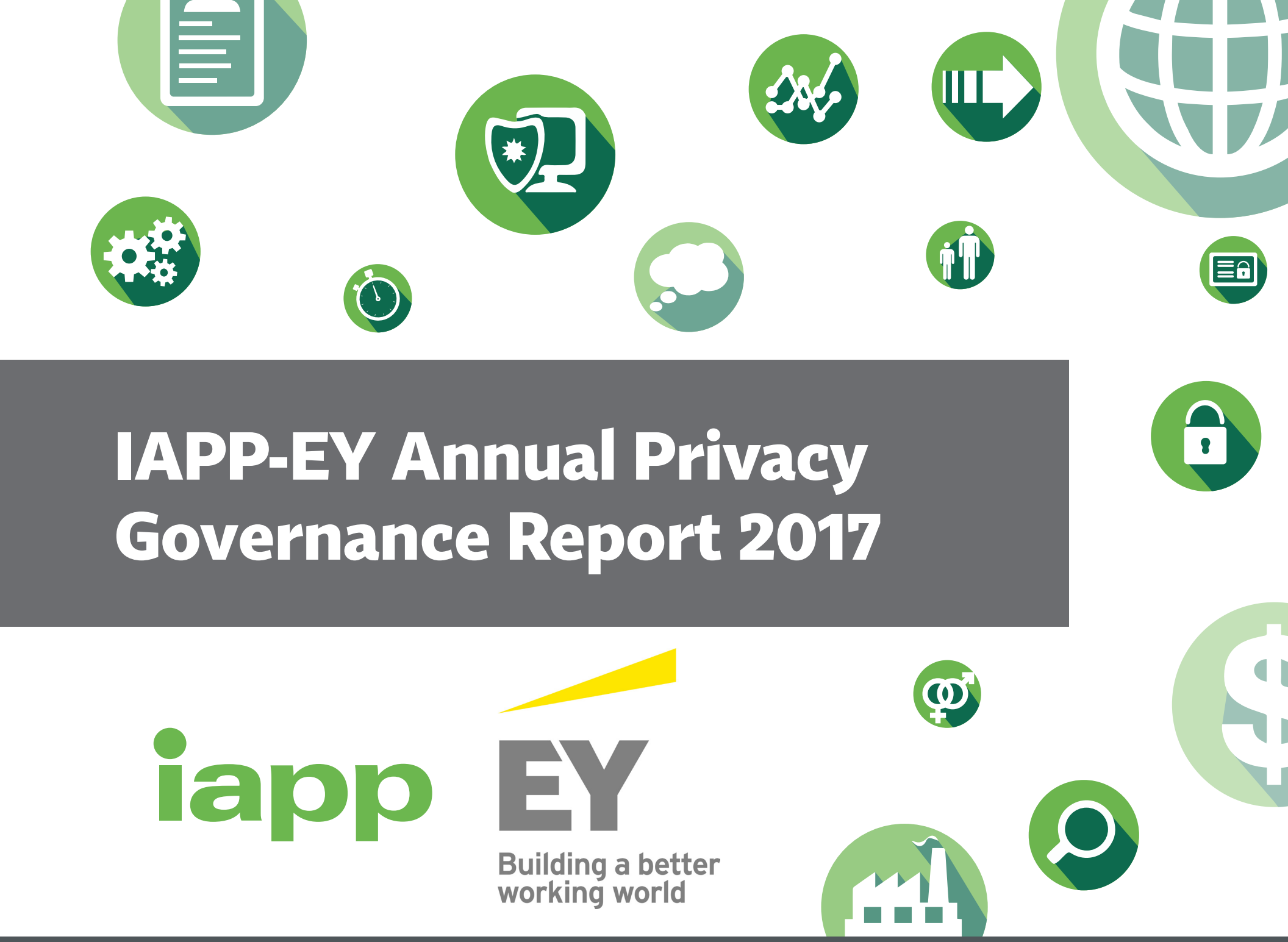


IAPP-EY Annual Privacy Governance Report 2017

iapp

EY

Building a better working world

Introduction

Last year, we told you the broad marketplace response to the General Data Protection Regulation was finally materializing. This year, we see it in the data. As so many have been predicting since 2012 – and earlier – the GDPR is fundamentally changing the way privacy is managed within organizations around the globe.

The privacy leader is being elevated up the organizational ladder. Privacy staffs and budgets have grown. Privacy by design is moving from theory and advice to reality. Privacy professionals now consistently report real influence and integration within the product development lifecycle.

With this third annual IAPP-EY Privacy Governance Report, the result of data provided by nearly 600 privacy professionals across the globe, it's abundantly clear that organizations see the challenge the GDPR presents and are martialing resources to meet it.

And, yet, just 40 percent of organizations feel as though they'll be fully compliant on May 25, 2018, when the GDPR comes into force.

Quite simply, this is hard work. Data is slippery stuff, crossing borders effortlessly, hiding out on laptops and thumb drives, being created with every click of a mouse, swipe of a thumb, and step of a foot. So, too, is it hard to get people to actually understand and follow the policies privacy professionals put into place. Especially if you don't have much by way of budget.

Hopefully, this data can help with that. Do you need to spend money to modify products and services to comply with the GDPR? Our numbers say yes. Do most large companies outside of the EU fall under the GDPR's scope? Our numbers say privacy professionals think so. Does your company want to be an outlier in doing little to prepare for the GDPR? That's the question you need to be asking.

J. Trevor Hughes
CIPP,
CEO and President,
IAPP

Angela Saverice-Rohan
CIPP/US,
America's Leader for Privacy,
EY

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

With this report, we hope you can map your evolving privacy program to a baseline, getting some comfort from the fact that many are in the same boat, but perhaps also finding areas where you might be ahead of the game.

If you've got an active vendor management program in place, you're ahead of nearly a quarter of your peers. If you're doing privacy impact assessments for new products and services, you're similarly in a better place than 25 percent of privacy professionals who may be scrambling for organizational buy in. Maybe you're already asking for SOC2 Privacy documentation from your processors, joining a growing momentum.

Even those lucky programs with hundreds of staff and millions in budget surely have some holes that need patching. The rapidly changing nature of technology and how society uses it almost demands that be true.

This report may help you identify your gaps more quickly, brainstorm remedies, and get to work more efficiently. At the very least, it should help you create productive discussions within your organization and help you rally support to your side.

Good luck, and may May 25, 2018, pass you by uneventfully.

Contents

Executive Summary

In 2016, privacy professionals across the globe got an assignment: help their organizations prepare for the European Union's General Data Protection Regulation before it comes into force on May 25, 2018. The 2017 IAPP-EY Privacy Governance Survey shows they are in full preparation mode, having secured extra budget and staff to work toward meeting the GDPR's requirements and ramping up the operational tasks needed to approximate—if not quite achieve — compliance.

This third annual study of data governance in organizations, surveying modern privacy operations about the present and future of the privacy profession, reflects significant changes in privacy programs globally in response to the GDPR. An astonishing 95 percent of survey respondents, more than 75 percent of whom are located outside of the European Union, say the GDPR applies to their organization.

Many other signs point convincingly toward Europe this year:

- Membership in the IAPP has climbed rapidly to eclipse the 30,000 mark, with nearly 25 percent of the membership located in Europe, where the IAPP is growing most quickly.

- Survey respondents are noticeably more likely than in years past to be from companies with headquarters in the EU – 22 percent, compared to just 15 percent in 2015 and 19 percent in 2016.

- Among EU survey respondents, 75 percent report GDPR compliance is the main reason for their privacy program; the same is true of all organizations with more than 75,000 employees.

- Even when we isolate U.S. firms, 50 percent say GDPR compliance is driving their privacy programs.

- In fact, organizations expect to hire a total of more than two full-time employees just to help with GDPR compliance, and spend a mean of roughly $5 million in adapting products and services and other GDPR compliance activities.

- Those respondents with a CIPP/Europe certification – 22 percent – is double that in 2015.

Operationally, this year's survey confirms that privacy tasks and responsibilities continue to spread steadily throughout organizational functions and initiatives, responsive to privacy by design principles embedded in the GDPR.

We see increases across the board in the steps organizations are taking to prepare for the GDPR, including major leaps over last year in investments in training (up to 63 percent of respondents compared to 50 percent in 2016), as well as appointment of a data protection officer (48 percent vs. 34 percent) or multiple DPOs (up 7 percent over last year).

Perhaps the biggest takeaway from this year's survey, however, is the role that technology is now playing in privacy management. The second most popular tool for GDPR preparation is investing in technology: 55 percent of respondents plan to make such investments, compared to just 29 percent last year. Among privacy team duties, the use of privacy-enhancing software rose to 31 percent of respondents from 24 percent in 2016.

This has far-reaching implications for privacy professionals. For one, it means that, like the information security industry before it, the privacy technology industry is poised for rapid growth. For another, it means privacy leaders will need to acquire budget and authority for technology acquisition lest they lose control of such purchases to the CIO, CTO or CISO.

Privacy professionals' approach to privacy is also beginning to reflect the GDPR's risk-based approach. This year's survey sees an 11-point increase over 2016 in the percent of respondents working with risk management, and overall there is a shift in focus toward risk and away from pure compliance.

Firms are investing more in privacy staff, with organizations saying they've had to add an average of one full-time staffer for GDPR compliance alone. Privacy budgets are notably bigger, too, with mean privacy spending rising from $1.7 million to $2.1 million. All this new spending still isn't enough, however, according to 67 percent of respondents who claim their budgets are either somewhat less than sufficient or much less than sufficient to get the job done right.

The second most popular tool for GDPR preparation is investing in technology: 55 percent of respondents plan to make such investments, compared to just 29 percent last year.

They have a point: Of the firms that believe the GDPR applies to them, nearly 6 of 10 will be only partially compliant by the deadline in May 2018.

Indeed, as seasoned privacy professionals and those just coming online dive into the GDPR, they are finding it more challenging and complex that they initially thought. Nearly every category in our "GDPR Obligation Difficulty" scale rated a higher difficulty score than last year.

Adding to compliance complexity, privacy leaders – who often are asked to wear more than one hat – are now being asked to serve as the DPO, a position mandated by Article 37 of the GDPR. Although 44 percent of respondents report their organization does not yet have that position, 32 percent report the privacy lead is filling the DPO role themselves.

The EU has tremendous leverage as an economic powerhouse and its ability to affect how organizations around the globe manage data collection, storage, and use cannot be doubted. Even though the EU's GDPR has yet to take effect, organizations the world over are spending money on hiring and promoting privacy staff, training employees on privacy, purchasing technology to help with GDPR compliance, and pushing privacy awareness into every corner of the firm. Privacy issues are now board-level concerns – even apart from data breach issues – as organizations are more likely than ever before to see privacy as risk management, and business opportunity.

With so many firms struggling to be GDPR compliant by next May, the privacy profession's growth trends are likely to continue in the coming year.

Contents

Research Objectives

The overarching goals of this research are to:

- Profile privacy program structures within organizations of various sizes and sectors
- Identify the most critical issues privacy departments are facing
- Track how both of the above are evolving over time

Method

General Target:
Privacy professionals known to the IAPP.

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

Response:
A total of 548 completed the interview, with some sections having somewhat smaller sample sizes.

The survey asked for a variety of detailed information on privacy budgets, employees, salaries, and department structures.

NOTE: The year's wave of the Governance survey was conducted only among in-house privacy professionals.

WEIGHTING: The 2017 results were statistically weighted to match the employee size distribution of firms answering the 2016 survey. This distribution matching allows us to make apples to apples comparisons between findings from the two years.

Glossary

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

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

CISO: Chief Information Security Officer

CISSP: Certified Information Systems Security Professional – a certification offered by (ISC)[2]

Customer target: For the purposes of comparison, we ask respondents to categorize themselves as primarily business-to-business (B2B), business-to-consumer (B2C), or a blend of both sales channels.

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

Full-time vs. part-time: You will see references to "full-time" and "part-time" privacy employees. This is not intended to mean that "part-time" employees are not full-time employees of the organization. Only that they spend part of their time on privacy matters.

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

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

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

PIA: Privacy impact assessment – this should be thought of as synonymous with data protection impact assessment, but not specific to the DPIAs as outlined in the General Data Protection Regulation.

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

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

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

Contents

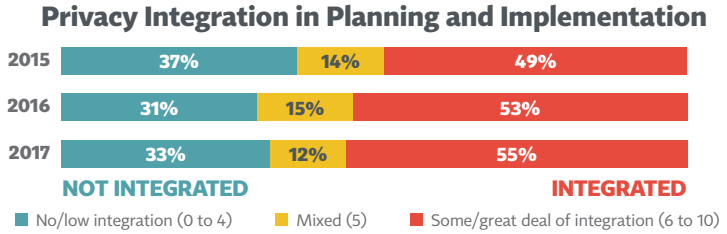
How the Job of Privacy Is Done in the GDPR Era

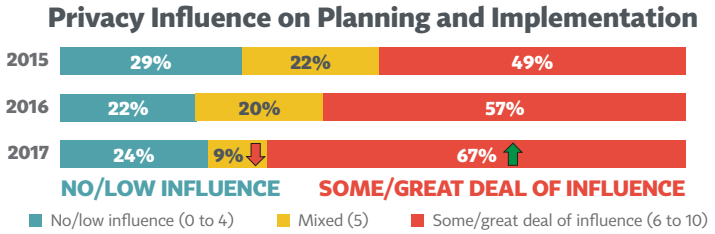
"Privacy by design" moves privacy deeper into the organization

Increasingly, privacy professionals have become ingrained in the inner workings of the enterprise, which will serve them well as they strive to comply with the complexities of the EU's General Data Protection Regulation and other privacy laws around the world.

The GDPR has brought into law for the first time the concept of privacy by design, something pushed by regulators in theory previously, but now ensconced in legal text. Organizations are clearly responding.

Privacy professionals' colleagues show increasing willingness to involve privacy pros early and often in activities and new initiatives. For ongoing activities, privacy professionals report getting involved at the outset 43 percent of the time (up from 31 percent just two years ago). They are also much more likely than ever before to be included during the development stage of new initiatives. Indeed, privacy's integration in project planning and implementation has increased steadily since this survey was first launched in 2015 – 76 percent report such integration in 2017, up from 59 percent two years ago.





Profile of Survey Respondents

The English-language survey was sent to subscribers of the IAPP's Daily Dashboard, roughly half of whom are IAPP members. We limited our survey to those who hold in-house privacy positions and did not gather data from outside attorneys or consultants as in years past. Accordingly, this year's survey results reflect primarily the experiences of in-house privacy professionals in the private sector (80 percent), with a modest showing of government-based privacy pros (17 percent).

Although more than half of the respondents this year — as before — are headquartered in the United States, for the first time it's a slim majority. Whereas two years ago 69 percent of survey respondents worked in the U.S., and last year 63 percent did, this year only 59 percent of respondents are from the U.S. while 22 percent — up from 13 percent in 2015 and 19 percent last year — hail from organizations headquartered in the

continued on xii

The GDPR also encourages firms to take a risk-based approach to privacy. This is reflected in where privacy professionals work within the organization. As in prior years, privacy pros are most likely to work in or with the legal or compliance department (72 percent), or in information security/IT (47 percent), but they are increasingly finding their way into risk management departments (44 percent).

In terms of whom privacy professionals work with, moreover, the year-over-year numbers show a steady increase in cooperation with legal, compliance, and IT, and even sharper growth in cooperation with marketing and records management. This may be explained at least in part by the importance the GDPR and other privacy laws place on demonstrating consumer consent for many direct marketing activities.

GDPR drives bigger privacy budgets and staff increases

Fifty seven percent of last year's survey respondents predicted budget increases for their privacy teams – and it turns out they were right. The average mean privacy budget leapt from $1.7 million to $2.1 million. Excluding salaries, average budgets grew from $457,000 in 2016 to $610,000 overall in 2017. Both U.S.- and EU-headquartered respondents showed budget increases over last year, and for the most part so did firms of all employee sizes and revenue segments.

Not surprisingly, the biggest overall spenders are the companies with the biggest overall budgets and the most employees. On a per-employee basis, however, the survey shows that what we define as "unregulated" industries (i.e., those not traditionally tightly regulated, like health care and financial services) spend more per employee than regulated or government organizations, likely reflecting the size and global reach of technology and telecom companies as well as their vulnerability to GDPR's stringent requirements.

