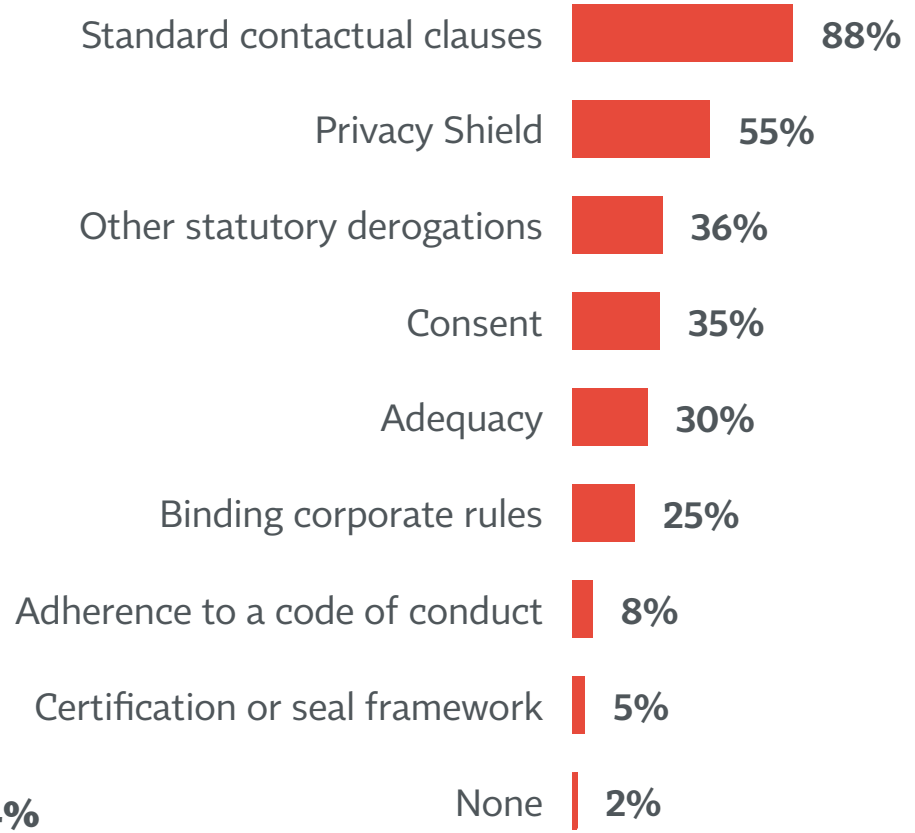
J18: How would you rate your organization's current level of EU General Data Protection Regulation compliance?

# For those who transfer data from the EU/EEA, the vast majority use SCCs

## Data transfer with EU



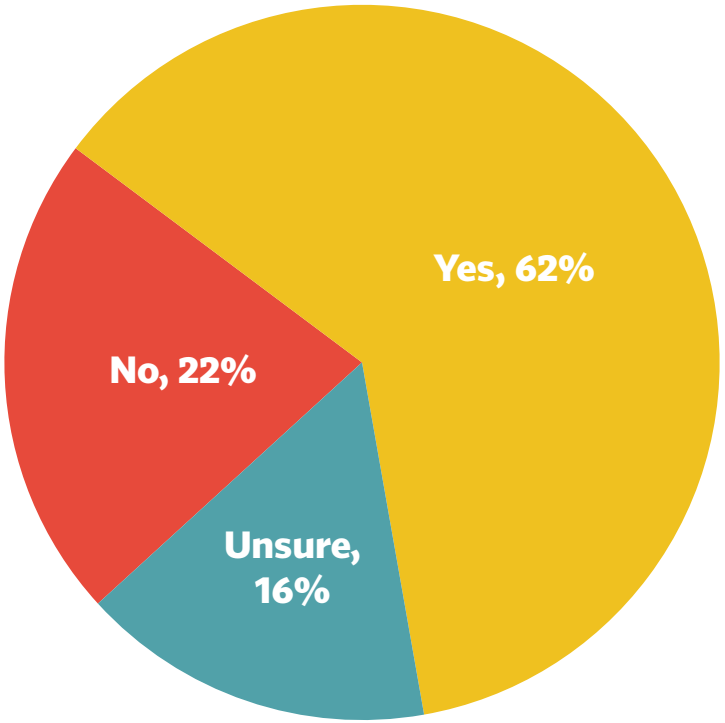

## Data transfer mechanisms
(Base: Transfer data with EU)



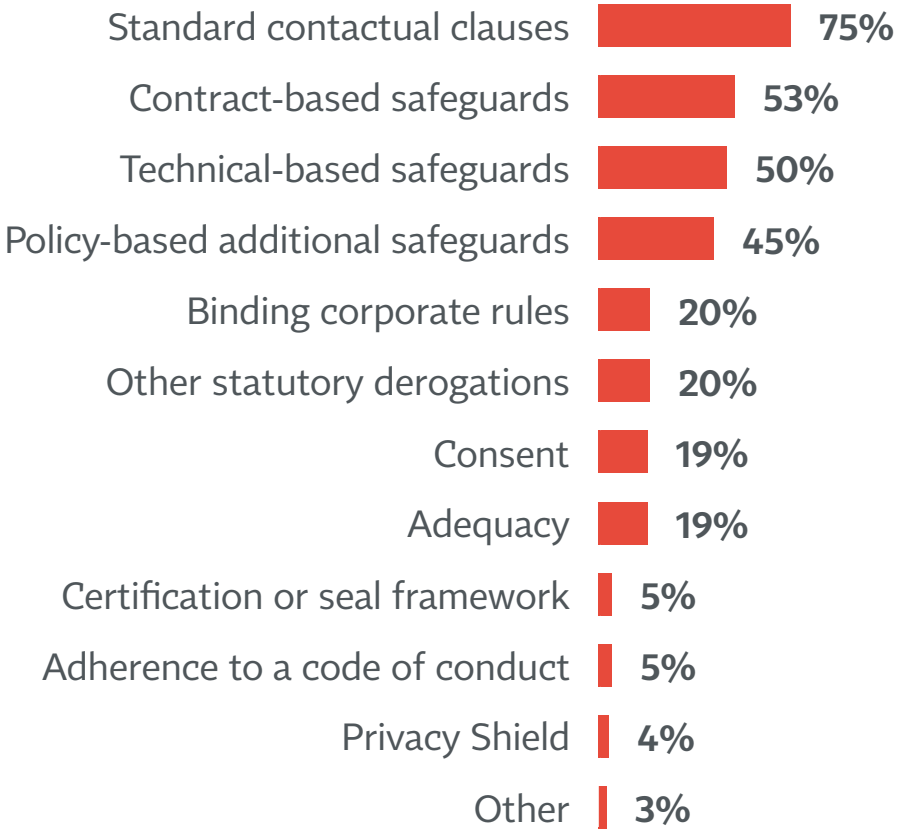

J41: Does your company transfer personal information from the European Union and/or those countries in the European Economic Area to another country outside of the EU?
J42: What mechanisms does your company currently use to transmit data outside the EU?

# Following the 'Schrems II' CJEU decision, more than 60% plans to switch data transfer mechanisms

## Planning to switch mechanisms
(Base: Transfer data with EU)



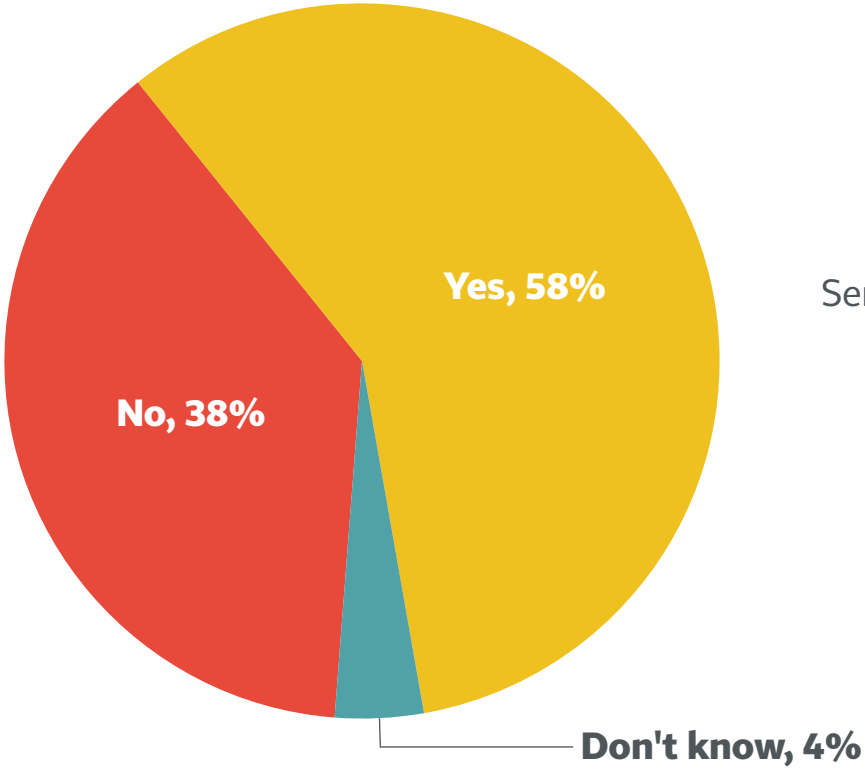

## Planning new mechanism(s) and additional safeguards
(Base: Plan to switch based on CJEU decision)



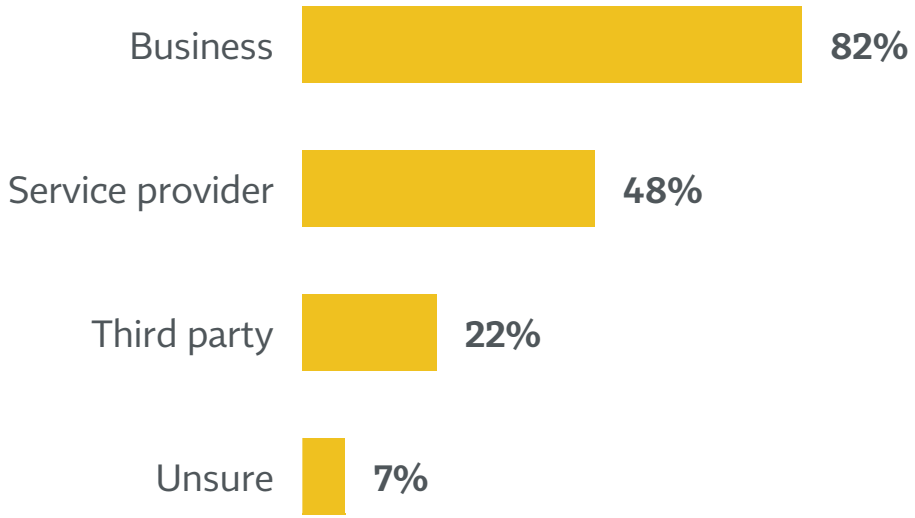

J43: In light of the July 16 decision by the Court of Justice of the European Union regarding the validity of standard contractual clauses, is your company planning to switch data transfer mechanisms?
J44: Which data transfer mechanism does your company plan to adopt in light of the CJEU decision?