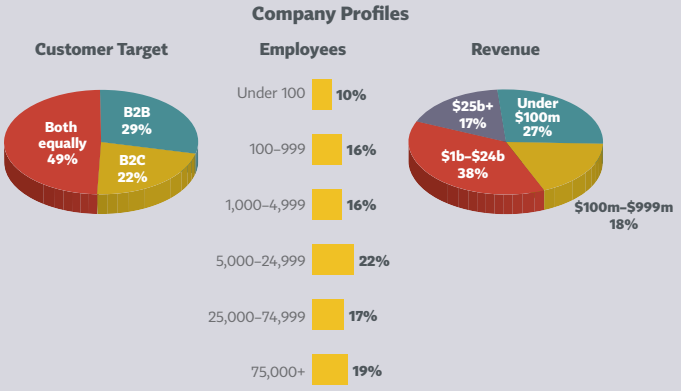
B2B firms also spend more per employee than B2C or blended firms. One likely explanation is the presence of the quintessential data processor in the B2B model. Processors must reassure clients of their data protection safeguards, in not only the contracts they sign but as well potentially by

continued from xi

EU. Canadians represent 14 percent of 2017 survey respondents, a legacy of the IAPP's early establishment in Canada.

Fewer respondents work in industries we call "regulated" industries such as health care, pharmaceuticals, financial services and insurance (35 percent) than in "unregulated" industries (46 percent). Breaking out the regulated industries, 23 percent represent financial services or insurance, while 12 percent are in health care or pharma. The bulk of respondents from unregulated industries work in the technology or telecommunications sectors (22 percent).

In terms of business models, revenues, and employee size, the 2017 survey — like last year's — reflects a balanced representation of the market. Nearly half



continued on xiii

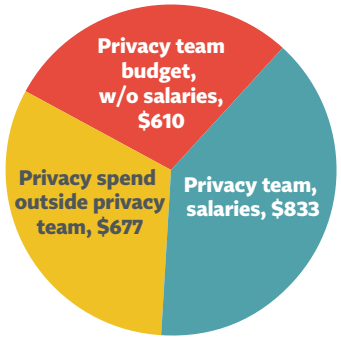
hosting their controller-clients for on-site inspections and acquiring privacy and security credentials like ISO 27001 or SOC 2. This requires strong and experienced privacy leadership and many well-trained privacy professionals working at least part-time on privacy throughout the firm.

Budgets are not likely to stop growing for next year, either, as 56 percent of respondents predict continued budget increases while 34 percent believe budgets will hold steady. It may not be enough, however. Overall, 67 percent believe budgets are insufficient – 48 percent saying they are "somewhat less than sufficient" and 19 percent claiming they are "much less than sufficient" for what is needed to meet risk and compliance demands.

TOTAL PRIVACY SPEND
2017 MEAN: $2.1M 2016 MEAN: $1.7M 2017 MEDIAN: $571,500 2016 MEDIAN: $415,000
Mean spending per employee*: 2017: $147 2016: $124

*Outliers over $1000 removed

Estimated Privacy Spend (000)
Base: Director or Higher



Far and away the largest budget item in 2017 – and thus the biggest reason for budget increases this year – is spending on people in the form of salary and travel (54 percent). The mean number of full-time privacy professionals on the privacy team is 6.8 in 2017 – up from 5.8 last year – while the mean number of privacy pros spending part of their time on the privacy team is 6.7 – up from 3.6 in 2016.

When we break out the number of full-time versus part-time privacy staff by industry or customer target, we see significant differences. Regulated firms have the largest privacy teams across the board – full and part-time in privacy and in other units – compared with unregulated firms or governmental organizations.

Organizations with B2C customer targets are considerably more likely to employ privacy professionals dedicated full-

continued from xii

(49 percent) work in industries that have a mix of B2B and B2C customer targets, with the other half weighted only slightly toward B2B (29 percent) over B2C (22 percent) models. Companies are evenly represented by annual revenues as well; the category with the most responses includes firms earning between $1 billion and $24 billion at 38 percent. Finally, regarding employee size, responses also come from companies across the size spectrum — 22 percent of respondents work for organizations employing 5,000-24,999 people, while 36 percent work for larger organizations (over 25,000) and 42 percent work for smaller ones (under 5,000).

We see a jump this year in the number of respondents holding manager-level positions, up to 27 percent from 20 percent in 2016, and a slight fall in those with a director-level title (17 percent in 2017 vs. 22 percent last year). This could be explained by the larger percentage of respondents from EU-headquartered organizations, where titles of "director and higher" are less likely. Indeed, those working for U.S.-based firms have a 12 percent chance of holding a "vice president" title compared to just 1 percent in the EU, and 21 percent of U.S. respondents are directors compared to just 15 percent in the EU.

time to privacy (12.7) than part-time (1.6) in their privacy programs, while B2B-focused firms are just the opposite. They are heavier with employees working on privacy only part time (11.2) on the privacy team, with just an average of 3.9 full-time employees in the privacy program. Blended B2B/B2C firms also have a balanced blend of full-time privacy (6.9) and part-time privacy-focused (5.3) staff working in the privacy program.

Employees Dedicated to Privacy
Base: Director and Higher

	2017		2016	
	Mean	Median	Mean	Median
Full-time privacy, in privacy program	6.8	2	5.8	3
Part-time privacy, in privacy program	6.7	1	3.6	1
Full-time privacy, in other units	5.2	0	4.4	0
Part-time privacy, in other units	15.6	3	16.6	3

Staff growth may be flatting out a bit after the ramp-up to GDPR this year, however. Although 28 percent predict they will need to hire more into the full-time privacy ranks, 68 percent believe they have enough full-time privacy staff for now, and 84 percent of this year's respondents have no need for additional staff working part-time on privacy.

GDPR Economics

The slight flattening of the hiring curve doesn't mean organizations are done spending on GDPR preparation. Far from it. Organizations expect to hire an average of more than two full-time staffers simply due to the GDPR's looming obligations, and spend a fair bit of money as well.

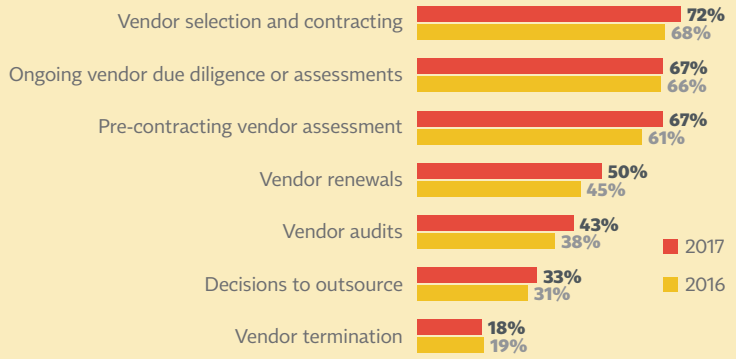
Of the survey respondents that fall under the GDPR (95 percent), more than 8 in 10 firms overall expect their organization will need to adapt their existing product and service offerings to comply. They anticipate spending upward of $5

Vendor management

Privacy risk mitigation involves allocating some risks to vendors through contracts. The GDPR requires this by mandating, principally in Article 28, that data controllers enter agreements with data processors that guarantee certain data protection safeguards. And standard contractual clauses remain a popular tool for cross-border data transfers, finding their way into many vendor agreements where personal data will be transferred between parties.

General counsel may not have familiarity with these legal provisions so it stands to reason that privacy professionals are often called upon to get involved in negotiating the privacy and security provisions in vendor agreements. Consistent with the 2016 results, 70 percent of respondents have a vendor management program. Among those with such a program, 72 percent

Involvement in Vendor Management



continued on xv

million for product adaptation and other expenses. Financial firms expect to be the biggest spenders, anticipating costs of over $4 million on product and service adaptation, and another $8.4 million on other GDPR spending.

Tying this in with other trends in the survey – including major growth in technology acquisition, training and awareness plans, and consumption of privacy-related content – one can surmise that winners in the GDPR economics game will be privacy tech developers, as well as those that conduct GPDR training and education (including attorneys and consultants).

Privacy professionals themselves should enjoy job security for the foreseeable future, especially if they invest in learning the GDPR.

Privacy leadership and the DPO

As part of GDPR compliance, 29 percent of respondents report their organization has made changes in reporting structures – 30 percent say this involved elevating the privacy leadership position, with an additional 15 percent reporting such changes are in the works.

Among those most likely to have elevated the privacy leader's role due to the GDPR are firms headquartered in the EU (38 percent) and the smallest firms (38 percent). Organizations profiting from B2B business models, as well as those in the health care and technology/telecom sectors, are also more likely than the overall total to have given the privacy leader more authority in light of the GDPR's requirements.

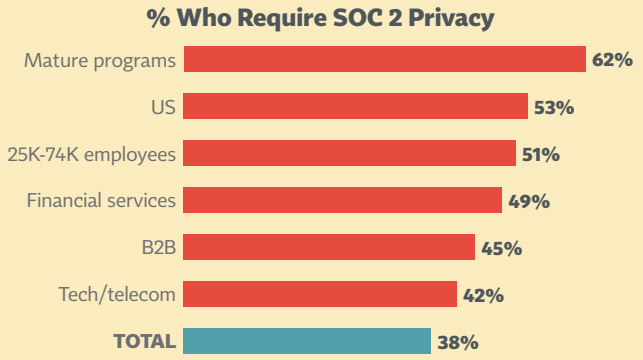
If the privacy lead is wearing two hats, it very likely is that of the data protection officer, a position mandated by Article 37 of the GDPR. Although 44 percent of respondents report their organization does not yet have that position, 32 percent report the privacy lead is filling the DPO role themselves.

Diving in deeper, we find that privacy leaders who are also DPOs often hold a CIPP/E (49 percent), and report that GDPR compliance is one of the top three reasons for their

continued from xiv

involve their privacy team in vendor selection and contracting, while 67 percent involve privacy in both pre-contracting vendor assessment as well as ongoing vendor due diligence.

Significantly, one in two privacy professionals look for ISO 27001 compliance from vendors, up from just 39 percent in 2016. Making a surprising move into second place are SOC 2 privacy credentials, with 38 percent requiring them compared to 32 percent in 2016. Drilling deeper into these statistics, we find that 62 percent of mature privacy programs require SOC 2 Privacy compliance, along with 53 percent of U.S.-based organizations and 51 percent of those with between 25,000 and 75,000 employees. SOC 2 is also popular among financial services (49 percent) and tech/telecom (42 percent) firms, as well as those favoring a B2B business model



organization's privacy program (74 percent). They are also highly likely to be integrated in their firm's ongoing activities (70 percent).

Key DPO Characteristics
Higher Than Average Results

BY CPO/DPO STATUS

	CPO Is Also DPO	CPO Is Not DPO
Works in unregulated firm	63%	45%
Works in tech firm	39%	30%
Works in B2B firm	46%	35%
Has CIPP/E	49%	12%
Firm transfers data from EU to US	73%	54%
Program is in early maturity stage	28%	15%
Top 3 Importance: Compliance with EU GDPR	74%	52%
Privacy involvement in ongoing activities: Throughout process	70%	50%

Anecdotally, the IAPP has seen a leveling-off of chief privacy officer roles. And yet the title, or something close to it, is still very much in circulation with 63 percent of privacy leaders using the term "privacy" in their title, and approximately half calling themselves "officers" (55 percent) or "chief" (45 percent). Far less common for the privacy lead are titles like "counsel" (19 percent), "director" (19 percent), "vice president" (16 percent), or even "global" (16 percent).

Shooting for the C-Suite or a VP title? The best bet is in the tech industry, in a mature privacy program, and with a company between 25,000 and 75,000 employees.

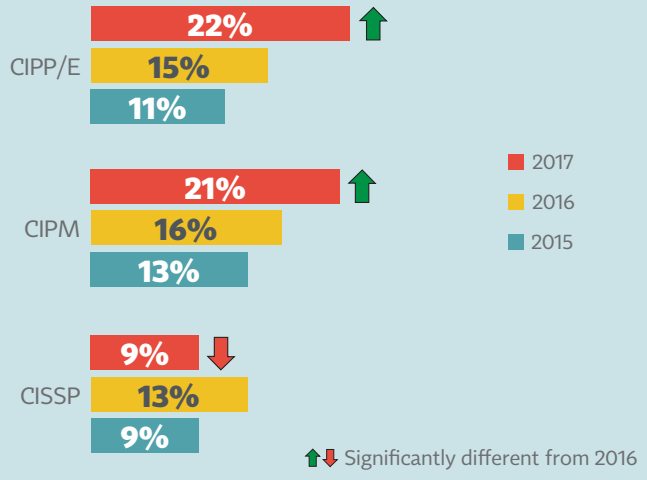
GDRP-Ready Credentials

As this report demonstrates in many ways, GDPR is driving privacy teams' compliance obligations and thus their need to understand the Regulation's responsibilities. It is also creating opportunities — for tech vendors, for privacy professionals, and for those who educate and train privacy professionals.

The IAPP has seen an explosion in the number of people taking the Certified Information Privacy Professional / Europe (CIPP/E) exam, which tests knowledge of the EU data protection regime including the forthcoming GDPR. Many are also taking the Certified Information Privacy Manager (CIPM) exam, which tests knowledge of privacy program development, implementation and ongoing management.

The IAPP recommends these credentials in combination for privacy professionals seeking to be "GDPR-Ready," especially for those seeking or being appointed to fill the DPO role.

Credentials and Degrees Held

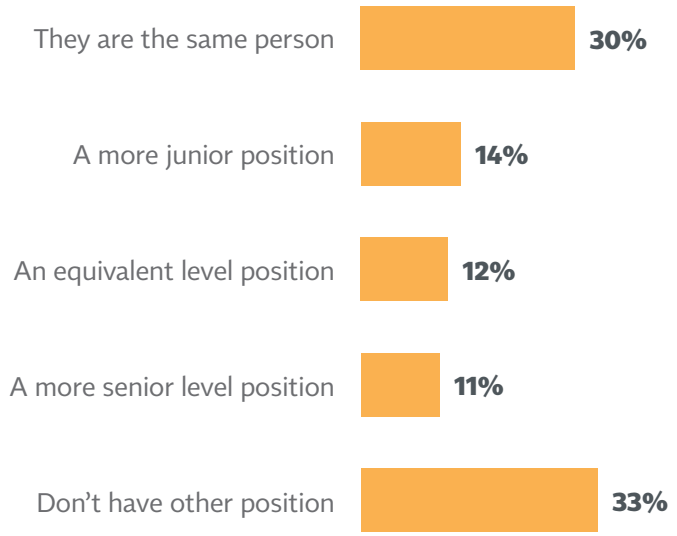


continued on xvii

Words and titles matter, of course, and this year reflects that the GDPR has not yet been able to bridge, entirely, the "privacy" versus "data protection" divide between U.S. and EU-headquartered firms. "Privacy" is used by 70 percent of U.S.-based privacy leaders, and only 43 percent of those working in the EU. Privacy leads in the EU are more likely than their American counterparts to use the term "data" in their title (37 percent in the EU compared to just 8 percent in the U.S.), and much less likely to hold a "vice president" title (3 percent in the EU vs. 20 percent in the U.S.).

Some firms are asking their CPO to serve the role of DPO, of course, with or without the added title. Such firms are most likely in unregulated industries and those with B2B business models, once again suggesting that such firms tend to appoint fewer but perhaps more educated or qualified personnel to privacy leadership roles and then ask more of them.

Privacy Leader Relative to Chief Privacy Counsel
Base: Director or Higher



continued from xvi

All the froth around the GDPR has stirred up a fair amount of interest in training and certifying DPOs. Indeed, supervisory authorities — many of whom have responsibility for consumer protection beyond privacy — have expressed some concern about the quality and credibility of the myriad GDPR-preparedness programs springing up in the EU.

The IAPP recommends asking the following questions when considering a GDPR training or credentialing program:

- Does the credentialing body follow ISO 17024 standards, and does it have independent accreditation from a third party?
- Does the credential require ongoing education?
- Is the credential based on real-world job requirements or simply a test of knowledge?
- Does the training simply teach you how to take the test?
- Does the exam assess experience and competence, or merely retention of knowledge?
- Is the credentialing body for profit or not-for-profit?
- Is the credential local, regional, or global in scope? How broadly is it recognized and understood?
- Does the credentialing body offer continuing education for the credential?
- Does the credentialing body offer connection to a broader professional community?

Nearly one in three privacy leaders (30 percent) is also filling the role of Chief Privacy Counsel. Unregulated firms, and those that use either a B2B or blended business model, are more likely than regulated firms and B2C firms to have their CPO serve as Chief Privacy Counsel. This corresponds with the slightly leaner full-time privacy staff reported in their privacy departments, suggesting that these organizations are more likely to have lawyers working in full-time privacy roles and completing myriad privacy tasks, thereby needing fewer overall headcount for the same number of legal and compliance tasks.

Although privacy leads are unlikely to simultaneously fill the Chief Information Security Officer role (just 12 percent do), overall 41 percent report they are on even par with the CISO in the corporate hierarchy while 32 percent are lower on the corporate ladder and 10 percent are senior to the CISO.

Firms headquartered in the EU, however, are more likely than those in the U.S. to double-up the CPO and CISO roles, or to have the CPO serve in a role senior to the CISO position.

GDPR stress points

Although privacy professionals reap the benefits of the GDPR in terms of staff and budget growth, and career opportunities, building compliant programs is not easy. The more time privacy pros have spent reading and interpreting the Regulation, it seems, the more they appreciate its complexity.

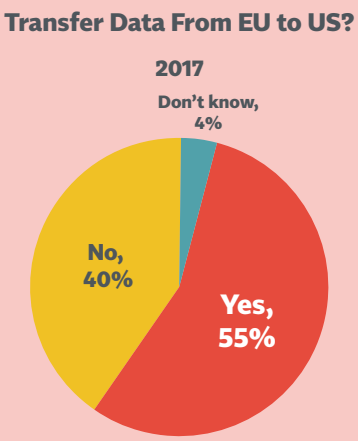
Both last year and this year, we asked respondents to rate the compliance difficulty of 12 GDPR requirements on a 10-point scale (with 10 being "extremely difficult"). Com-

Cross-border data transfer mechanisms

Personal data transfers between the EU and the U.S. implicate billions of dollars and euros in trade. Yet the EU Data Protection Directive — and soon, the GDPR — preclude such transfers in the absence of certain safeguards.

More than half of the IAPP-EY Privacy Governance Survey respondents (55 percent) report their organization transfers data from the EU to the U.S. Slicing the data more finely we find that the largest firms — 82 percent of organizations with revenue exceeding $25 billion and 75 percent of those with more than 25,000 employees — engage in EU-U.S. data transfers, along with 79 percent of EU-headquartered respondents.

Luckily, valid data transfer mechanisms can take many forms. These include government-level arrangements such as a formal declaration that the receiving organization's country has an "adequate" legal regime to protect data subjects' rights, or participation in bilateral programs like the U.S.-EU Privacy Shield Framework. They also include company-level tools like binding corporate rules and standard contractual clauses, and even derogations specific to individual data subjects and their relationship with the controller (e.g. consent, contract fulfillment, and the like). Certifications,

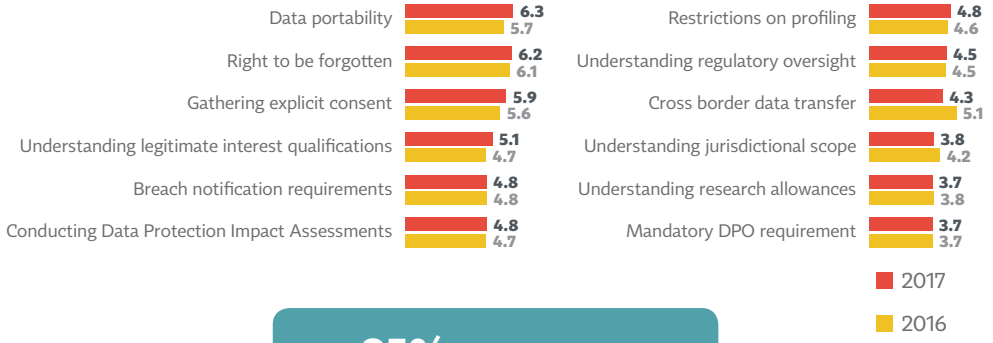


continued on xix

pared with last year, nearly every category received a higher difficulty rating. Data portability also rose in the ranks to become the top-rated, most-difficult compliance obligation – earning a 6.3 overall compared to 5.7 last year, and narrowly beating out the right to be forgotten (right of erasure). Privacy professionals also now see more complexity in the lawful basis obligations of Article 6; "gathering explicit consent" earned a 5.9 rating on the difficult scale, up from 5.6 last year, while "understanding legitimate interest" rose four tenths of a point in difficulty to 5.1 from 4.7.

Interestingly, cross-border data transfers did not seem to stump privacy professionals as much this year as last, earning a 4.3 difficult rating (down from 5.1 last year, where it was the fourth-rated concern overall). On the one hand, Privacy Shield, which was new last year, has settled into place in 2017. But on the other hand, the very popular standard contractual clauses have recently been called into question in the Irish High Court, setting up more uncertainty in the months and years to come.

GDPR Obligation Difficulty
(Mean Score on 0-10 Scale: 0=Not at All Difficult; 10=Extremely Difficult)



Over 95% of firms say they fall under the GDPR scope

continued from xviii

seals and codes of conduct are options under the GDPR but the market remains cool to them while awaiting guidelines — and approved providers.

The various tools present varying degrees of complexity and hardship. Standard contractual clauses may be the least time consuming and costly, which is why they have become far and away the most popular tool. Among all respondents, 88 percent rely on SCCs. When we factor out government, finance and health care organizations, the number climbs to 90 percent among those in the U.S. and 93 percent among EU respondents.

Recently, the Irish High Court signaled concerns about SCCs' validity under the EU Charter of Human Rights, questioning whether data exporters located in countries lacking adequacy status can rely on such private mechanisms to comply with EU data protection law.

Europe's highest court will soon have the question under review. The Court of Justice of the European Union is no stranger to such questions, having struck down the EU-U.S. bilateral cross border data transfer agreement known as "Safe Harbor" in October 2015. That decision spawned the Privacy Shield Program, which is popular among 47 percent of overall respondents — up a remarkable 13 percentage points from 2016 — and relied upon by 53 percent of EU-based organizations once government, finance, and health organizations are removed.

The Privacy Shield program is vulnerable, however, to the same challenges that brought down Safe Harbor and (potentially) SCCs. This leaves organizations relying

continued on xx

Different respondents feel different GDPR pain points, of course.

The largest firms – potentially concerned they are the most likely enforcement targets – reported higher than average difficulty ratings on four of the GPDR compliance requirements, including assigning a difficulty rating of 7.2 to "data portability," 5.5 to "restrictions on profiling," and 5.1 to "cross border data transfers."

Organizations headquartered in the U.S. also gave higher difficulty scores than the global average for several GDPR compliance obligations. U.S. firms struggle with the lawful basis requirements of explicit consent (6.3 difficulty rating) and legitimate interest (5.5).

The right to be forgotten also ranked high among U.S. firms, earning a 6.7 difficulty rating, as well as with financial firms, which assigned a 7.1 difficult score to the uniquely European privacy right.

Those privacy leaders who do not also serve as their employers' DPO gave high difficulty scores to many GDPR tasks, including an eye-catching 7.7 score to "gathering explicit consent." Other GDPR tasks that worry non-DPOs? Legitimate interest qualifications (5.9), breach notification requirements (5.7), regulatory oversight (5.7) and data protection impact assessments (5.6). They even reported a much higher than average concern with the DPO requirement itself (4.9).

GDPR readiness … and procrastination

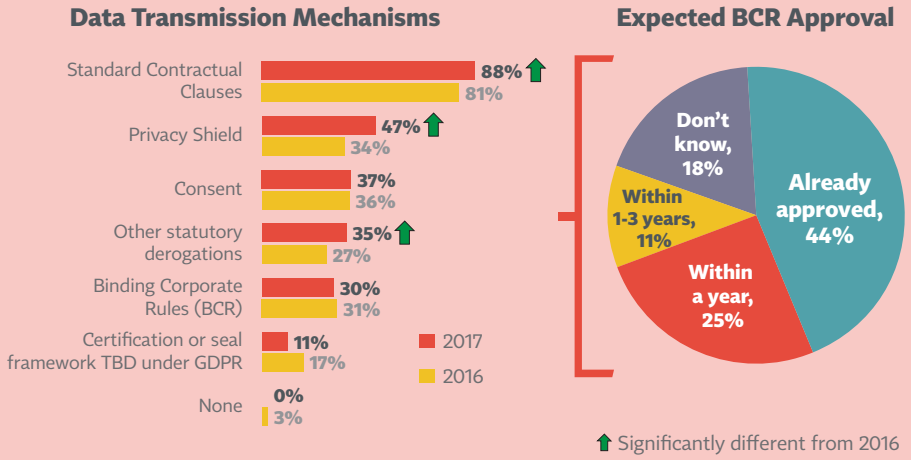
So, how will privacy professionals respond to the increasing GDPR-compliance pressure? Some are not yet sure.

continued from xix

on express consent from the data subject (37 percent) and increasingly other statutory derogations (35 percent overall, up from 27 percent in 2016). When we factor out government, health care, and finance respondents, and sort by geography, data subject consent is most popular among U.S.-based companies (41 percent).

Companies adapting to EU data protection law for the first time might do well to note that consent is significantly less popular among EU organizations; only 25 percent find this a reliable data export tool. Instead, they are more likely to use BCRs (38 percent) than their U.S. counterparts (23 percent).

BCRs are typically considered an option only for the wealthiest of firms with resources to fund the process and motivations to implement such programs globally. For those who are pursuing BCRs, the approval pipeline is solid with 69 percent reporting they are either already approved or expect to be within a year.



Although 8 in 10 firms expecting to fall under the GDPR's requirements have performed a gap analysis either internally or using an external group, only 57 percent of those firms have a plan for addressing the gaps.

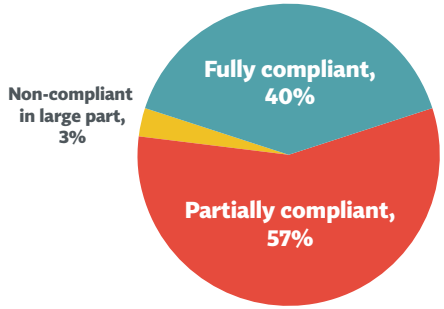
In fact, they are freely admitting they won't necessarily be ready by May 2018. Among all respondents, only 40 percent report they expect to be fully compliant by the deadline, while 57 percent overall expect to be only partially compliant. Interestingly, EU firms are more likely than U.S. firms to report only partial compliance expected (66 percent in the EU compared to 51 percent in the U.S.) and correspondingly less likely to expect full compliance (33 percent in the EU vs. 45 percent in the U.S.).

Firms that have already appointed a DPO are obviously compliance-minded already – 42 percent expect to meet the deadline, while 58 percent expect to be only partly there. Those who have NOT appointed a DPO will be scrambling, with a full 70 percent admitting they will at best be only partially compliant next May.

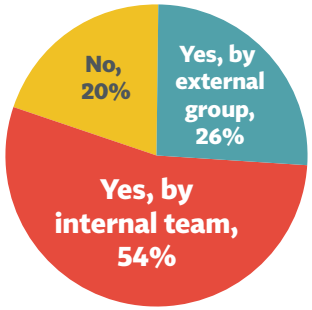
Yet, many are taking steps to meet the GDPR – including shopping for tech solutions.

Indeed, for privacy technology vendors, the GDPR presents huge opportunities. Whereas last year only 28 percent of survey respondents saw technology as the answer to their GDPR compliance concerns, this year 55 percent plan to invest in technology. In response to this massive growth in the privacy tech industry, the IAPP issued and now regularly updates the Privacy Tech Vendor Report, highlighting the major players in the exploding privacy technology industry.

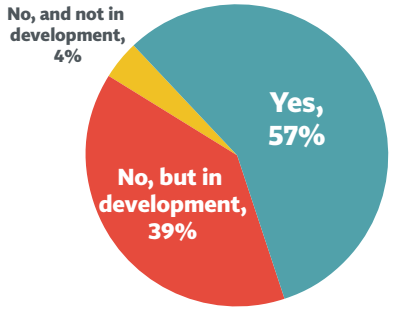
GDR Compliance Status in May 2018
(Base: Falls Under GDPR)



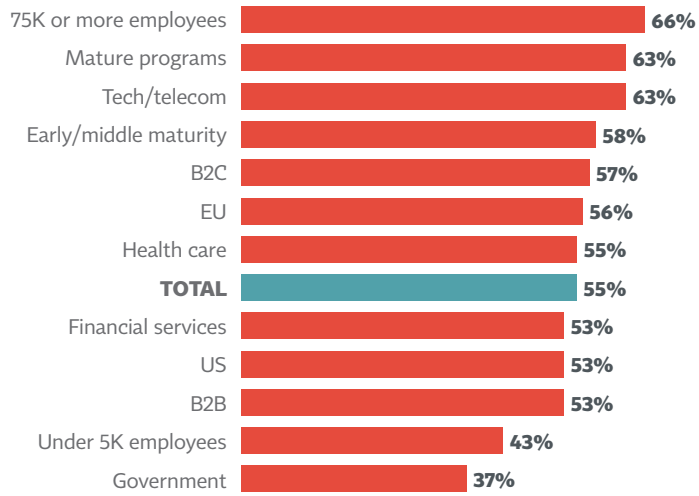
Had Gap Analysis Performed?
(Base: Falls Under GDPR)



Plan for Addressing Gaps?
(Base: Falls Under GDPR)



% Who Will Invest in Technology

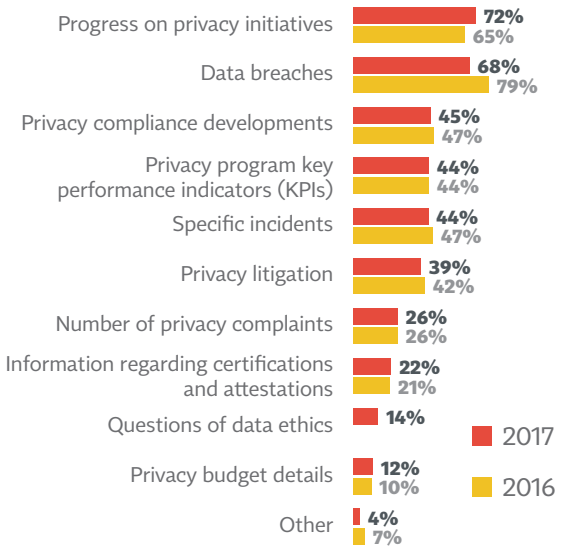


The best target markets for tech vendors are companies with 75,000 or more employees, 66 percent of which list "investing in technology" as a priority for GDPR preparation. Other targets could include organizations in the technology or telecommunications sector and those with mature privacy programs (63 percent). Least likely to rely on technology as a GDPR compliance solution are the smallest firms (under 5,000 employees) and those in the government sector.

In addition to buying tech solutions, organizations building toward GDPR compliance are also investing in training, creating new accountability frameworks, appointing one or more DPOs, and increasing privacy staff and budget. They are also more likely to seek privacy certifications for their employees, work with consultancies, and develop a new relationship with regulators.

They are less likely than last year to switch to a new law firm, or just sit on their hands doing nothing.

Specific Topics Reported
Base: Matters Reported to Board



Privacy Motivations

It will surprise no one that regulatory and legal compliance tops the list – for the third year – as respondents' highest privacy priority. Overall, 62 percent of organizations surveyed listed GDPR compliance specifically as a primary motivation for having a privacy program. This climbs to 75 percent among EU organization alone – and falls to only 50 percent where U.S. firms are concerned.

"Compliance" – with any privacy law — outpaces safeguarding against data breaches by 12 percentage points, with protecting reputation and brand coming in third. Indeed, 100 percent of health organizations responded that compliance was a top priority, assigning 81 percent to data breach risk reduction.

Meanwhile, tech firms are concerned with compliance, too – 89 percent – but are much more likely than other industries to hire privacy personnel for core business reasons such as meeting client expectations (84 percent), which outpaces even their concern about data breach avoidance (66 percent). Indeed, tech firms are also valuing privacy programs as a competitive differentiator (39 percent) as well as to increase data value (35 percent).