# Most firms do business in California and many will be subject to the CCPA as both a business and service provider

## Organization does business in California

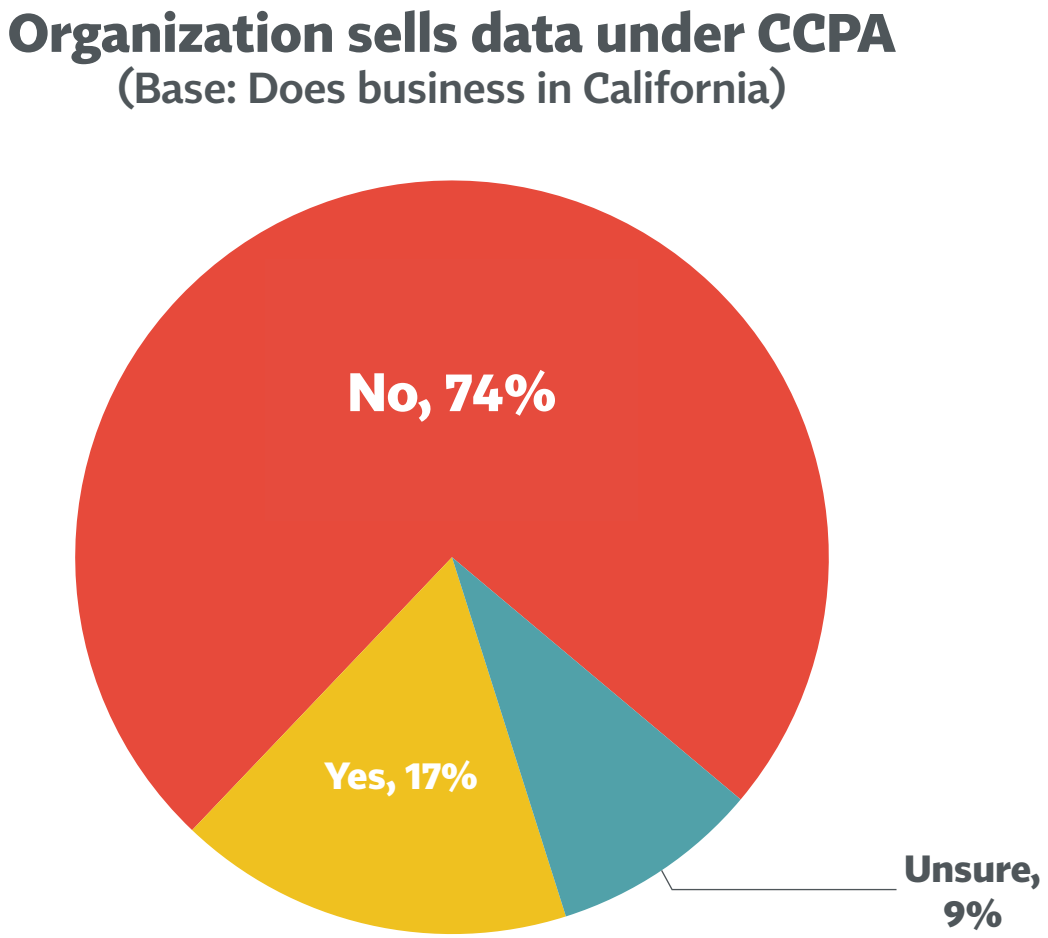



## Organizational classification under the CCPA
(Base: Does business in California)



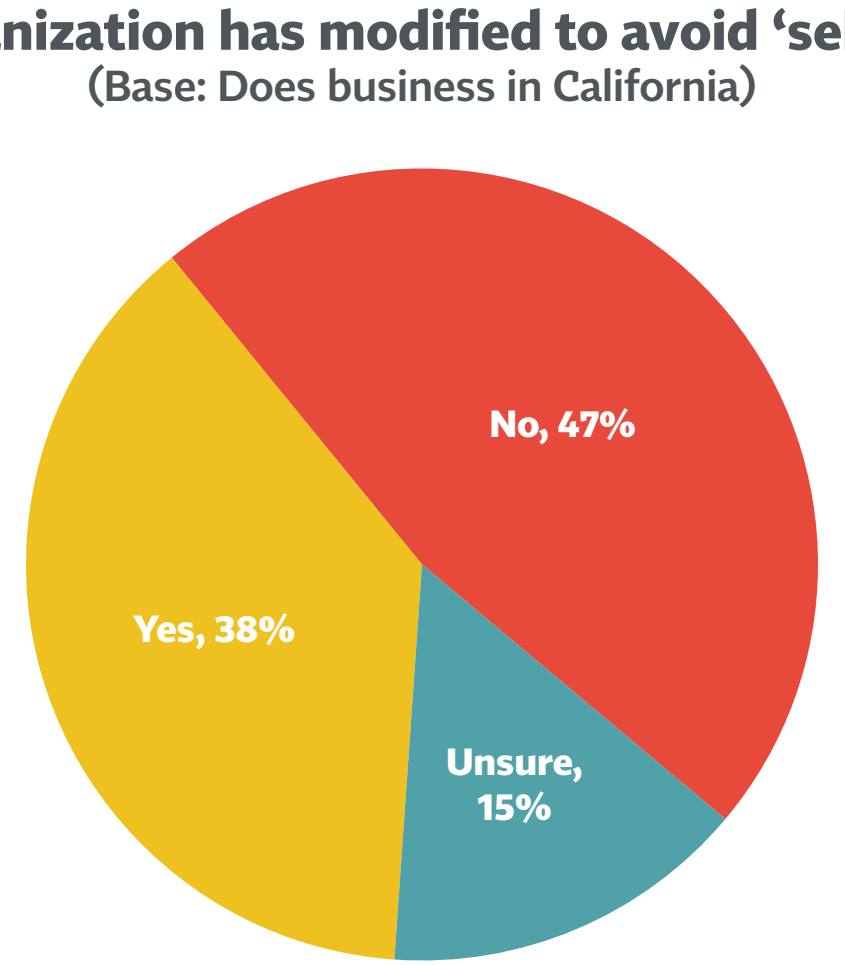

CP1: Does your organization do business in California?
CP2: Under the California Consumer Privacy Act, is your organization considered to be a business, service provider or third party? Select all that apply.

# Yet, of those doing business in California, fewer than 1 in 5 said they sell data under CCPA



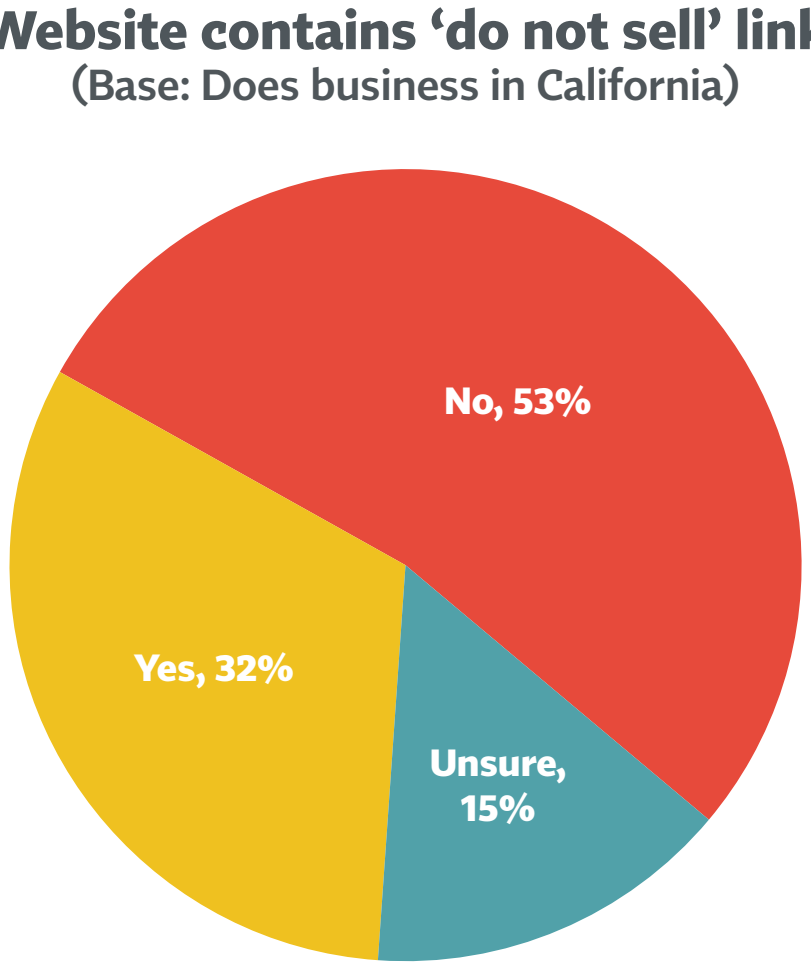

CP3: Under the California Consumer Privacy Act, does your organization sell data?

# 38% of firms doing business in California have modified their practices to avoid selling data under CCPA



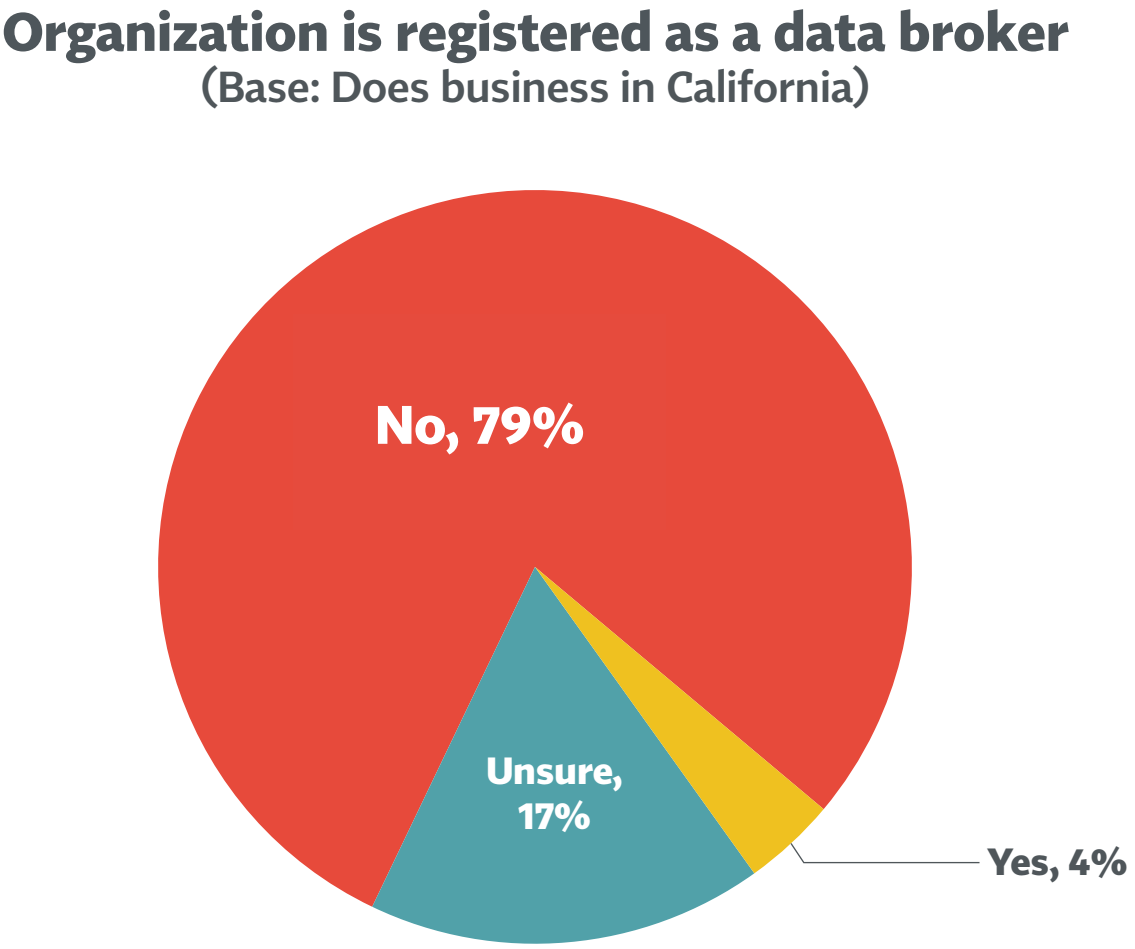

CP5: Has your organization modified its practices or contracts to avoid "selling" data under the California Consumer Privacy Act?