Privacy's importance within the firm can also be measured by how often and for what reason privacy issues are reported to the Board of Directors. In this year's survey, just as many respondents report visiting the Board with privacy issues (72 percent) as last year, even more often (topping 80 percent) for firms exceeding $100 million in annual revenue. This year, progress toward and status of privacy initiatives are the number one reported issue (72 percent), beating out data breaches, which were last year's top board topic.

What Privacy Pros Do

Privacy professionals plan programs, write policies, conduct training and awareness exercises … and go to a lot of meetings. Their program management functions include preparing privacy impact assessments, conducting privacy-related investigations, helping to develop and implement privacy controls, and addressing privacy by design in product development.

Privacy professionals are also called upon to assist with incident response, but consistent with the subtle trend toward valuing the privacy team for things other than data breach mitigation, incident response functions are slightly less prominent this year than last. Instead, privacy teams are directionally more likely this year to address privacy issues with existing products and services – possibly to retrofit core business drivers for GDPR compliance.

In terms of secondary responsibilities, GDPR compliance is important to more than half of respondents (59 percent), with one out of every two privacy teams working on "assuring proper cross-border transfer" duties this year. Consistent with the GDPR's record keeping requirements, data inventory and mapping tasks have leapt ahead in importance – 55 percent of privacy teams report engaging in this function, up from just 39 percent two years ago.

Privacy teams are consuming more privacy-related publications and subscriptions (up to 43 percent from 34 percent in 2015), and more privacy teams are spending time using privacy enhancing technology – a seven percentage increase over 2015. These trends bode well for industries that support privacy professionals by creating relevant tools and content.

Conclusion

The GDPR's seismic and lasting impact on the privacy profession and industry cannot be denied. Boards are taking notice, new jobs have been created, employees throughout the firm have privacy front of mind, and the privacy tech industry is exploding.

And while privacy is still seen by many organizations as an expensive necessity — something that must be proved through ISO and SOC credentials and promised in contract — it is also increasingly seen as key component of risk management and even a brand differentiator.

For privacy professionals, the GDPR offers promotions, lateral opportunities, and, at a minimum, job security for some time to come.


iapp

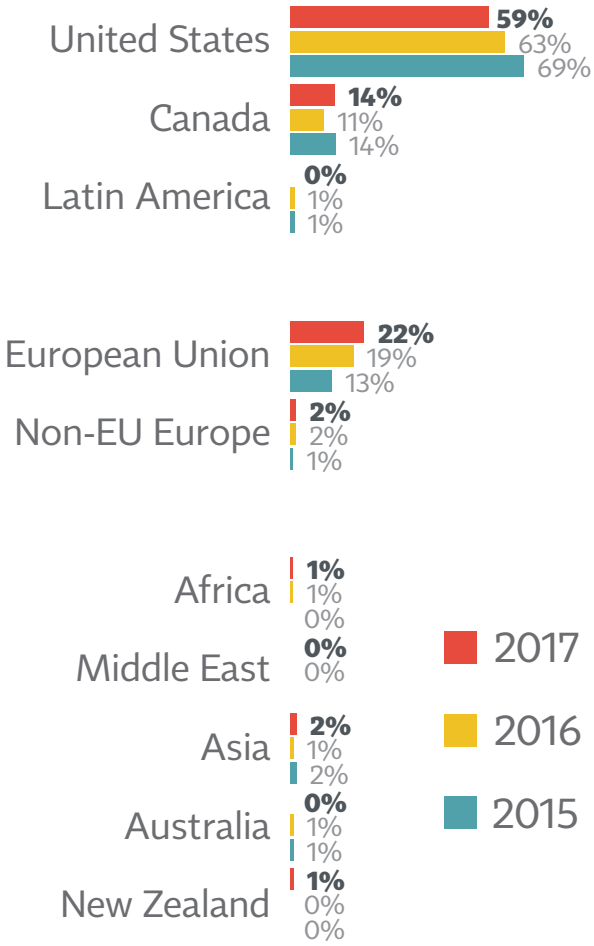

EY
Building a better
working world

Contents

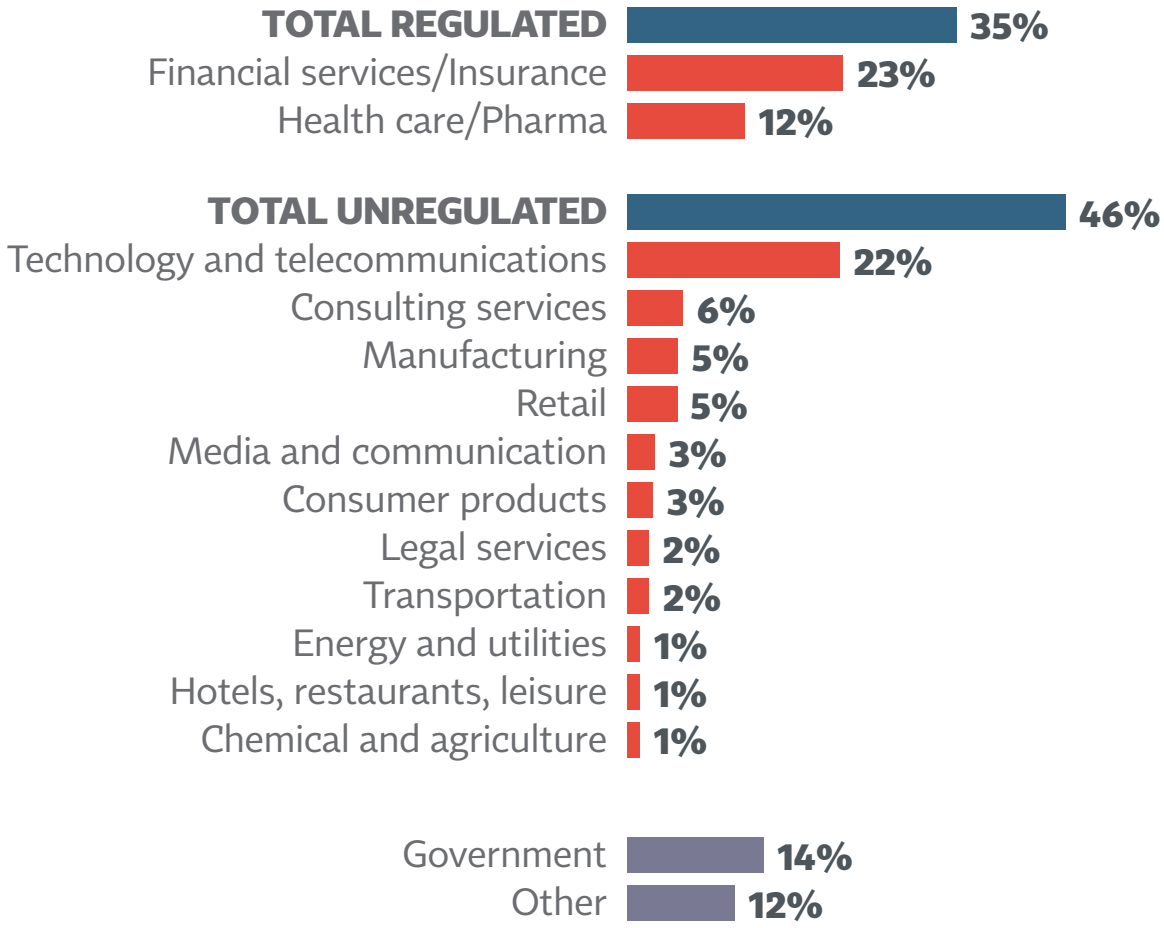
Although US-based professionals are still the majority, we've seen directional increases from the EU over time

Company Profiles

HQ Location



Industry



A6. What is the primary location of your company's headquarters?
A1. Which sector listed below best describes how your company would be classified?

US privacy pros are a bit more concentrated in tech than EU pros; employee size is also higher in the US

Background Characteristics:
Industry and Employee Size by Geography

BY GEOGRAPHY

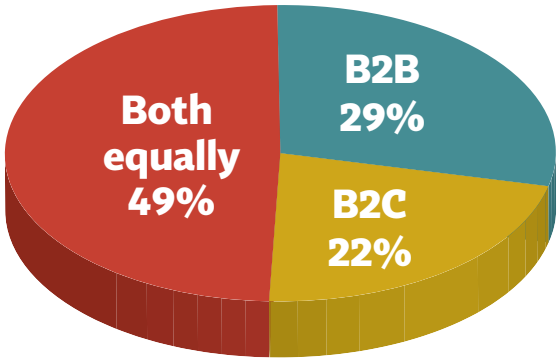
	US	EU
Financial services and insurance	25%	24%
Health care and pharmaceutical	12%	10%
Technology and telecommunications	26%	19%
Consulting services	6%	7%
Manufacturing	6%	6%
Retail	5%	8%
Media and communication	2%	7%
Consumer products	4%	2%
Legal services	2%	3%
Transportation	1%	2%
Energy and utilities	1%	4%
Hotels, restaurants, leisure	2%	1%
Chemical and agriculture	0%	3%
Government	13%	4%
Other	10%	9%
Mean Employees	**49,187**	**43,362**

Significantly higher than total

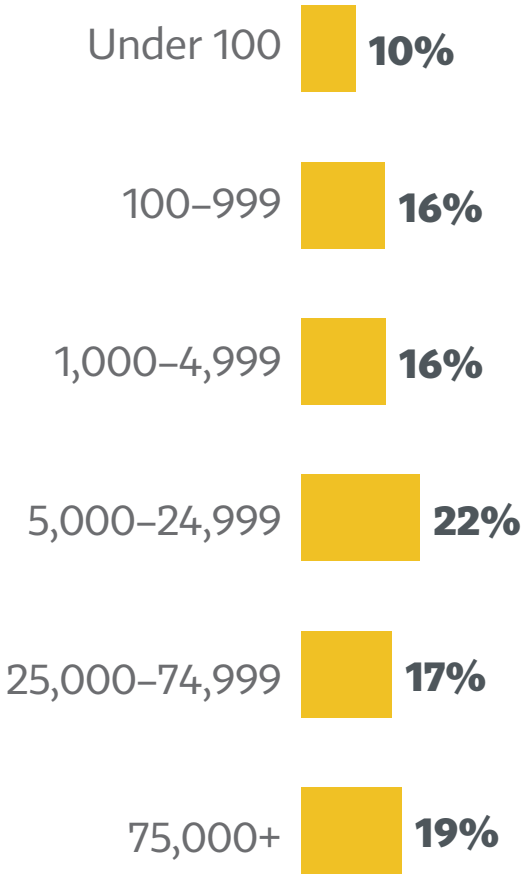
Respondents work at a wide array of firm types and sizes

Company Profiles

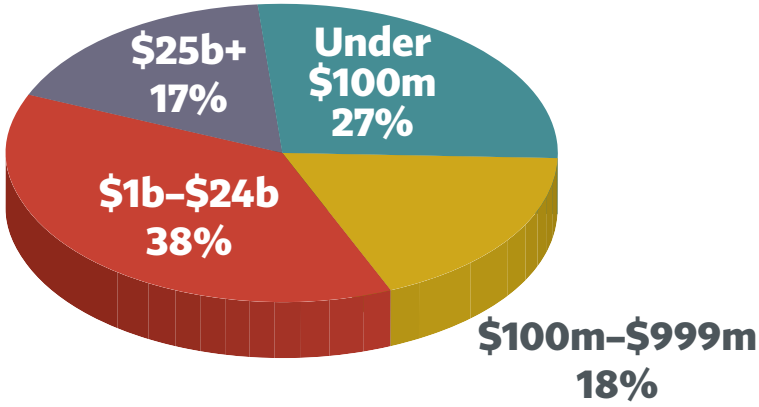
Customer Target



Employees

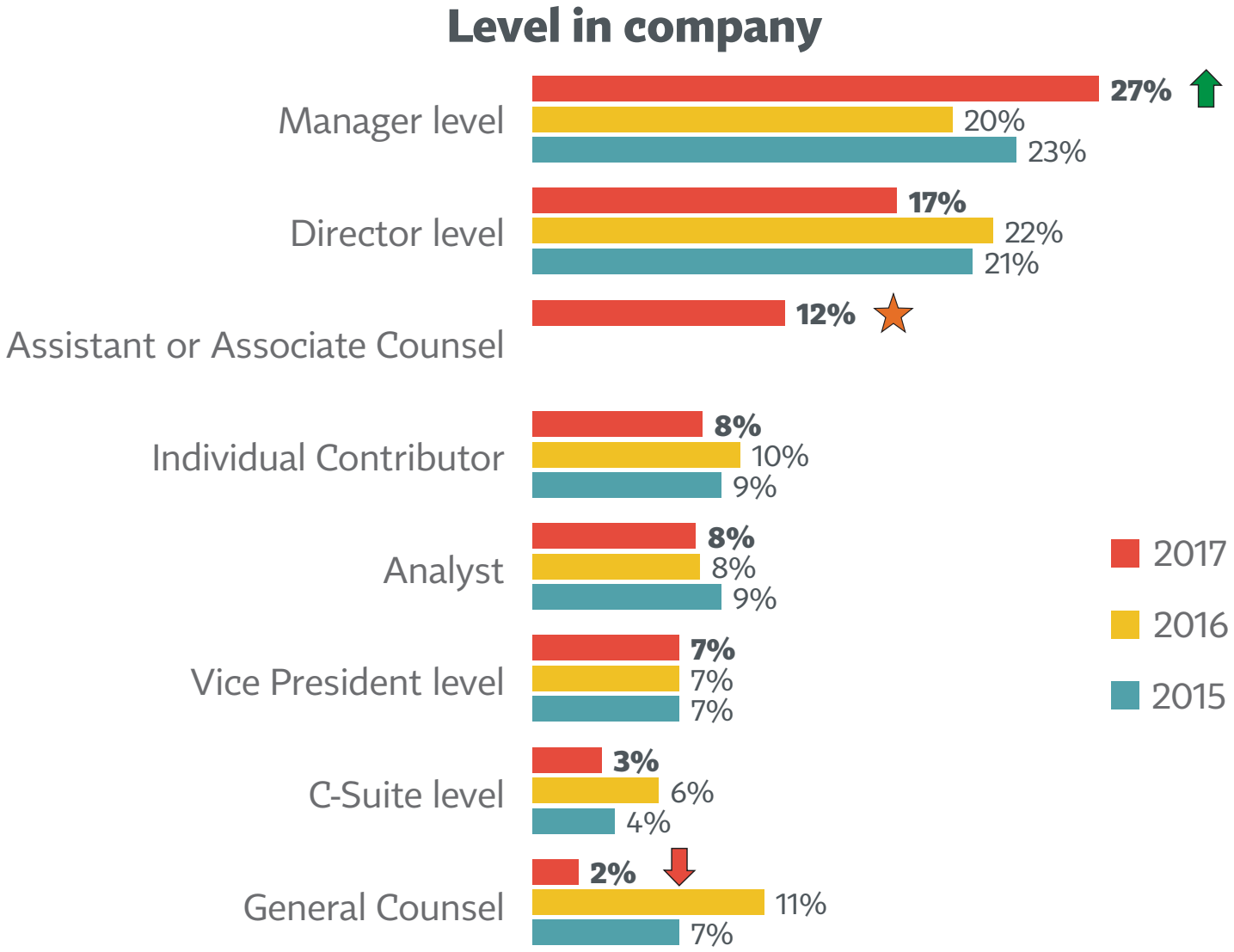


Revenue



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

The managerial level has emerged as the most common position for privacy professionals

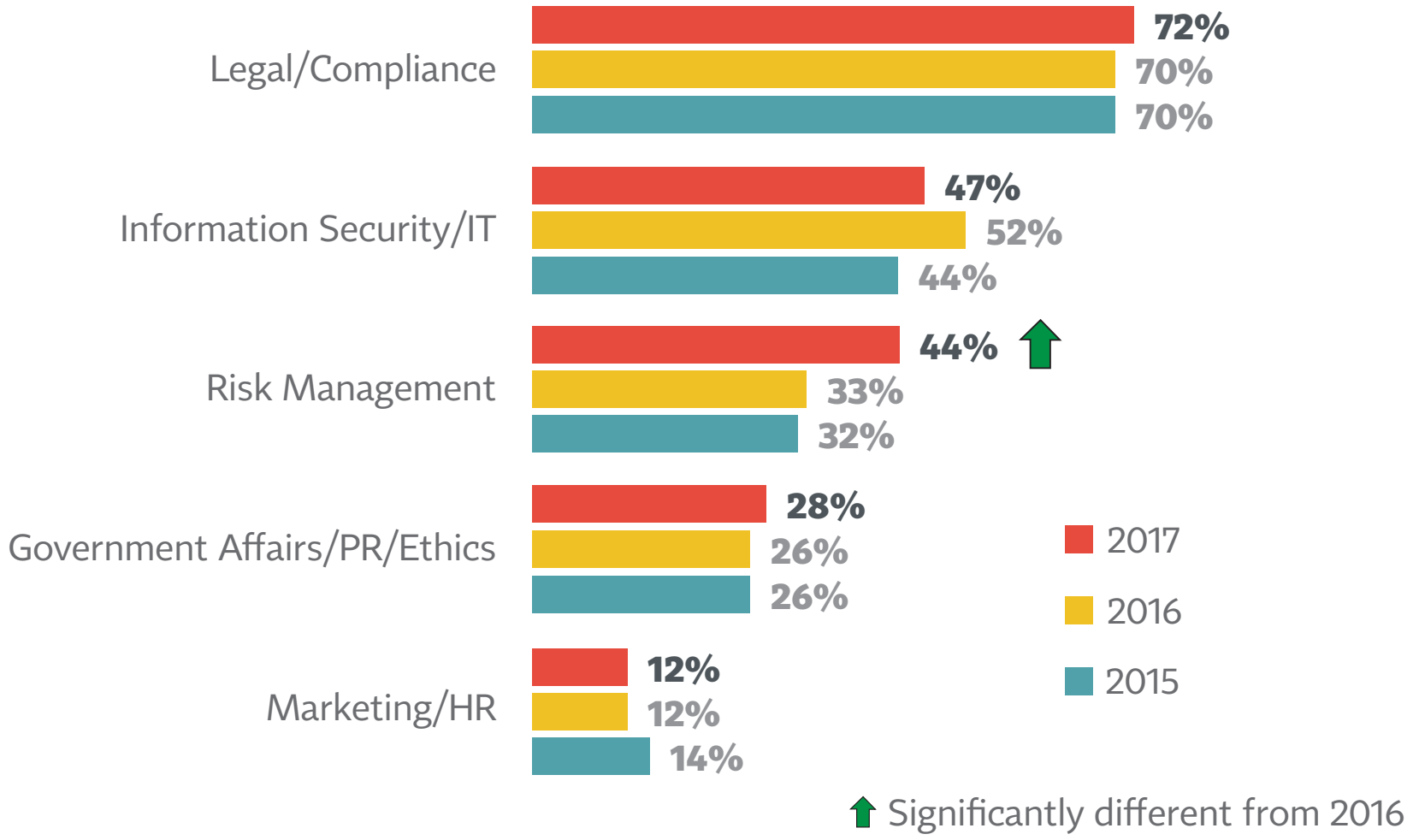


C1: Which of the following levels best describes your position in your company?

2017 sees an 11-point increase in the percent working in a risk-management function

- There's also been a directional increase for legal/compliance, the most common functional area by far

Main Functional Areas Work In

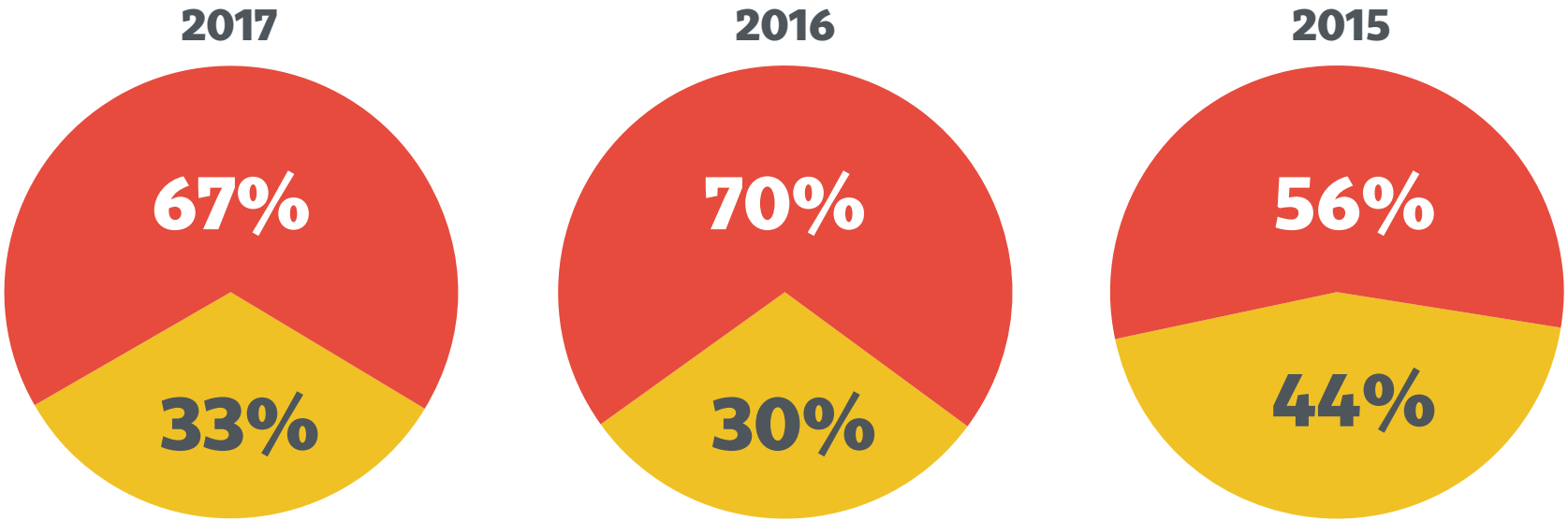


C3: Which of the following functions best describe the areas you regularly work in at your company?

On average, privacy professionals spend 70% of their work time on privacy responsibilities

- One-third say privacy makes up all time spent on their job, 100%; that's up directionally from 2016
- *Note*: Although only 33% say privacy is their entire job, a majority (52%) say privacy makes up 80% or more of their time, also higher than last year (44%)

Privacy Responsibility as % of Job



PRIVACY AS % OF JOB (MEAN)
2017: 70%
2016: 64%

100% of job

Less than 100% of job

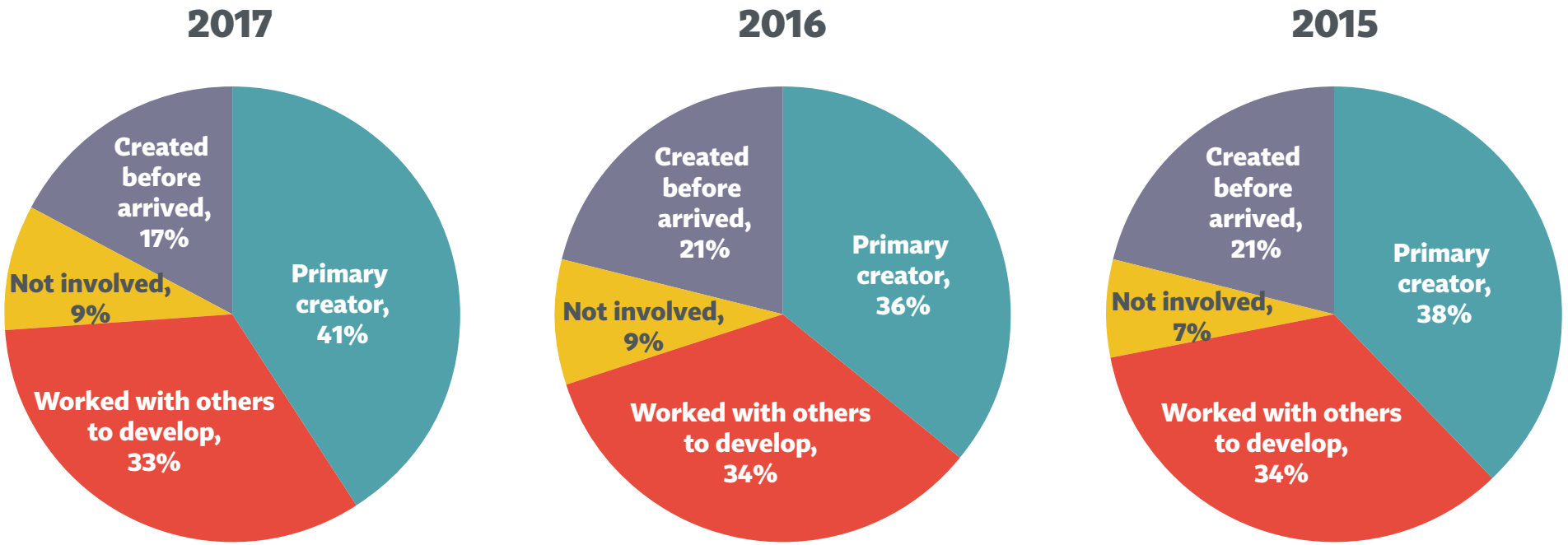
Note: Different question structure
2016/2017: D1: About what percentage of your work at your company is made up of privacy responsibilities?
2015: D1: Would you say that privacy responsibilities make up 100 percent of your work at your company or less than 100 percent?

This year's survey shows a directional increase in the percent saying they created their privacy program

- That percent is up 5 points since 2016 and is now at 41% of respondents

Respondent's Role in Developing Program

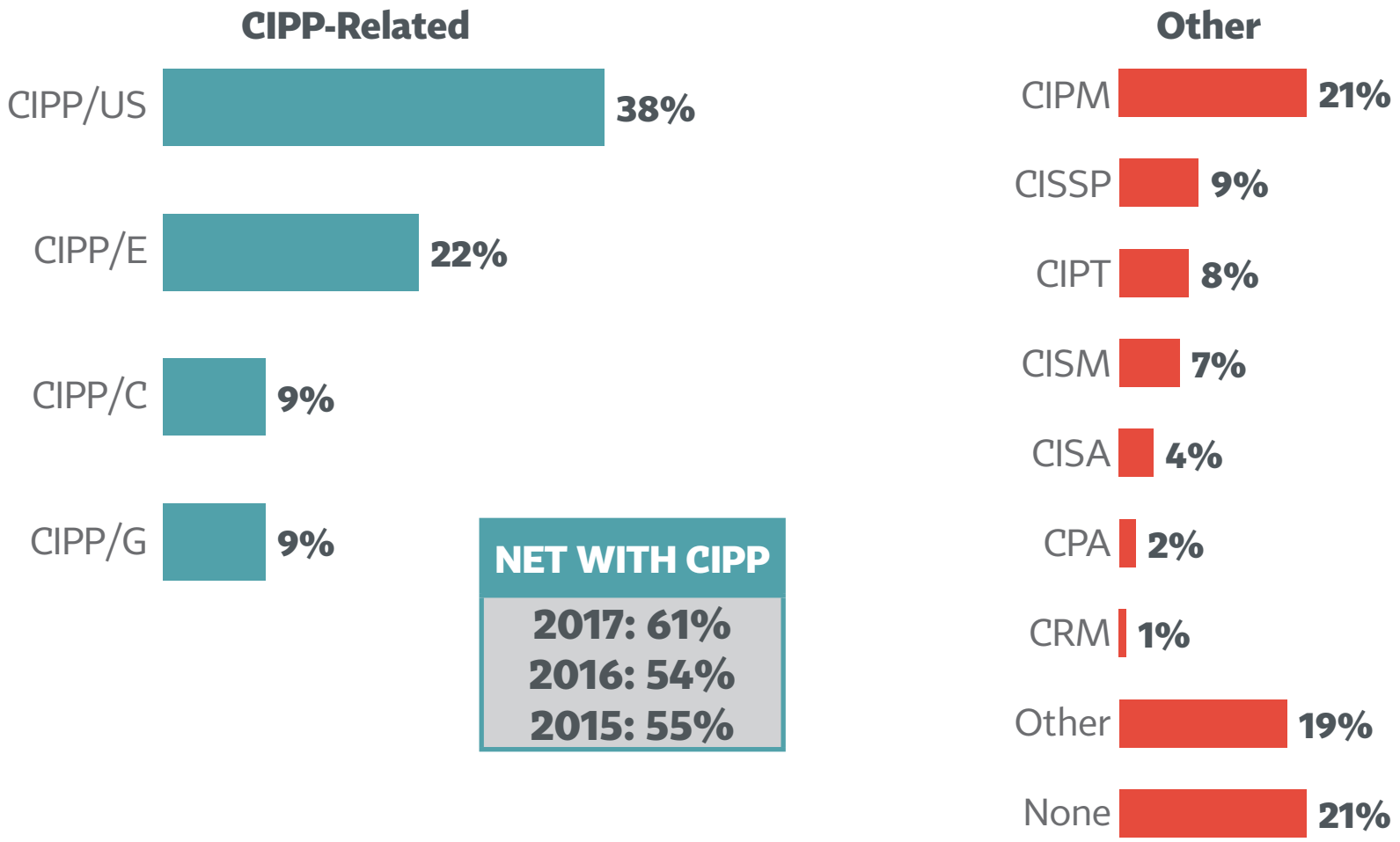
Base: Director or Higher



E3: Which of the following comes closest to describing your role in developing the privacy program of your company?

The proportion of privacy professionals with a CIPP is directionally higher than in 2016

Credentials and Degrees Held

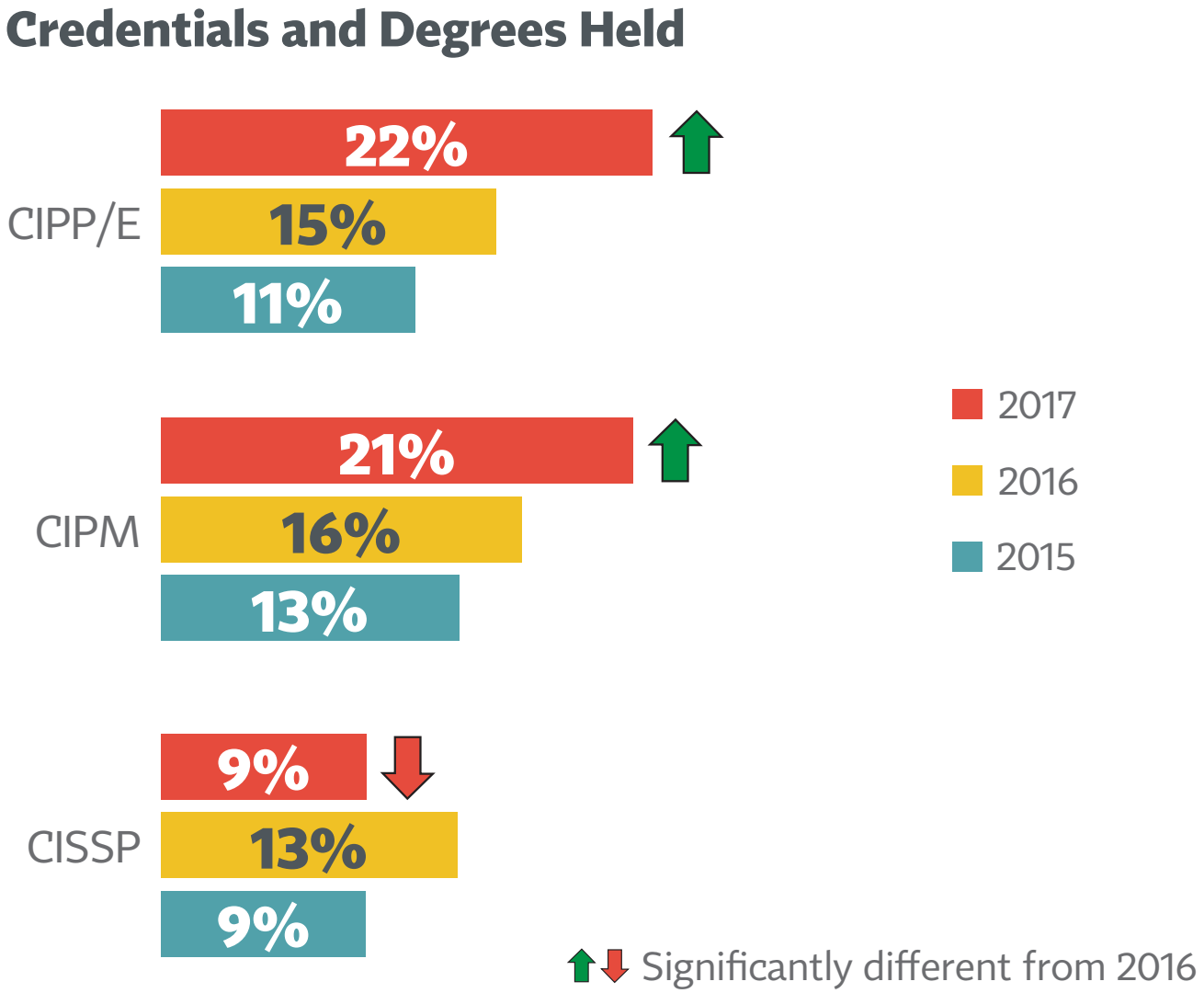


Most common mentions in "other" category: PMP, ISEB, JD, PCI, RHIA, FIP, CRISC, BCS

I1: Which certifications do you hold?