# Interestingly, almost twice as many firms have a ‘do not sell’ link that say they sell data under CCPA




CP4: Does your organization’s website contain a “Do Not Sell My Personal Information” link?

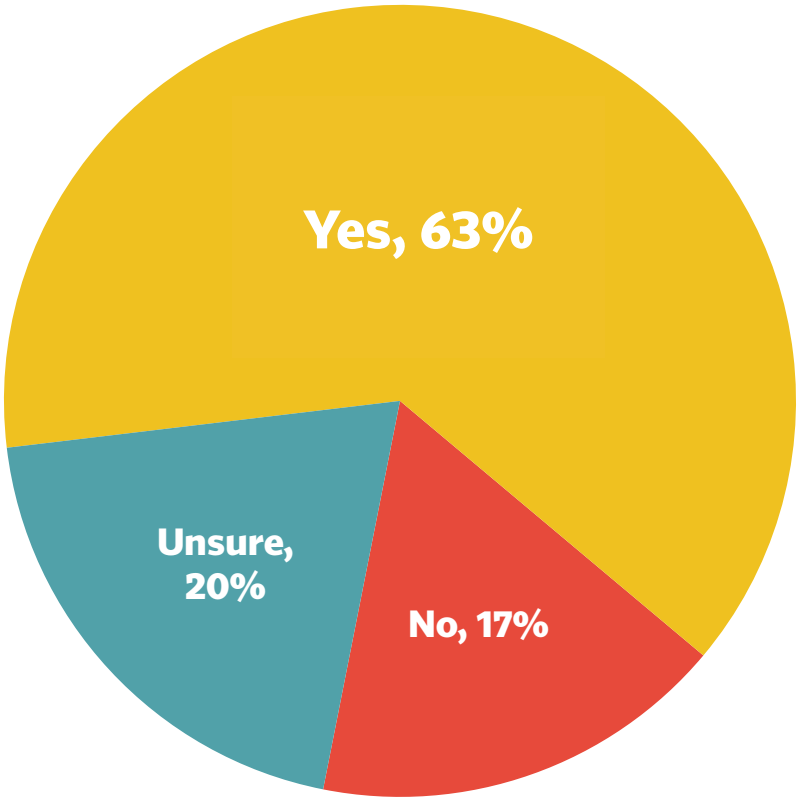
# About 1 in 20 firms doing business in California is registered as data brokers




CP6: Is your organization registered as a data broker in California?

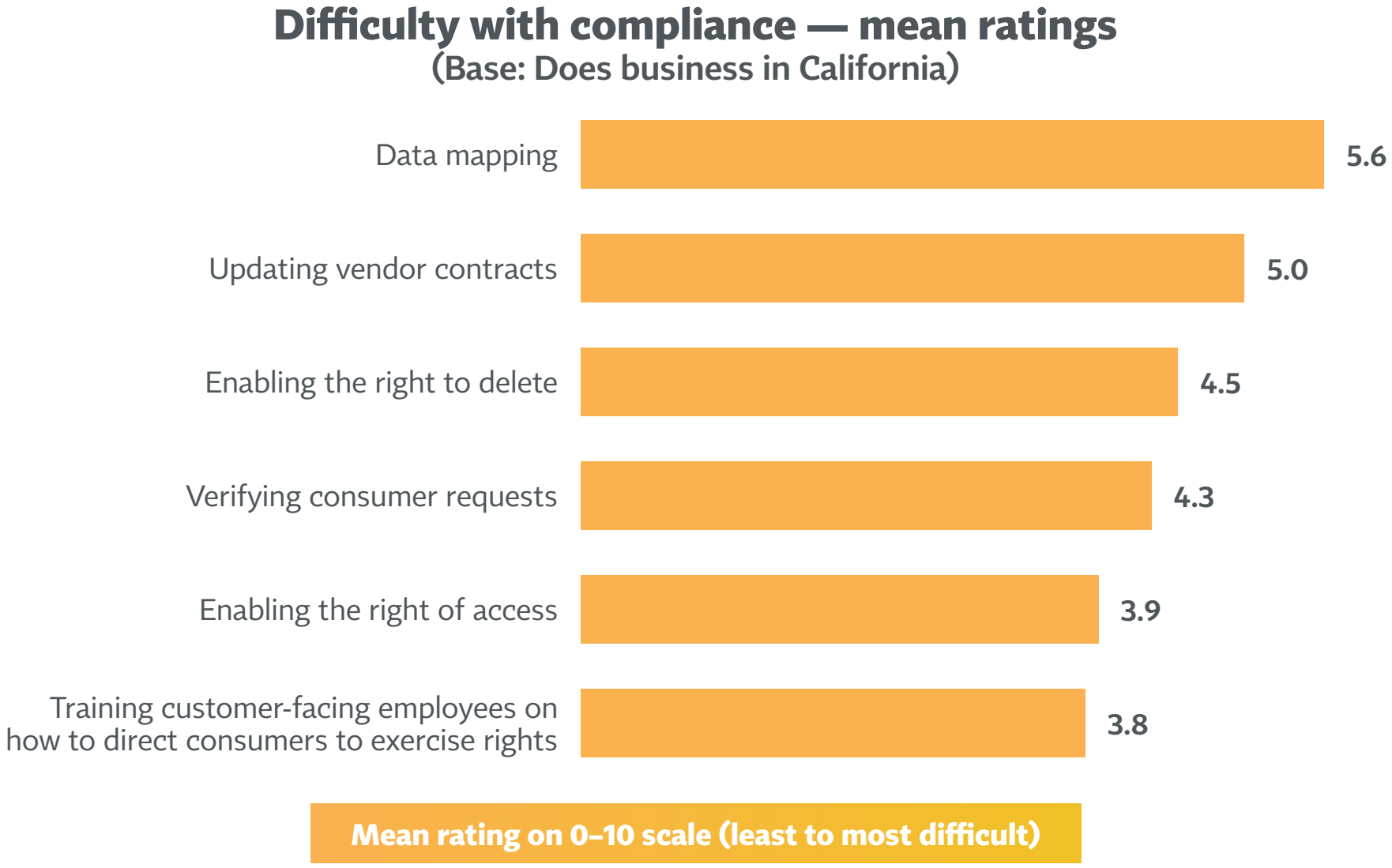
# Two-thirds of firms said they are considering CPRA requirements within their CCPA compliance program

## Organization considering CPRA initiative?
(Base: Does business in California)




CP8: Is your organization considering requirements of the California Privacy Rights Act ballot initiative — which, if adopted, would replace the California Consumer Privacy Act — as part of your CCPA compliance efforts?

# Data mapping, updating vendor contracts and right to delete are the most difficult CCPA requirements

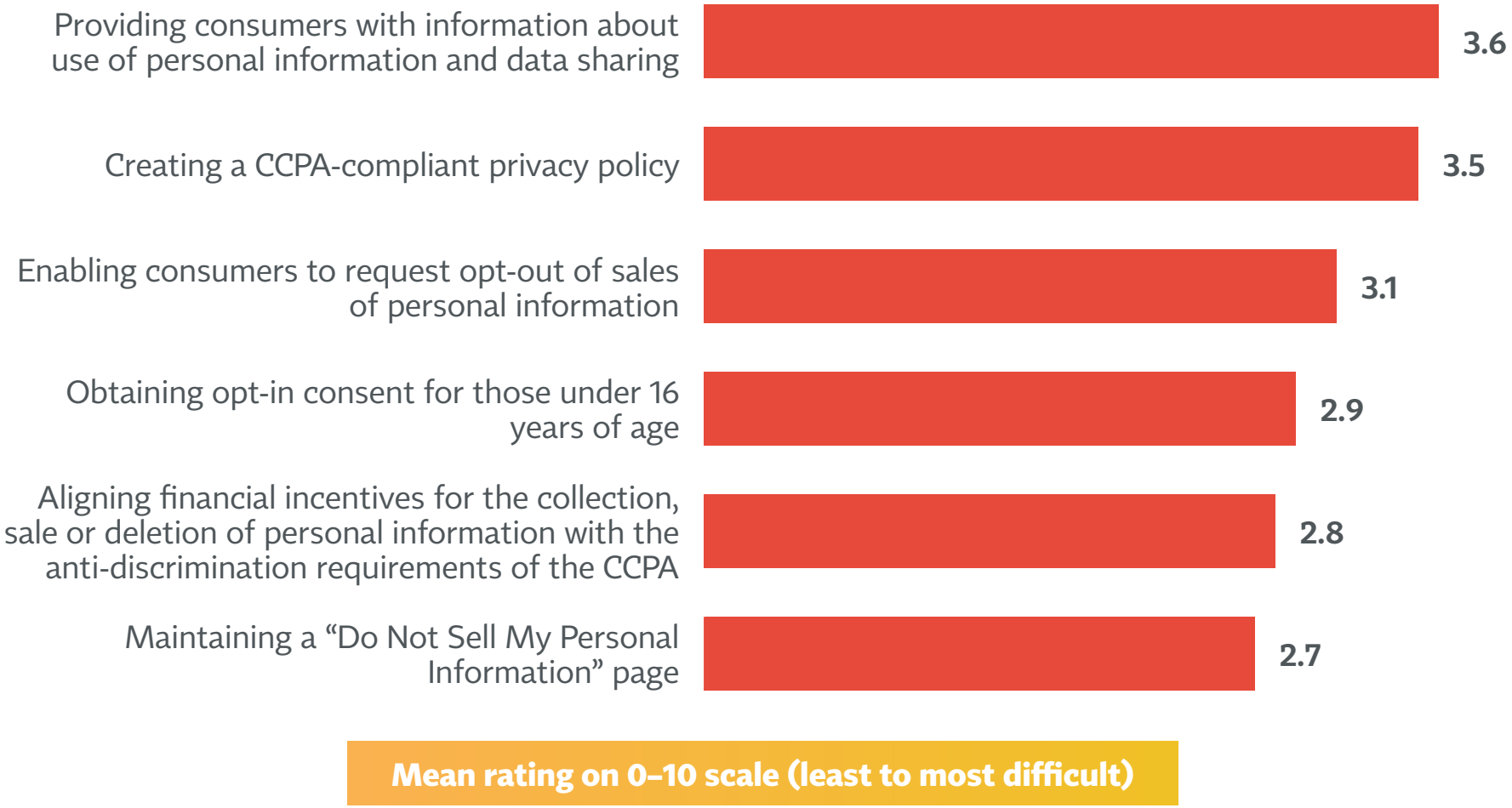



CP9: Using a scale of 0 to 10, where 0 means "not at all difficult" and 10 means "extremely difficult," please rate the following legal obligations of the California Consumer Privacy Act in terms of how difficult they are for your company to comply with.