In particular, CIPP/E and CIPM have shown significant growth since last year

- The percent with CISSP has dropped 4 points, back to 2015 levels



I10: Which certifications do you hold?

US pros are also most likely to have CIPP in particular; most differences by industry are not significant

Certifications By Geography and Industry

BY GEOGRAPHY

	US	EU
CIPP	71%	55%
CIPM	23%	22%
CISSP	10%	7%
CIPT	10%	5%
CISM	7%	8%
CISA	4%	4%
CPA	3%	0%

BY INDUSTRY

	Gov't	Finance	Health	Tech
CIPP	58%	67%	65%	64%
CIPM	14%	21%	13%	26%
CISSP	6%	9%	9%	14%
CIPT	11%	8%	7%	13%
CISM	2%	10%	4%	7%
CISA	2%	5%	2%	4%
CPA	1%	1%	0%	7%

Significantly higher than total

Professionals in companies that are both B2B and B2C are most likely to spend all of their time on privacy

In-House Privacy Professionals:
Segments with Higher Than Average Results

BY INDUSTRY/CUSTOMER

	Finance	Health	Tech	B2B	B2C	Both
Respondent spends full-time privacy	34%	43%	28%	19%	36%	39%
Respondent spends less than full-time privacy	66%	57%	72%	81%	64%	61%
Worked with others to create	32%	13%	46%	36%	27%	33%

Significantly higher than total

As was the case in 2016, the largest firms are most likely to have dedicated privacy professionals

- As we also saw last year, those in less than mature privacy programs are most likely to have been involved in developing the program

In-House Privacy Professionals:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Respondent spends full-time privacy	16%	39%	45%	48%
Respondent less than full-time privacy	84%	61%	55%	52%
Primary Creator	53%	33%	46%	11%

BY PRIVACY LIFESTAGE

	Early/Middle	Mature
Respondent involved in creating program	80%	59%

Significantly higher than total

As in 2016, CIPx certification is highest in the largest firms and in firms with "mature" privacy programs

- Professionals in the smallest firms are especially likely to be involved in records management and internal audit; those in less mature firms are more likely to work in corporate ethics or compliance

Background Characteristics:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
CIPx certification	57%	72%	76%	80%
Vice President	5%	7%	15%	5%
Consulting	15%	7%	6%	8%
Records mgmt.	27%	12%	20%	19%
Internal audit	21%	10%	11%	11%

BY PRIVACY LIFESTAGE

	Early/Middle	Mature
CIPx certification	71%	79%
C-Suite, EVP, SVP, VP	39%	46%
Legal	64%	46%
Corporate ethics	27%	19%
Compliance	51%	67%

Significantly higher than total

Contents

2017 sees directional increases in the size of privacy program staff, full-time and part-time

- The average firm has more than 13 privacy professionals in the privacy program itself and additional 21 privacy pros in other units

Employees Dedicated to Privacy
Base: Director and Higher

	2017		2016	
	Mean	Median	Mean	Median
Full-time privacy, in privacy program	6.8	2	5.8	3
Part-time privacy, in privacy program	6.7	1	3.6	1
Full-time privacy, in other units	5.2	0	4.4	0
Part-time privacy, in other units	15.6	3	16.6	3

Outliers over 999 removed

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

As in 2016, regulated organizations tend to have more full-time privacy professionals than average

Mean Privacy Employee Size

Base: Director or Higher

	INDUSTRY		CUSTOMER TARGET		
	Regulated	Unregulated	B2B	B2C	Both
Full-time privacy, in privacy program	10.2	4.3	3.9	12.7	6.9
Part-time privacy, in privacy program	11.6	3.1	11.2	1.7	5.3
Full-time privacy, in other units	9.6	2.0	0.6	1.9	9.3
Part-time privacy, in other units	17.3	16.9	6.4	12.5	22.6

Significantly higher than total

Naturally, we see a direct relationship between overall firm employee size and privacy staff size

Mean Privacy Employee Size
Base: Director or Higher

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+*
Full-time privacy, in privacy program	1.5	3.2	10.8	20.7
Part-time privacy, in privacy program	1.2	2.1	2.8	34.1
Full-time privacy, in other units	0.5	0.8	5.1	24.7
Part-time privacy, in other units	2.0	5.0	25.0	56.3

* Small sample size Significantly higher than total

Privacy staffs are also larger in firms with the highest company revenue levels

Mean Privacy Employee Size
Base: Director or Higher

BY COMPANY REVENUE

	Under $100 million	$100–$999 million	$1–$24 billion	$25 billion or more*
Full-time privacy, in privacy program	1.5	5.8	5.6	18.5
Part-time privacy, in privacy program	1.8	0.8	9.4	12.7
Full-time privacy, in other units	4.9	0.8	5.6	10.3
Part-time privacy, in other units	6.9	2.5	10.3	56.7

* Small sample size

Significantly different than total

We see directional increases since 2016 in the percent saying privacy staff won't change in the coming year

- Accompanying that are directional decreases in the percent saying staff will increase—perhaps not surprising, given the increases we've seen from 2016 to 2017

Expected Employee Change in Coming Year

Base: Director or Higher

	% Saying Increase		% Saying Decrease		% Saying Stay the Same		Net % Change	
	2017	2016	**2017**	2016	**2017**	2016	**2017**	2016
Full-time privacy, in privacy program	**28%**	37%	**4%**	2%	**68%**	61%	**+13%**	+11%
Part-time privacy, in privacy program	**13%**	25%	**3%**	1%	**84%**	75%	**+6%**	+7%
Full-time privacy, in other units	**18%**	24%	**2%**	0%	**80%**	76%	**+5%**	+8%
Part-time privacy, in other units	**38%**	39%	**3%**	2%	**59%**	60%	**+12%**	+11%

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.

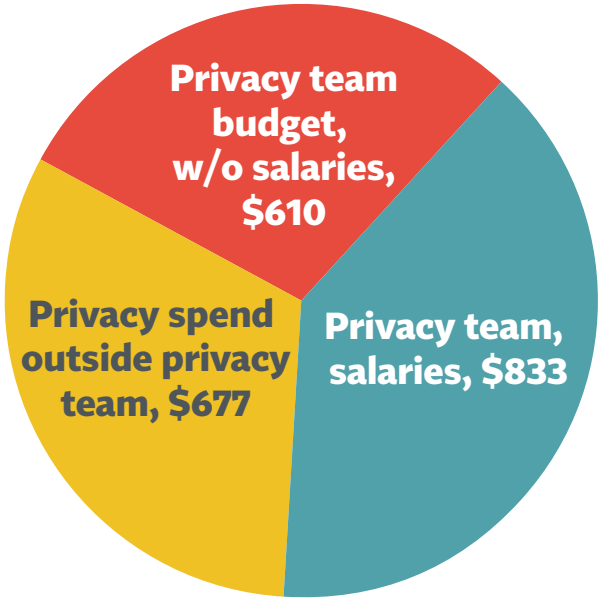
Along with privacy staff increases since last year, we see an increase in privacy budgets as well

- Average privacy spending outside of salaries has gone from $457K in 2016 to $610K today
- Overall privacy spend has also increased appreciably, from $1.7 million to $2.1 million

TOTAL PRIVACY SPEND
2017 MEAN: $2.1M 2016 MEAN: $1.7M 2017 MEDIAN: $571,500 2016 MEDIAN: $415,000
Mean spending per employee*: 2017: $147 2016: $124

*Outliers over $1000 removed

Estimated Privacy Spend (000)
Base: Director or Higher



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

Privacy budgets increase dramatically once one reaches the 25K employee level

Estimated Privacy Spend
Base: Director or Higher

BY EMPLOYEE SIZE

	Under 5K	5–24.9K	25–74.9K	75K+
Privacy Team Budget, w/o Salaries (000)	$143	$177	$1,261	$1,587
Privacy Team Salaries (000)	$267	$428	$1,025	$2,701
Spend Outside Privacy Team (000)	$246	$136	$494	$2,927
Total Privacy Spend (000)	$655	$740	$2,779	$7,215
Privacy Spend per Employee	$312	$80	$72	$49

Significantly different than total

As expected, privacy budgets are highest among companies with the most revenue generally

Estimated Privacy Spend
Base: Director or Higher

BY COMPANY REVENUE

	Under $100 million*	$100–$999 million*	$1–$24 billion	$25 billion or more*
Privacy Team Budget, w/o Salaries (000)	$226	$128	$676	$1,527
Privacy Team Salaries (000)	$224	$259	$769	$2,508
Spend Outside Privacy Team (000)	$90	$47	$633	$2,307
Total Privacy Spend (000)	$541	$434	$2,078	$6,342
Privacy Spend per Employee	$312	$221	$95	$84

* Small sample size

Significantly higher than total

We don't see appreciable differences in spend by customer target or industry category

Estimated Privacy Spend
Base: Director or Higher

	BY INDUSTRY CATEGORY		BY CUSTOMER TARGET		
	Regulated	Unregulated	B2B	B2C	Both
Privacy Team Budget, w/o Salaries	$675	$660	$399	$487	$791
Privacy Team Salaries	$981	$786	$605	$1,197	$869
Spend Outside Privacy Team	$435	$899	$521	$203	$933
Total Privacy Spend (Mean)	$2,092	$2,344	$1,524	$1,887	$2,593
Privacy Spend per Employee	$141	$142	$134	$186	$142

Spending has increased among all firm size segments, except firms with 5-24K employees

Estimated Privacy Spend
Base: Director or Higher

BY EMPLOYEE SIZE

	<5K		5–24.9K		25–74.9K		75K+	
	2016	2017	2016	2017	2016	2017	2016	2017
Privacy Team Budget, w/o Salaries (000)	$175	$143	$531	$177	$448	$1,261	$929	$1,587
Privacy Team Salaries (000)	$211	$267	$866	$428	$495	$1,025	$980	$2,701
Spend Outside Privacy Team (000)	$82	$246	$337	$136	$755	$494	$2,338	$2,927
Total Privacy Spend (000)	$478	$655	$1,734	$740	$1,698	$2,779	$4,248	$7,215
Privacy Spend per Employee	$282	$312	$92	$80	$38	$72	$28	$49

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

Similarly, spending has increased in all revenue segments, except $100-$999M firms

Estimated Privacy Spend
Base: Director or Higher

BY COMPANY REVENUE

	Under $100 million*		$100–$999 million*		$1–$24 billion		$25 billion or more*	
	2016	2017	2016	2017	2016	2017	2016	2017
Privacy Team Budget, w/o Salaries (000)	$64	$226	$98	$128	$743	$676	$750	$1,527
Privacy Team Salaries (000)	$206	$224	$360	$259	$600	$769	$1,470	$2,508
Spend Outside Privacy Team (000)	$61	$90	$155	$47	$716	$633	$2,030	$2,307
Total Privacy Spend (000)	$331	$541	$614	$434	$2,059	$2,078	$4,251	$6,342
Privacy Spend per Employee	$195	$312	$192	$221	$117	$95	$46	$84

* Small sample size

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

Spending has been relatively flat for regulated firms, while unregulated orgs have seen a jump

Estimated Privacy Spend
Base: Director or Higher

BY INDUSTRY CATEGORY

	Regulated		Un-regulated	
	2016	2017	2016	2017
Privacy Team Budget, w/o Salaries (000)	$669	$675	$349	$660
Privacy Team Salaries (000)	$664	$981	$620	$786
Spend Outside Privacy Team (000)	$779	$435	$728	$899
Total Privacy Spend (000)	$2,112	$2,091	$1,697	$2,344
Privacy Spend per Employee	$264	$585	$149	$142

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

Firms with a B2B focus, a B2C focus, or both all report higher privacy spending vs. last year

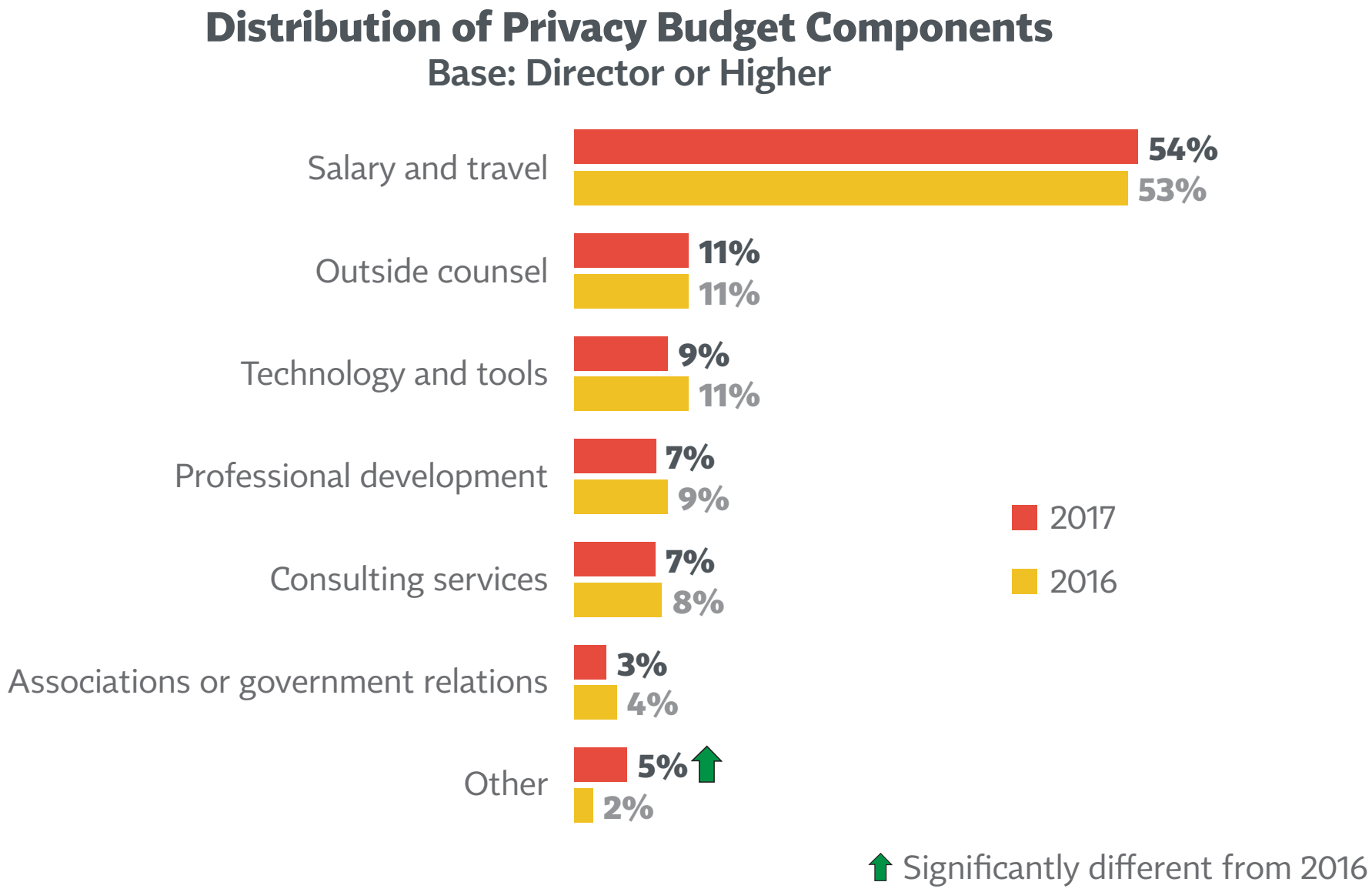
Estimated Privacy Spend
Base: Director or Higher