# Aligning financial incentives and maintaining a 'do not sell' page are among the least demanding obligations

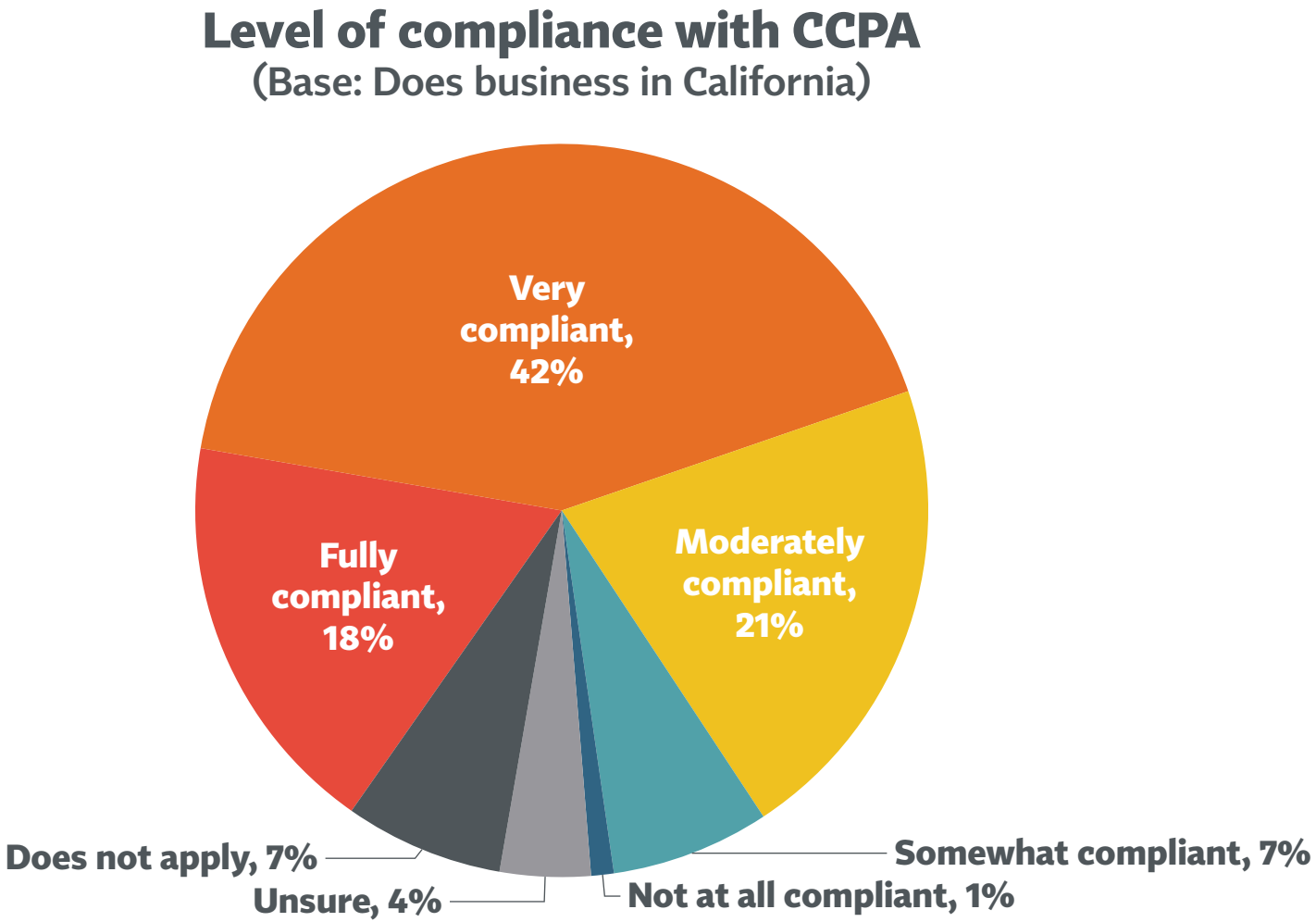
## Difficulty with compliance — mean ratings (cont'd.)

(Base: Does business in California)




CP9: Using a scale of 0 to 10, where 0 means "not at all difficult" and 10 means "extremely difficult," please rate the following legal obligations of the California Consumer Privacy Act in terms of how difficult they are for your company to comply with.

# 60% are fully or very compliant with CCPA; another 21% are moderately compliant

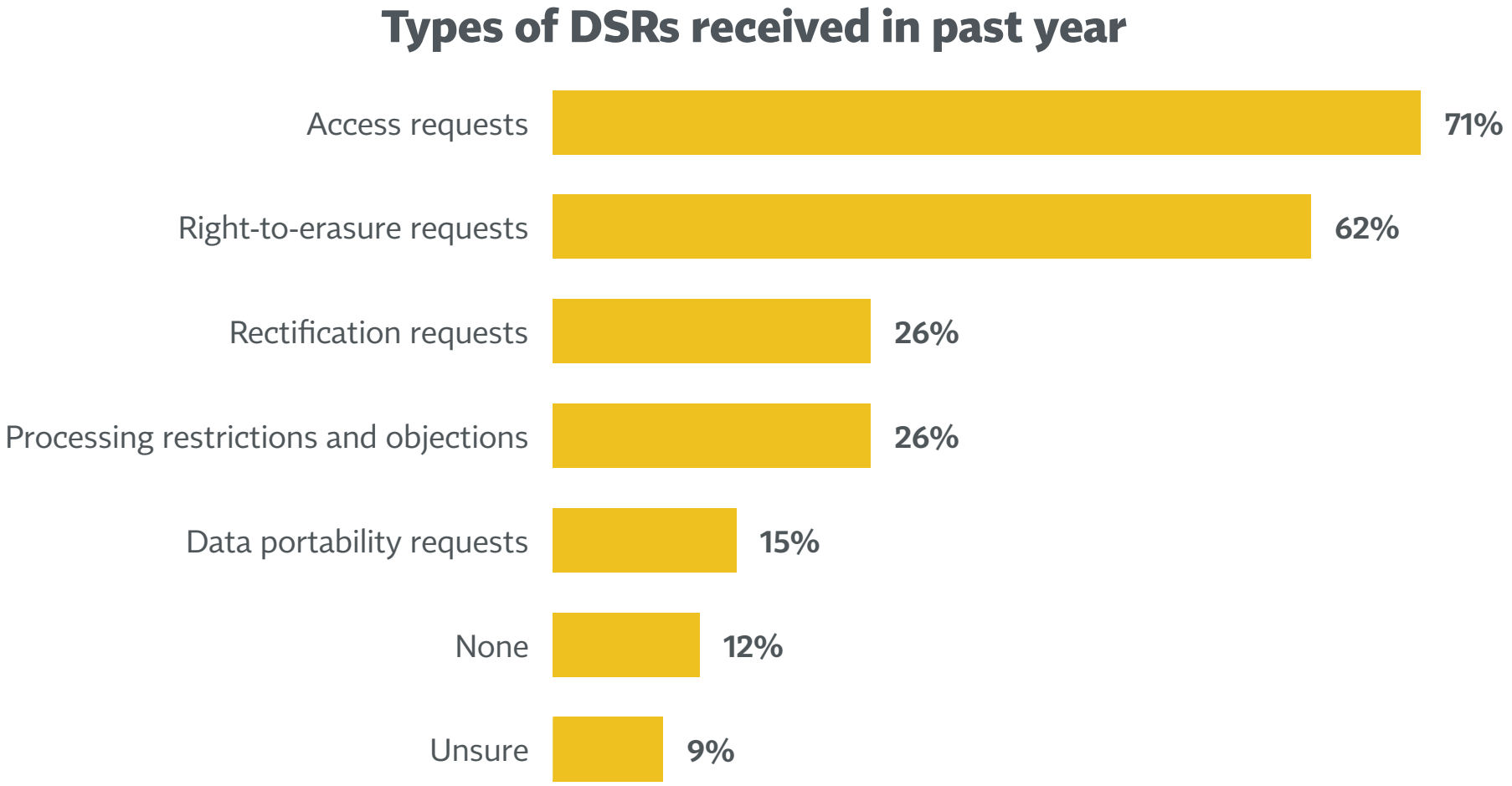



CP7: How would you rate your organization's current level of California Consumer Privacy Act compliance?

# Contents

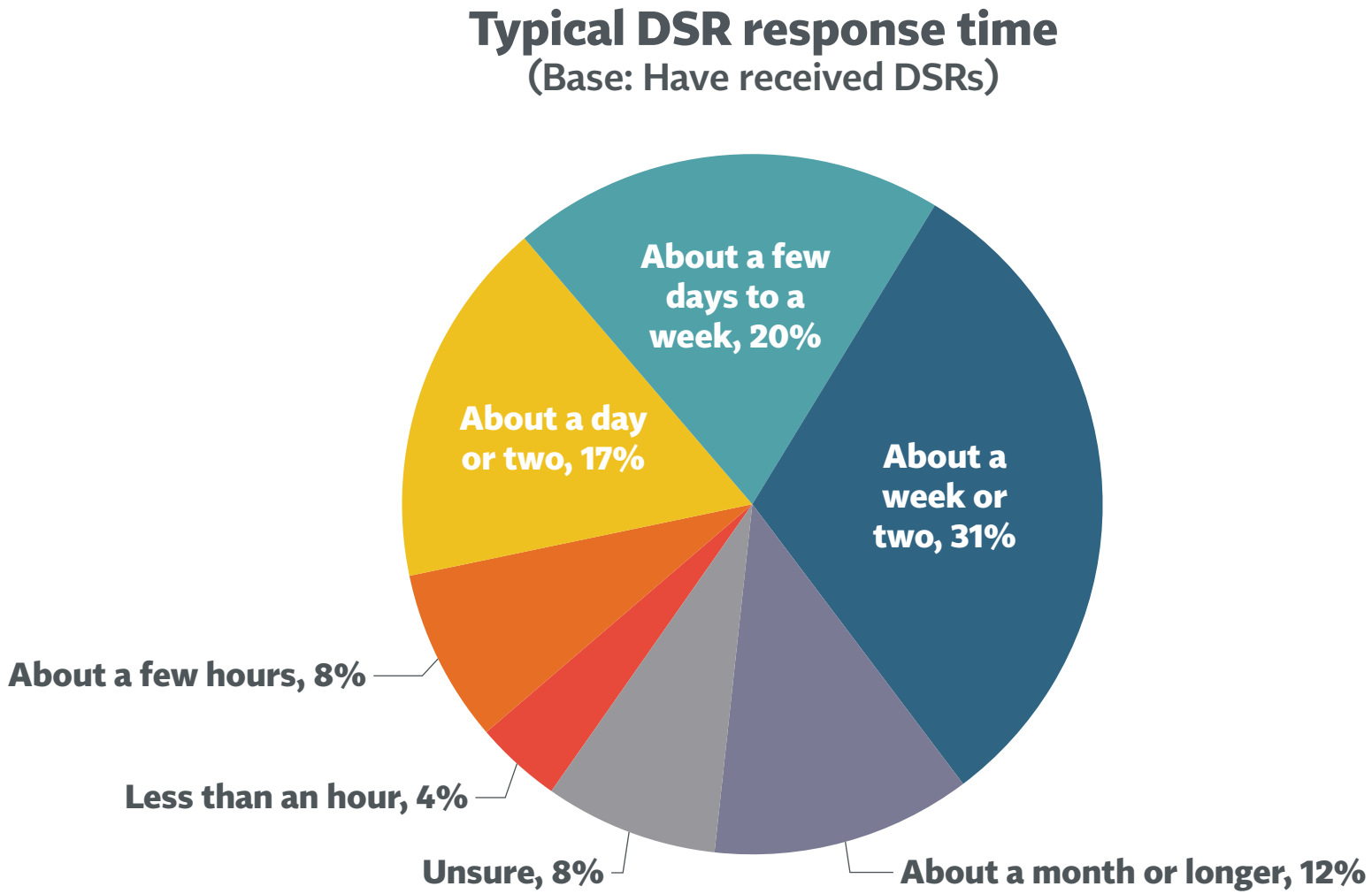


# Access requests and right-to-erasure requests top the list of DSRs received




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

# Only 3 in 10 firms respond to DSRs within a day or two; the rest take anywhere from a few days to a month or more

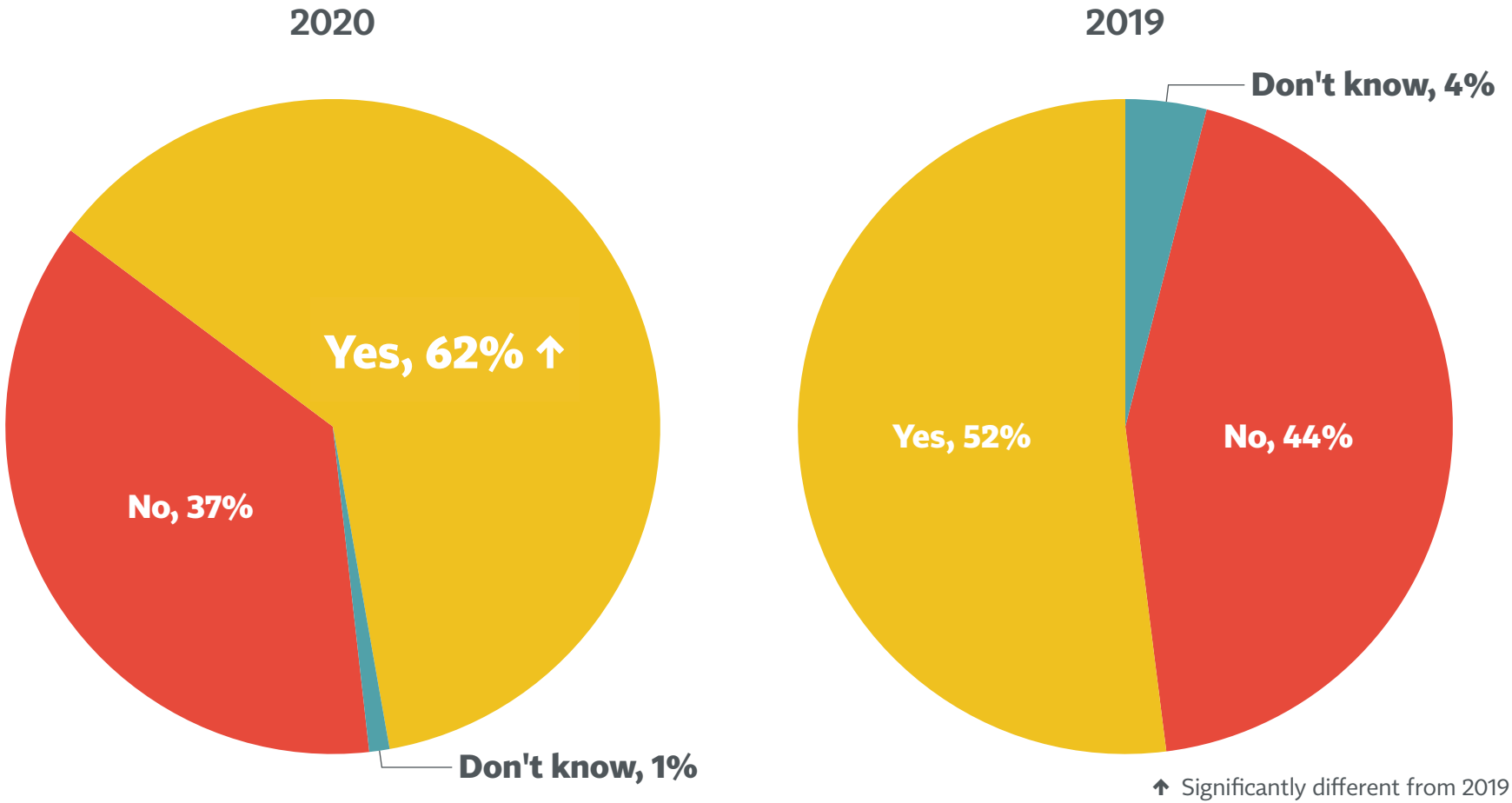



R5: For most data subject requests, approximately how long does it take your organization to respond?

# More than 60% of firms receiving DSRs have a dedicated team to handle them, up from barely half last year

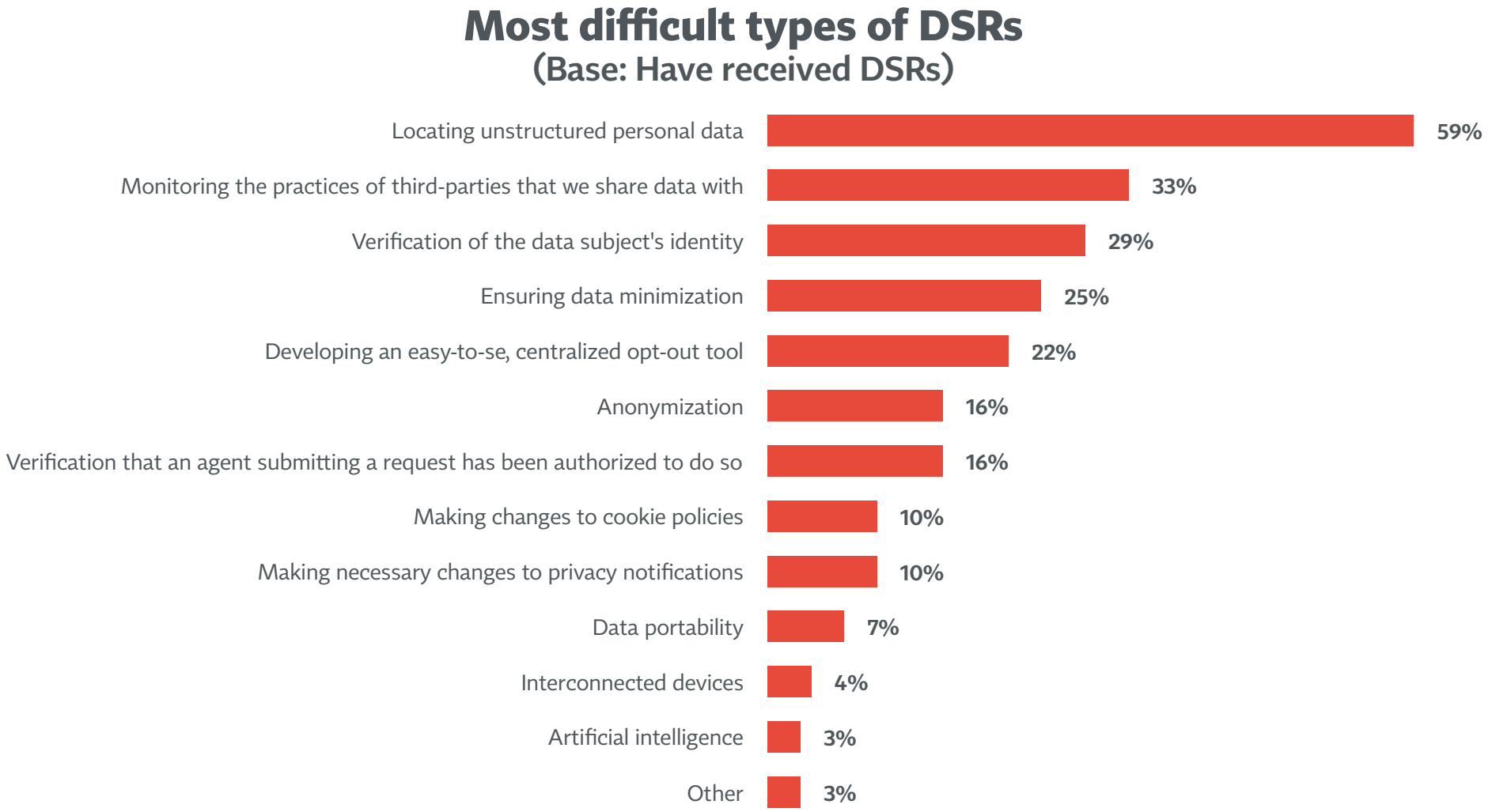
## Whether team is dedicated to handling DSRs

(Base: Have received DSRs)



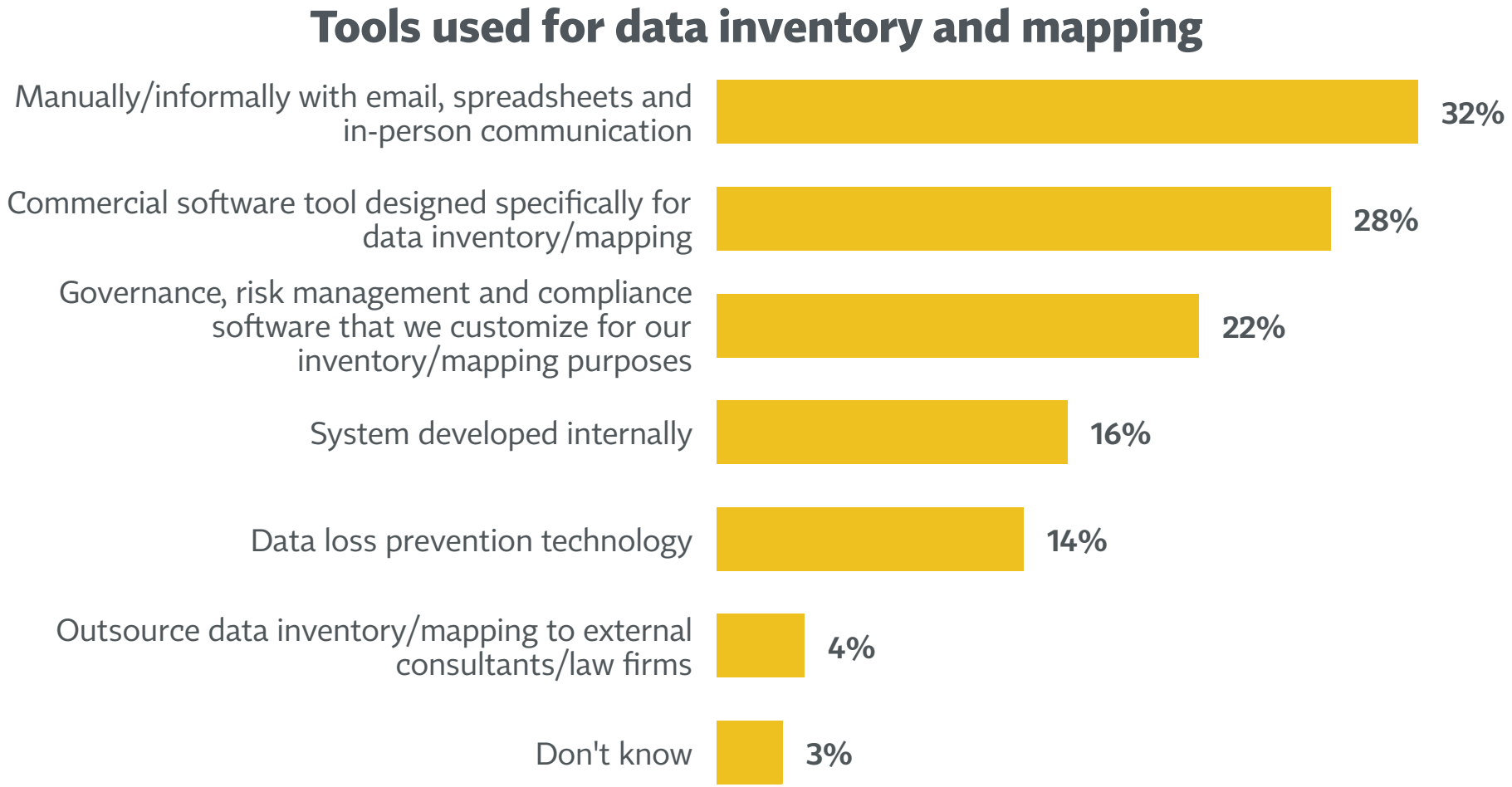

R6: Is there a team at your company dedicated to handling data subject requests?