BY CUSTOMER TARGET

	B2B		B2C		Both	
	2016	2017	2016	2017	2016	2017
Privacy Team Budget, w/o Salaries (000)	$512	$399	$196	$487	$541	$791
Privacy Team Salaries (000)	$387	$605	$599	$1,197	$700	$869
Spend Outside Privacy Team (000)	$432	$521	$327	$203	$918	$933
Total Privacy Spend (000)	$1,330	$1,524	$1,122	$1,887	$2,158	$2,593
Privacy Spend per Employee	$161	$134	$126	$186	$104	$142

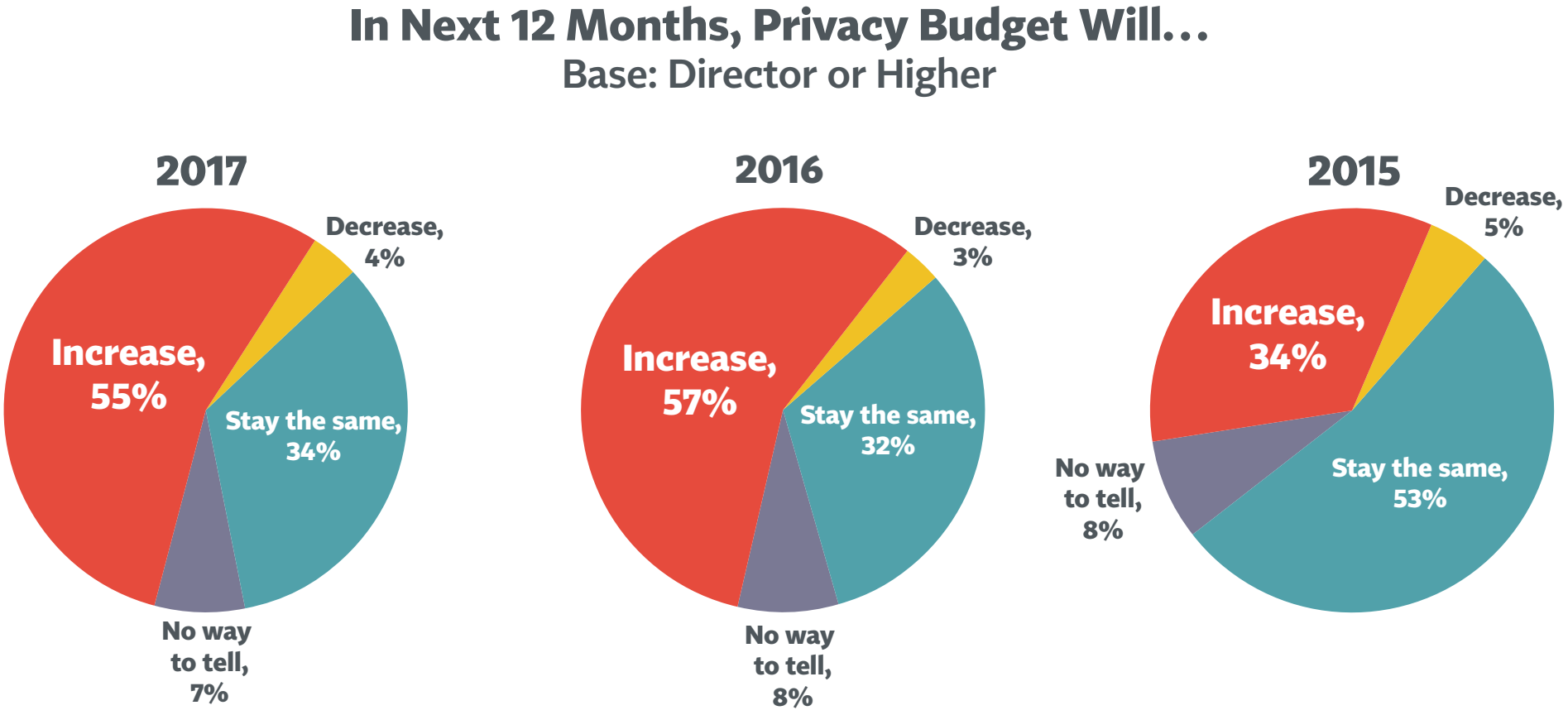
F4: And what is the total privacy spend for your company in each of the following categories?

There's been little change in the proportion of privacy budget that's allocated to salaries



F7: What percent of your company's total privacy budget is allocated to each of the following components?

Similar to what we saw with employees, we see a slight increase in those saying budgets will not change



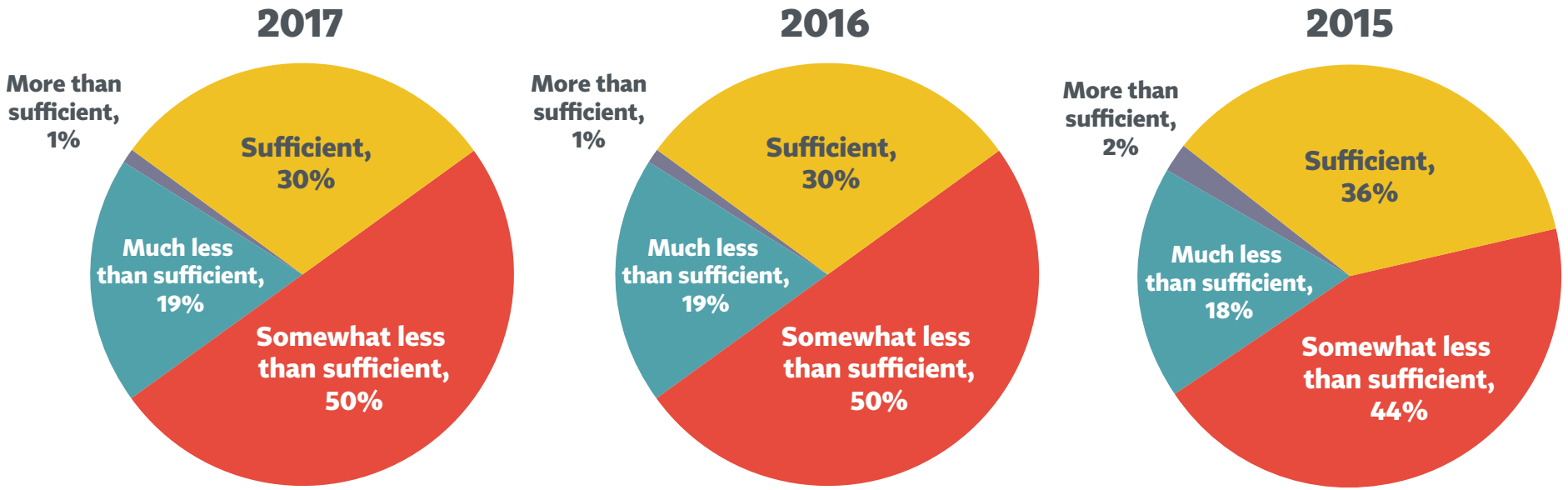
F5: In the next 12 months, you expect your company's privacy budget will …

There's been little change in the perceived sufficiency of privacy budgets

- Overall, 67% feel budgets are insufficient, comparable to 69% in 2016

Privacy Budget Is…

Base: Director or Higher



NET LESS THAN SUFFICIENT
2017: 67%
2016: 69%
2015: 62%

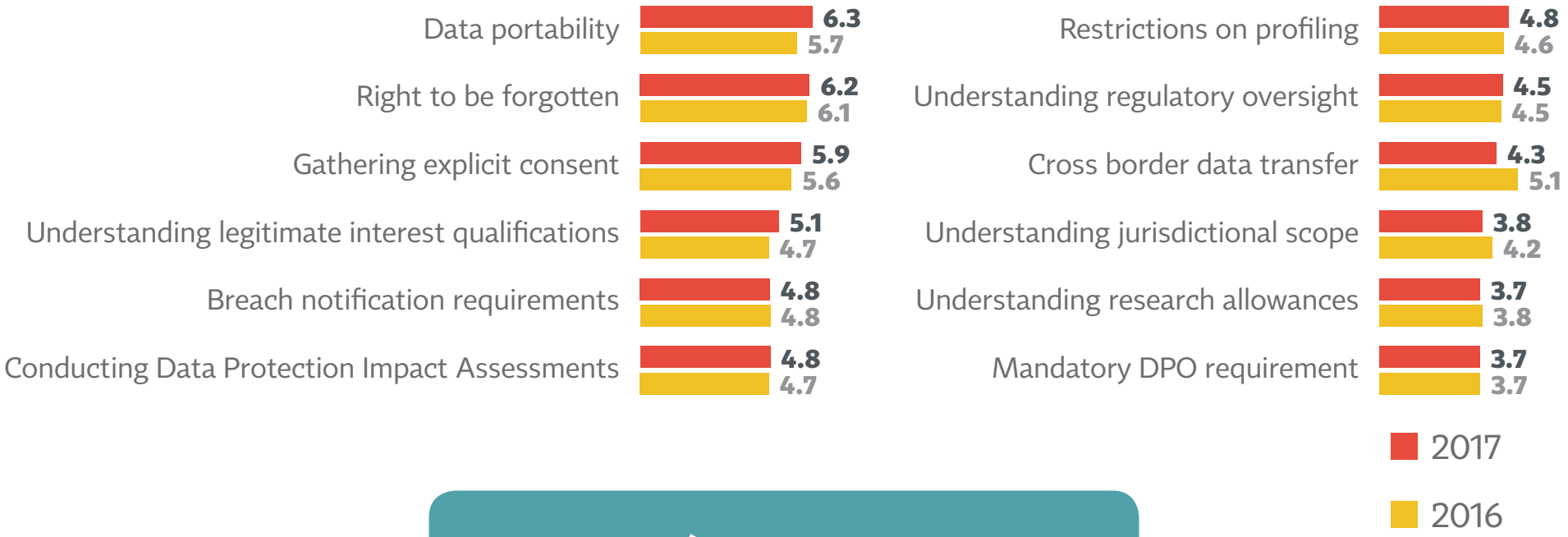
F6: In your opinion, your company's privacy budget is … to meet your privacy obligations

Contents

Nearly all firms say they fall under the scope of GDPR

- In addition, two of the top three perceived GDPR difficulties are now seen as even more difficult: data portability and gathering explicit consent

GDPR Obligation Difficulty
(Mean Score on 0-10 Scale: 0=Not at All Difficult; 10=Extremely Difficult)



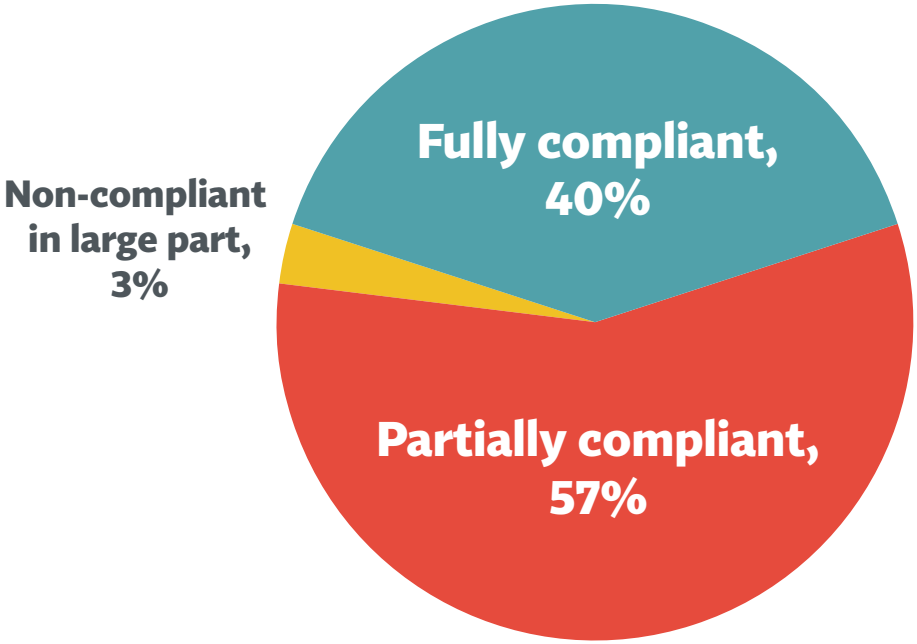
Over 95% of firms say they fall under the GDPR scope

J6: Does your organization fall under the scope of the General Data Protection Regulation (GDPR)?
J7: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

Only 4 in 10 affected firms say they'll be fully compliant by the GDPR launch date next year

- About 6 in 10 say they'll be partially compliant

GDPR Compliance Status in May 2018
(Base: Falls Under GDPR)



J16: All things considered, when the GDPR comes into force in May 2018, will your company be...

Large-revenue firms give higher than average "difficulty" ratings to 4 GDPR requirements, led by data portability

GDPR Obligation Difficulty: Higher Than Average Concerns

(Mean Score on 0–10 Scale: 0 = Not at All Difficult; 10 = Extremely Difficult)

Revenue $25B+:
Data Portability (7.2)

Revenue $25B+:
Restrictions on Profiling (5.5)

Revenue $25B+:
Cross Border Data Transfer (5.1)

Revenue $25B+:
Understanding Research Allowances (4.4)

J7: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

US firms give higher difficulty ratings to several needs, including explicit consent and right to be forgotten

GDPR Obligation Difficulty: Higher Than Average Concerns

(Mean Score on 0–10 Scale: 0 = Not at All Difficult; 10 = Extremely Difficult)

US: Right to be Forgotten (6.7)

US: Gathering Explicit Consent (6.3)

US: Understanding Legitimate Interest Qualification (5.5)

US: Understanding Regulatory Oversight (4.8)

US: Cross Border Data Transfer (4.6)

US: Mandatory DPO (4.3)

J7: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

Financial firms are more concerned about right to be forgotten; health care about understanding allowances

GDPR Obligation Difficulty: Higher Than Average Concerns

(Mean Score on 0–10 Scale: 0 = Not at All Difficult; 10 = Extremely Difficult)

Financial Services: Right to be Forgotten (7.1)

Financial Services: Restrictions on Profiling (5.3)

Health Care: Understanding Research Allowances (5.1)

J7: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

Less mature privacy programs give higher difficulty scores to explicit consent and PIAs

GDPR Obligation Difficulty: Higher Than Average Concerns

(Mean Score on 0–10 Scale: 0 = Not at All Difficult; 10 = Extremely Difficult)

Early/Middle Maturity:
Gathering Explicit Consent (6.5)

Early/Middle Maturity:
Conducting Data Protection Impact Assessments (5.3)

J7: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

Privacy leaders who are NOT DPOs rate difficulties higher, with explicit consent at the top

GDPR Obligation Difficulty: Higher Than Average Concerns

(Mean Score on 0–10 Scale: 0 = Not at All Difficult; 10 = Extremely Difficult)

Privacy Lead Is Not DPO: Gathering Explicit Consent (7.7)

Privacy Lead Is Not DPO: Understanding Legitimate Interest Qualifications (5.9)

Privacy Lead Is Not DPO: Understanding Regulatory Oversight (5.7)

Privacy Lead Is Not DPO: Breach Notification Requirements (5.7)

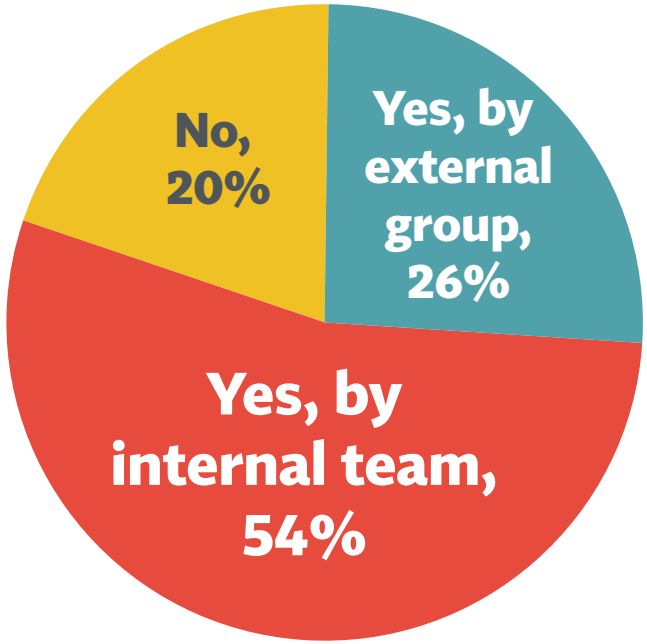
Privacy Lead Is Not DPO: Conducting Data Protection Impact Assessments (5.6)