# As in 2019, locating unstructured personal data is by far the most difficult type of DSR to handle



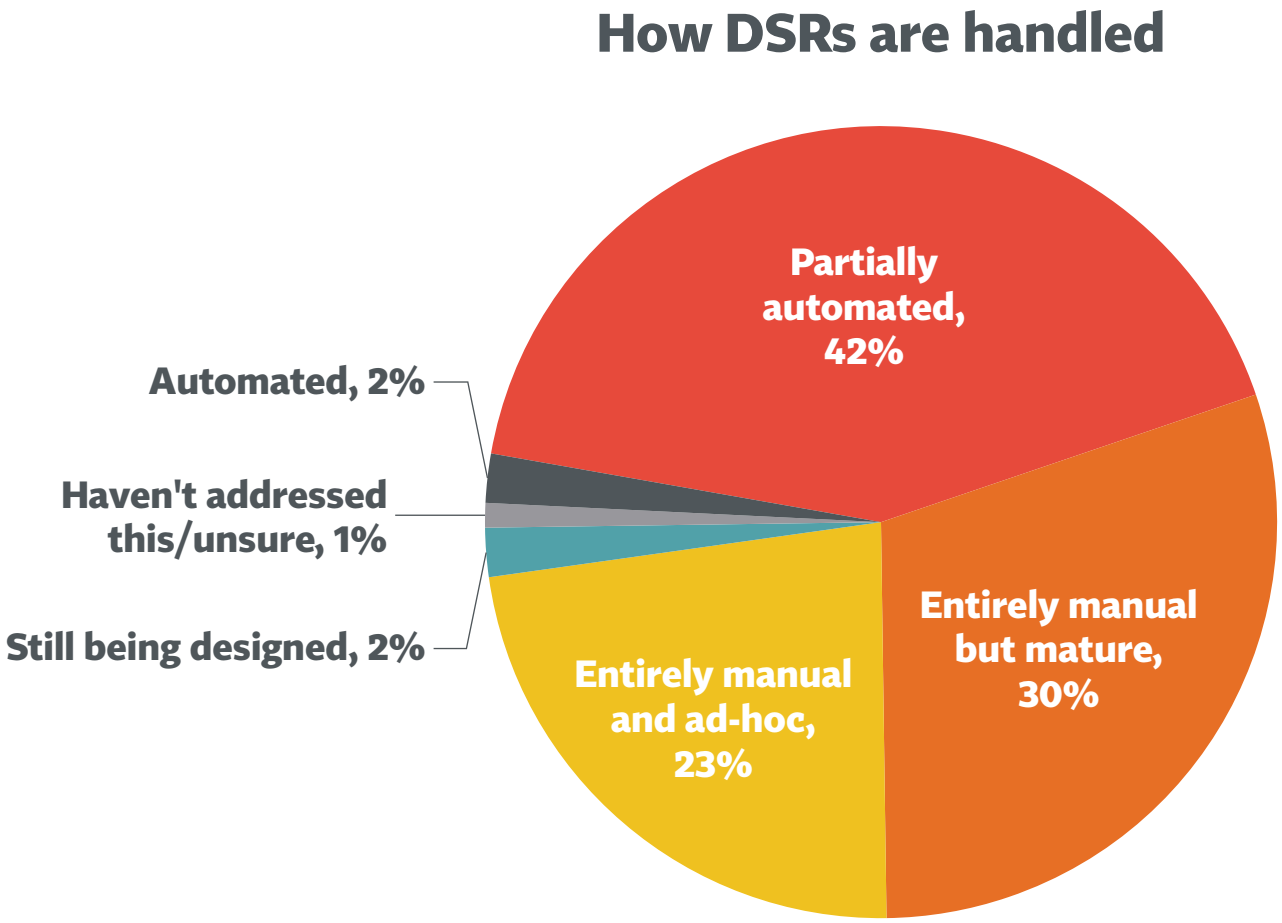

R7: Which of the following issues related to data subject requests are the most difficult to deal with?

# Manual tools for data inventory are the most used, followed by commercial software



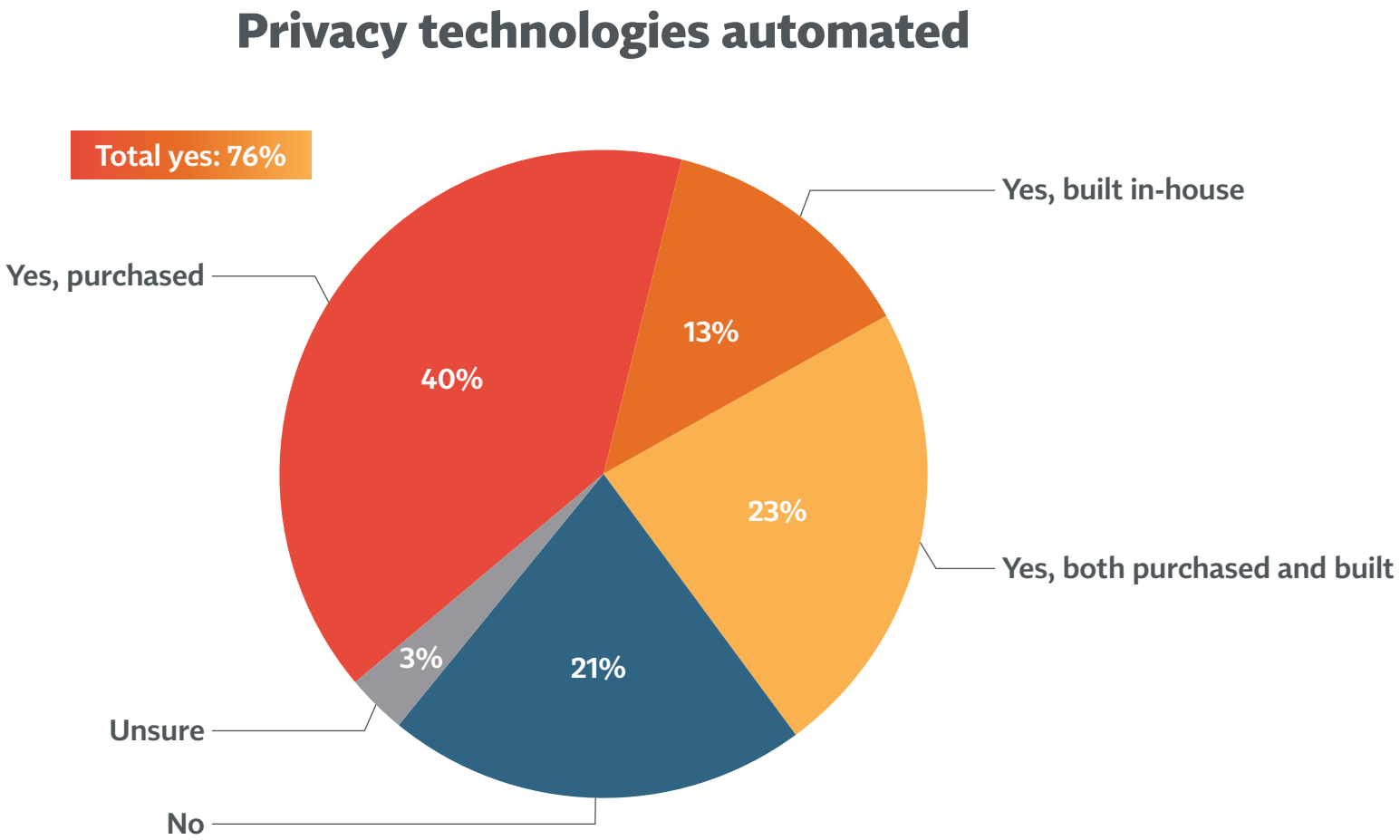

J20: Which of the following tools do you use to conduct data inventory and mapping?

# About half of respondents handle DSRs manually, while the other half uses some degree of automation



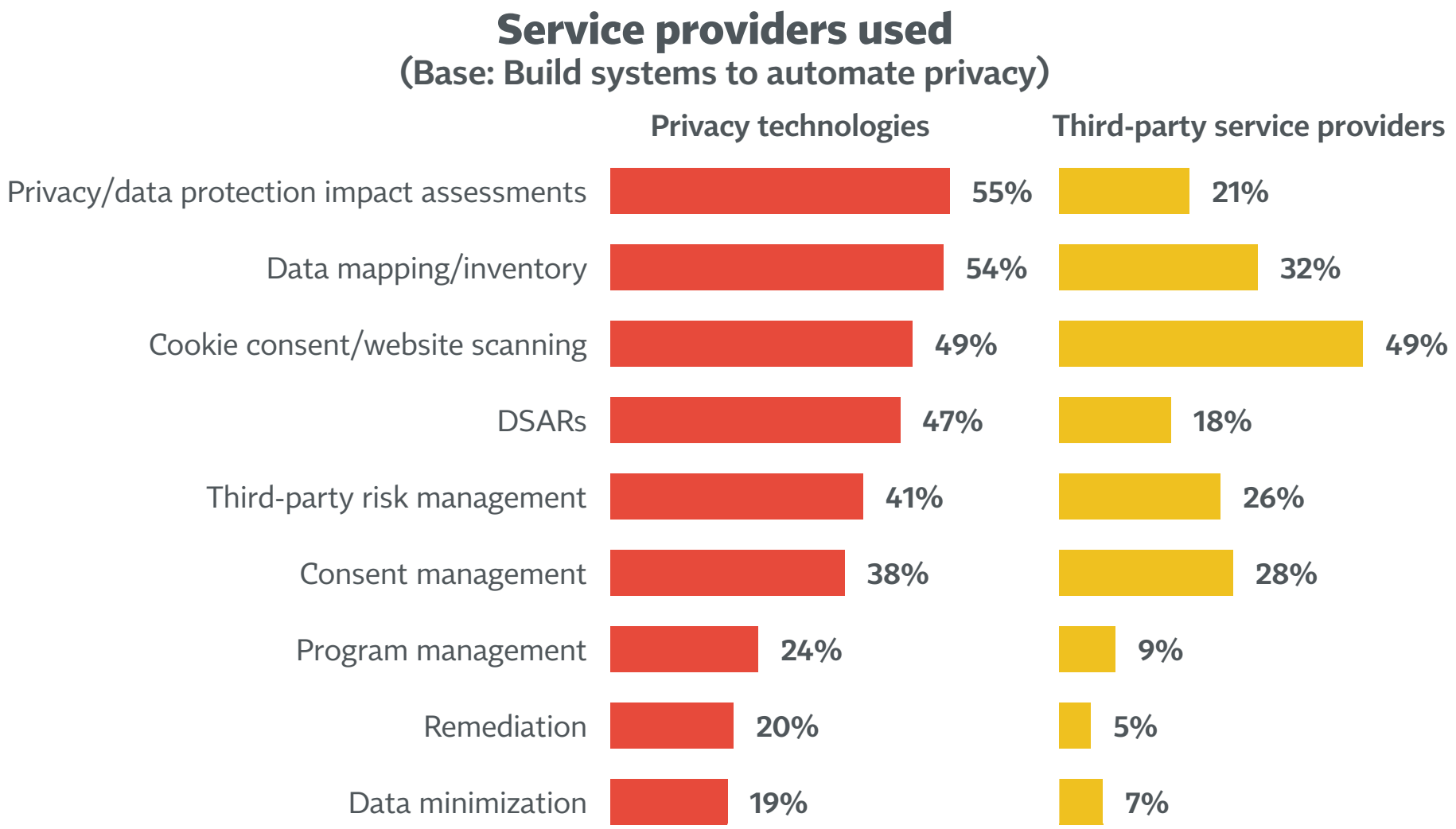

J23: How is your company addressing data subject requests, such as access, portability, right to be forgotten requests, or objections to processing?

# 3 in 4 firms use technologies to automate privacy functions




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

# Most firms use privacy technologies for DPIAs and data mapping/inventory

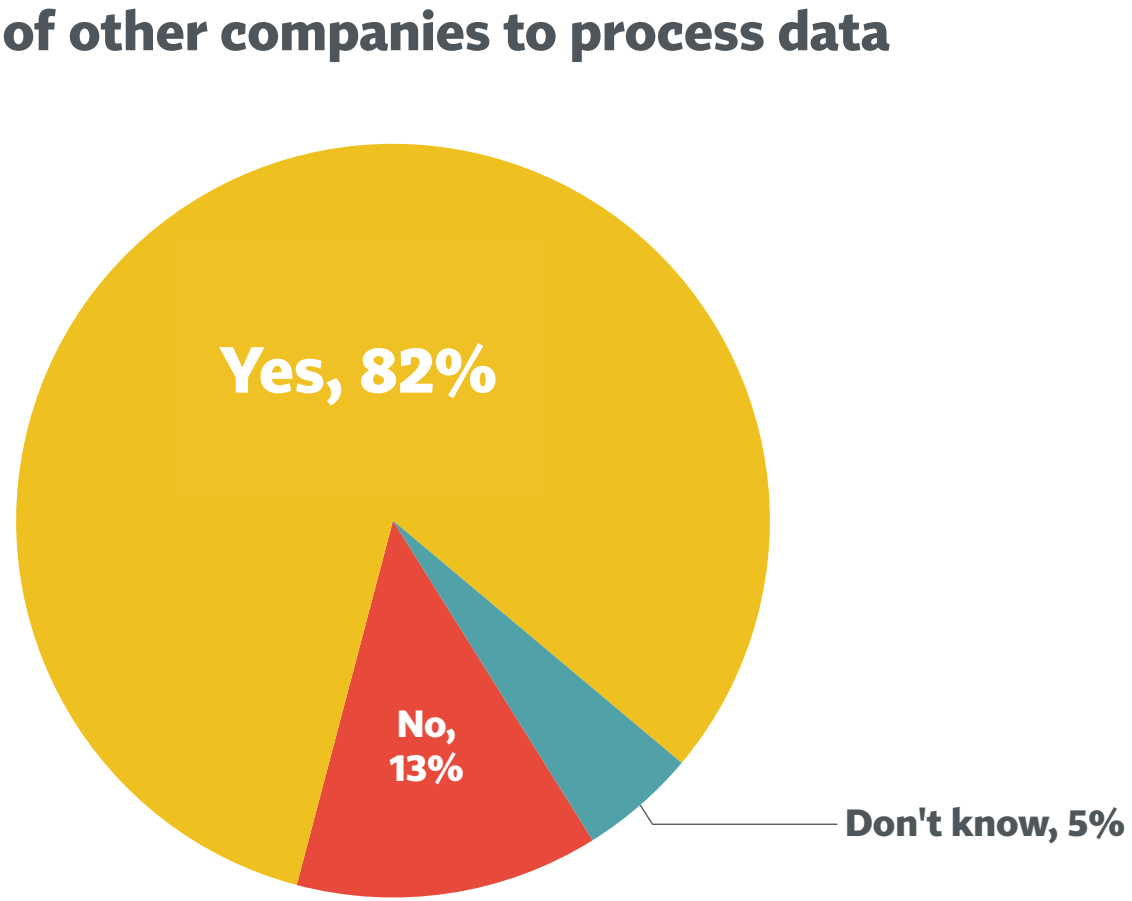



P4: Has your organization used privacy technologies or third-party service providers to perform any of the following tasks? Please check all that apply—if you have used both for a given task, select both.

# Contents

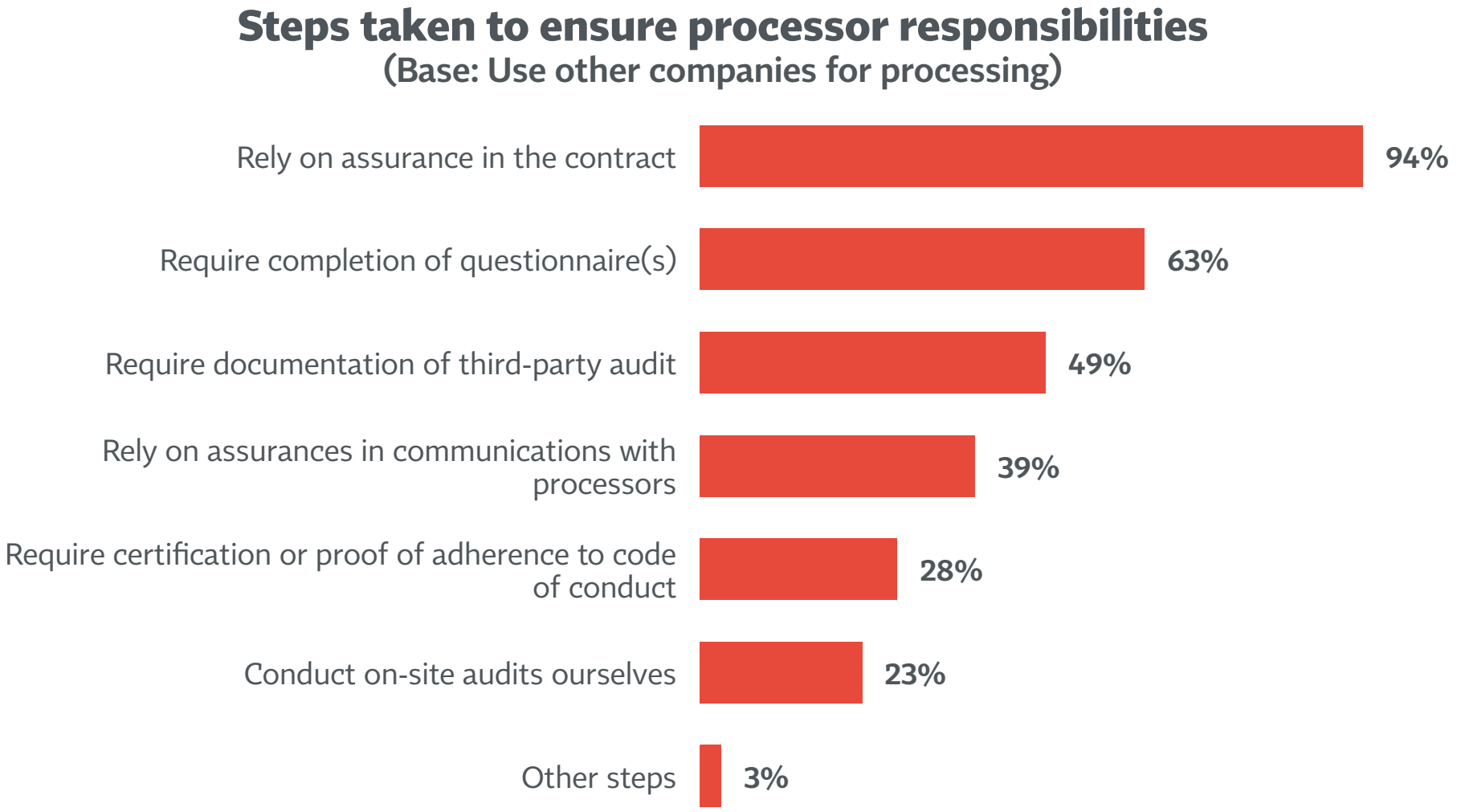


# More than 8 in 10 firms use outside firms for data processing



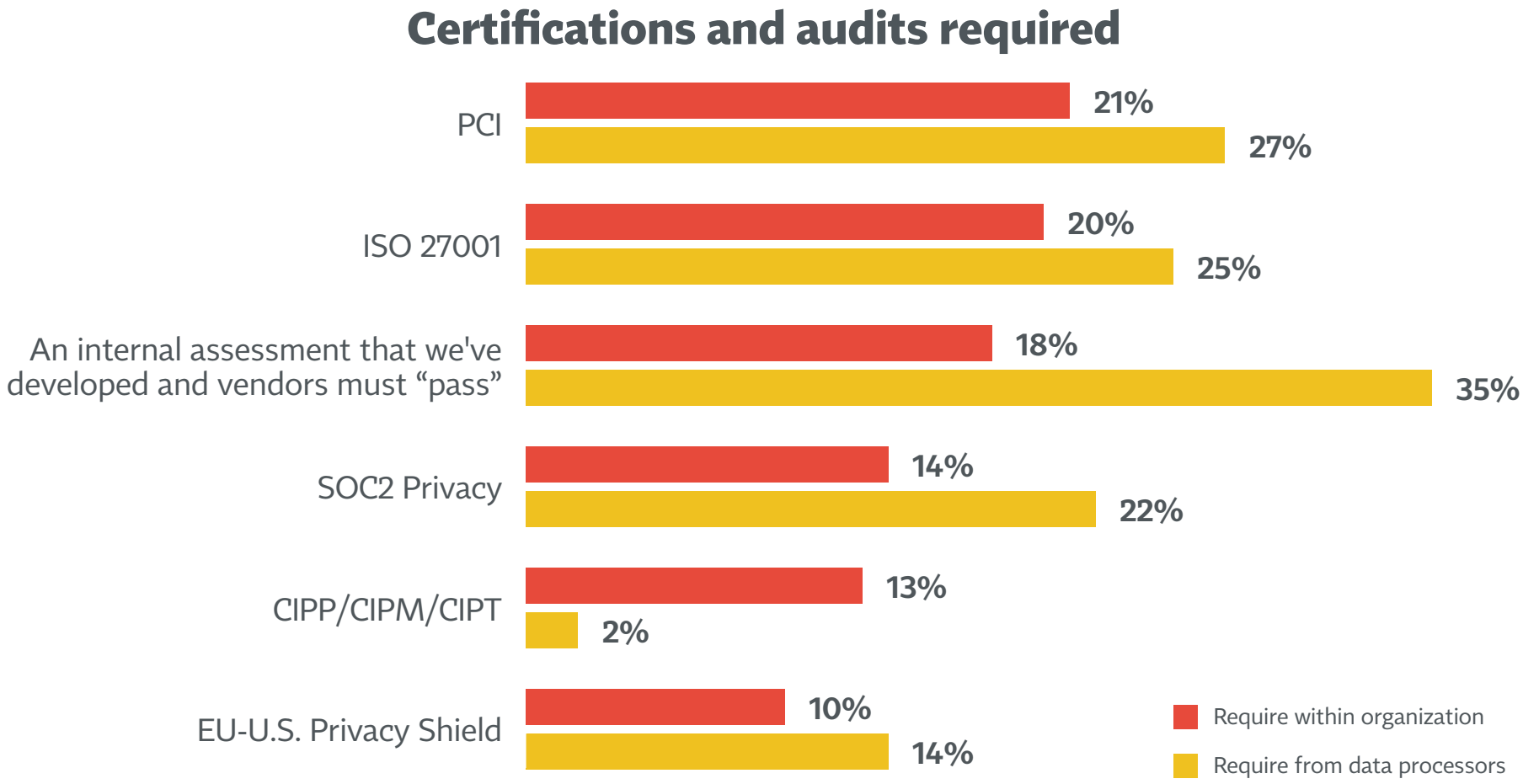

H3: Does your company have other companies process personal data on your behalf of your company (ie., do you use "processors")?

# Contractual assurances, questionnaires and third-party audits are the most common accountability tools




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

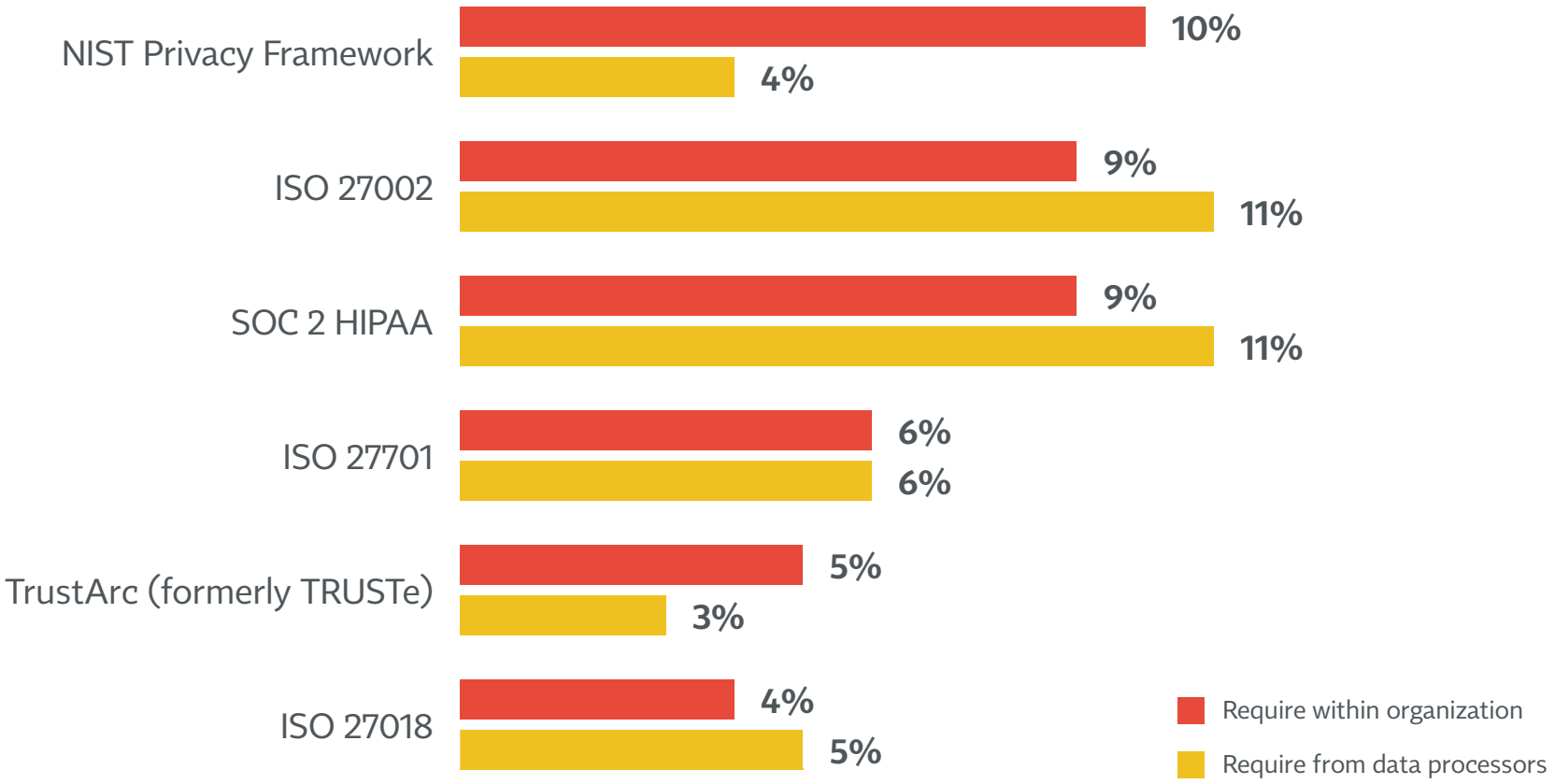
# 35% of firms require data processors to pass an internally designed assessment




K3: Which, if any, third party audits or certifications does your company require within your organization and from your data processors? If you require a given certification both within your organization and from data processors, select both columns.

# About 1 in 10 organizations require ISO 27002 or SOC 2 HIPAA of their data processors

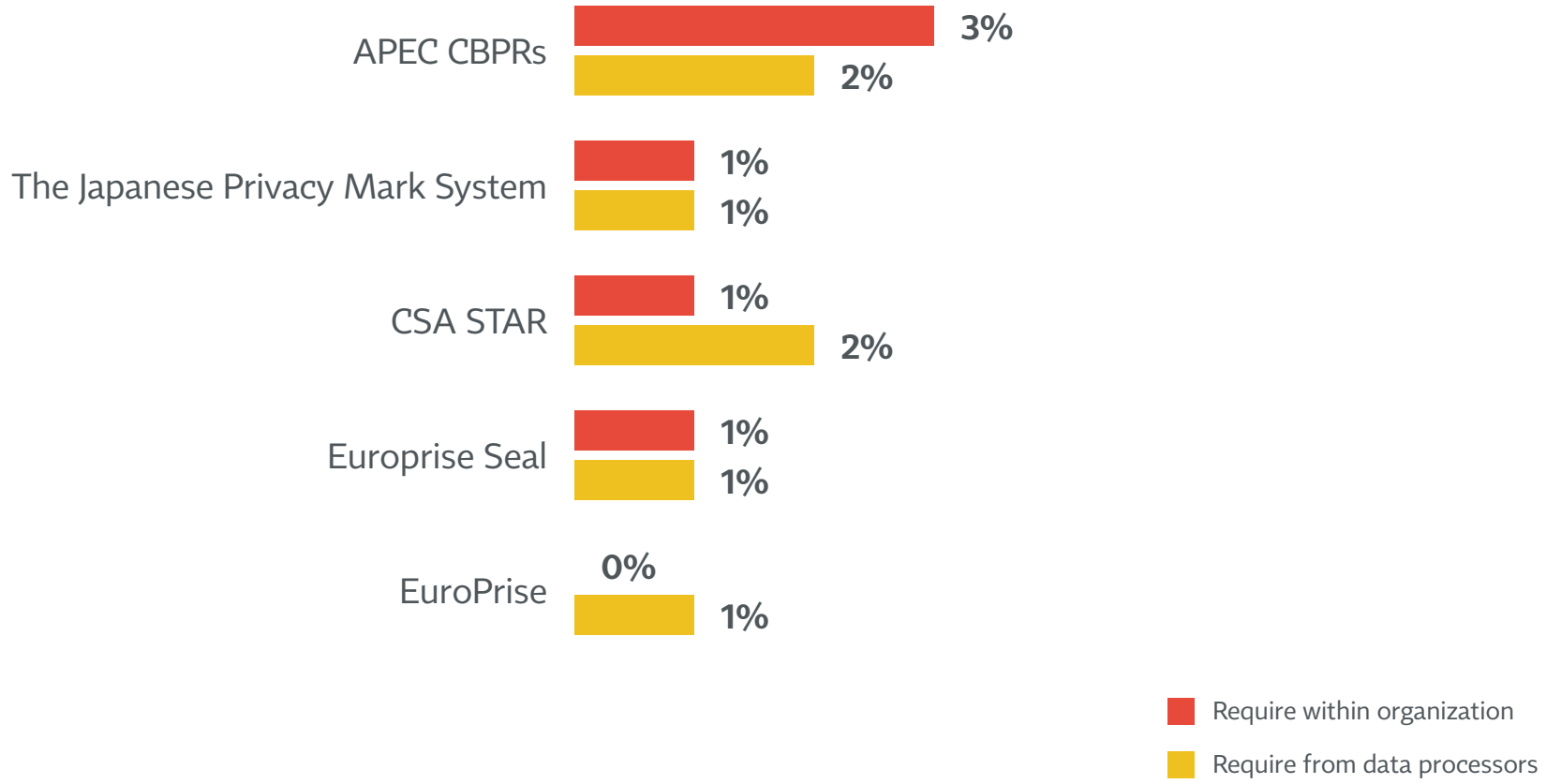
## Certifications and audits required (cont'd.)




K3: Which, if any, third party audits or certifications does your company require within your organization and from your data processors? If you require a given certification both within your organization and from data processors, select both columns.

# Few require APEC CBPRs, Japanese Privacy Mark System, CSA STAR, Enterprise Seal or EuroPrise

## Certifications and audits required (cont'd.)




K3: Which, if any, third party audits or certifications does your company require within your organization and from your data processors? If you require a given certification both within your organization and from data processors, select both columns.

# U.S. firms are far more likely than EU firms to require a range of certifications internally and externally

## BY HQ LOCATION

| | U.S. | EU |
|---|---|---|
| **Require within organization** | | |
| PCI | **28%** | **11%** |
| SOC2 Privacy | **21%** | **4%** |
| EU-U.S. Privacy Shield | **16%** | 3% |
| NIST Privacy Framework | **15%** | **2%** |
| SOC 2 HIPAA | **14%** | 2% |
| **Require from data processors** | | |
| SOC2 Privacy | **33%** | 12% |
| EU-U.S. Privacy Shield | **10%** | 26% |
| SOC 2 HIPAA | **16%** | 4% |

Significantly different than other segments