Privacy Lead Is Not DPO: Mandatory DPO Requirement (4.9)

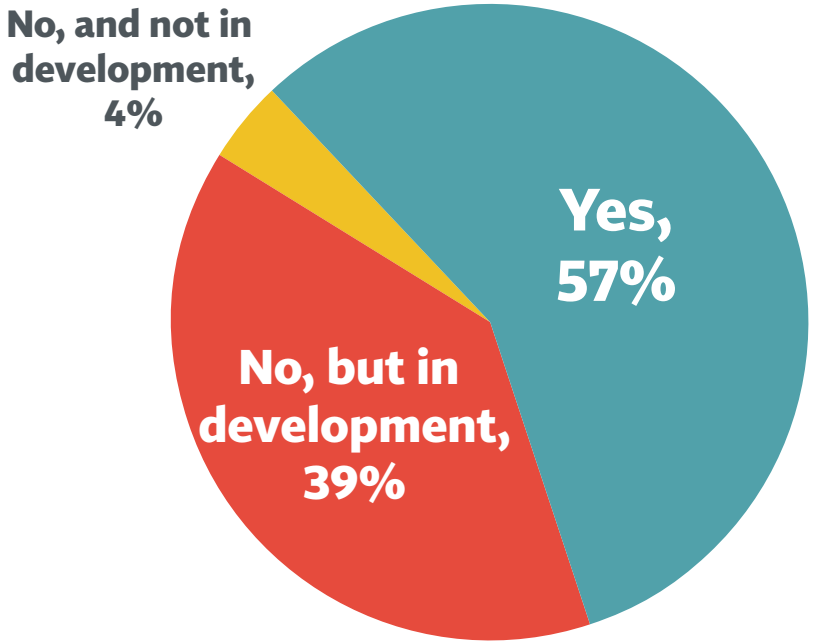
J7: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

8 in 10 firms falling under GDPR have had a gap analysis, but only 57% have a plan for addressing gaps

Had Gap Analysis Performed?
(Base: Falls Under GDPR)



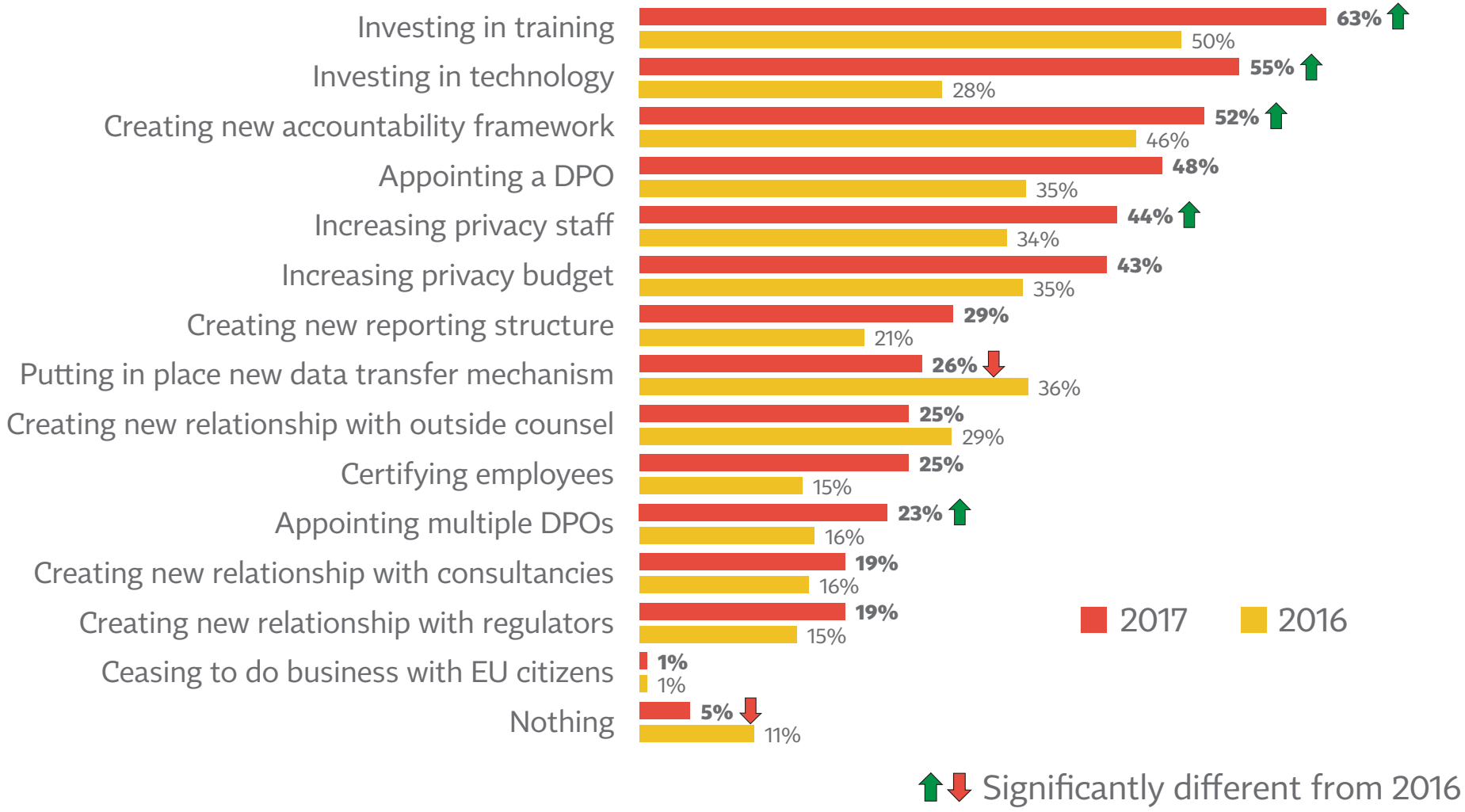
Plan for Addressing Gaps?
(Base: Falls Under GDPR)



J5: Has your company had a GDPR gap analysis performed on your privacy program?
J7: Does your company have an enterprise-wide plan for addressing any current or future GDPR compliance gaps?

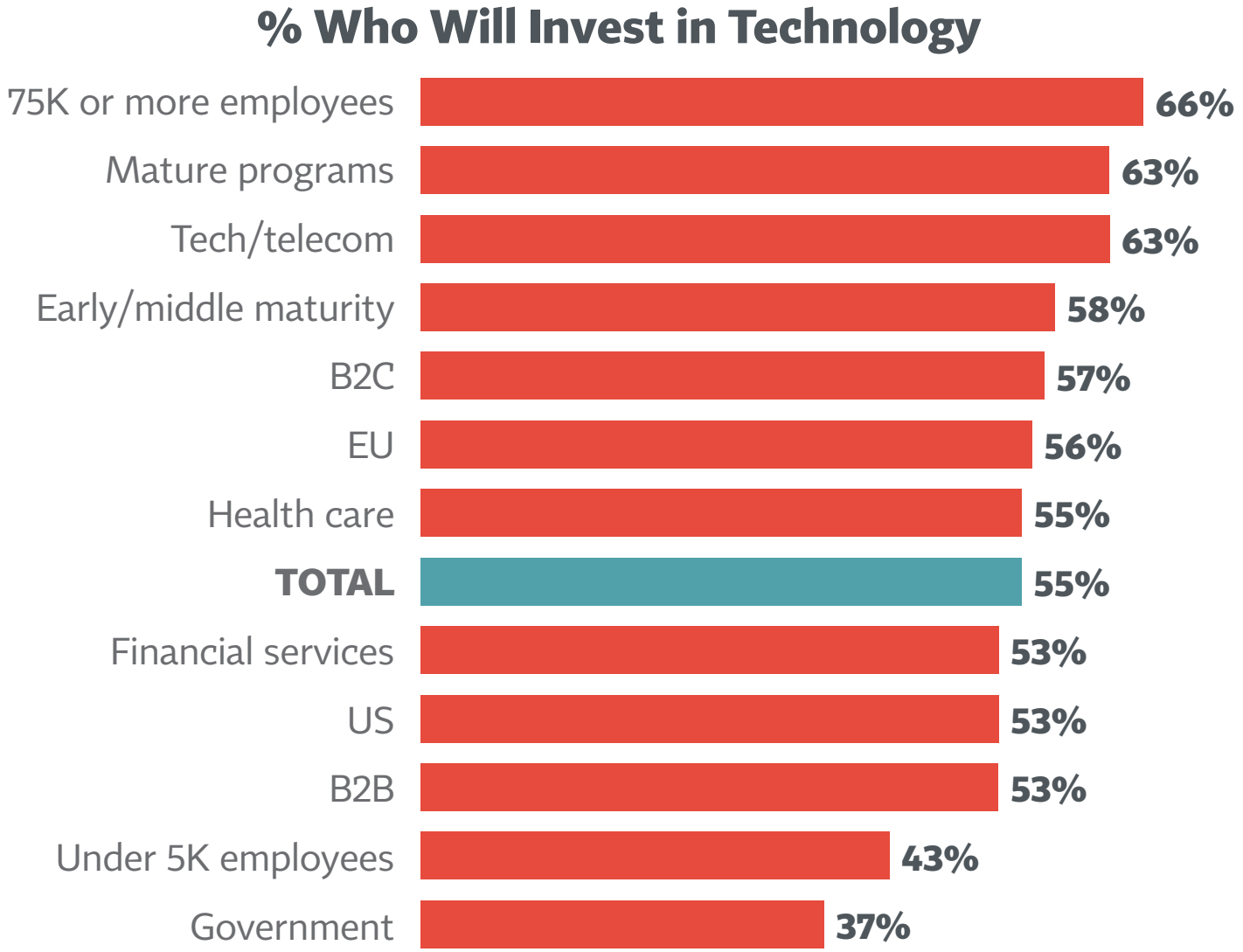
2017 sees large increases in most of the steps firms say they're taking to prepare for GDPR

Steps Being Taken to Prep for GDPR
(Base: Falls Under GDPR)



J8: What, if anything, is your organization doing to prepare for the GDPR?

The largest firms, the mature programs, and tech companies are most likely to invest in tech due to GDPR

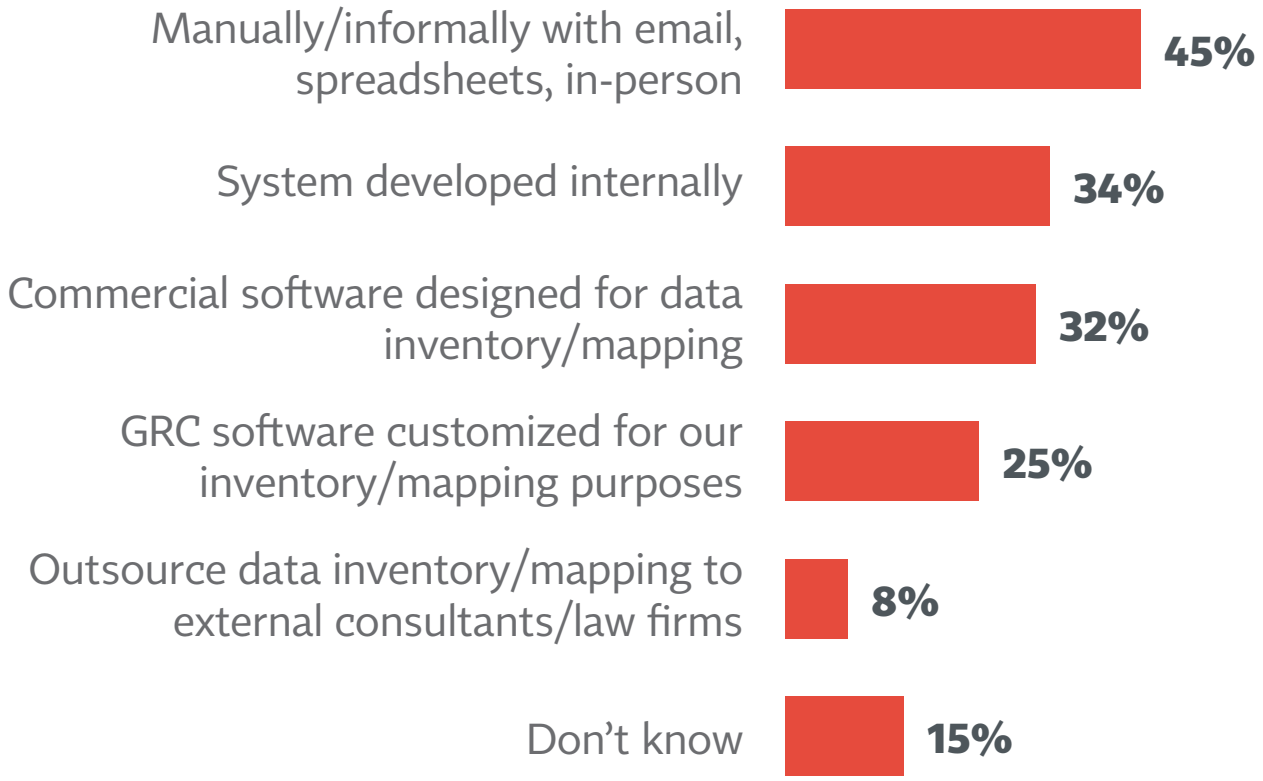


J8: What, if anything, is your organization doing to prepare for the GDPR?

Respondents still plan to address GDPR's Article 30 obligations largely with manual and informal tools

- Nearly a third say they will use software designed for purpose

Tools Will Use for Data Inventory and Mapping
(Base: Falls Under GDPR, Will Spend More)



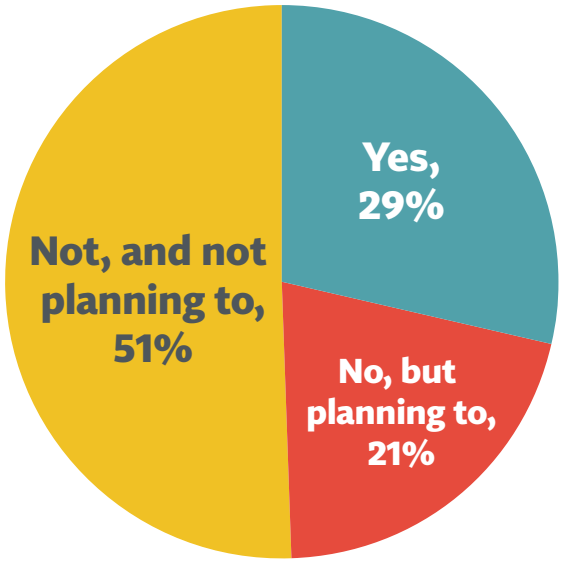
J17: Which of the following tools will you use to perform data inventory and mapping requirements of Article 30 of GDPR?

3 in 10 have elevated the privacy leader and changed reporting structure as a result of GDPR

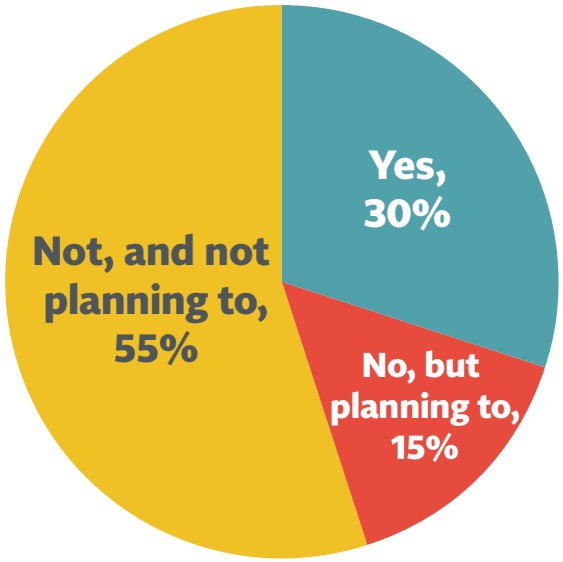
- On the other hand, more than half say they don't plan to make changes

As part of GDPR compliance efforts, has…
(Base: Falls Under GDPR)

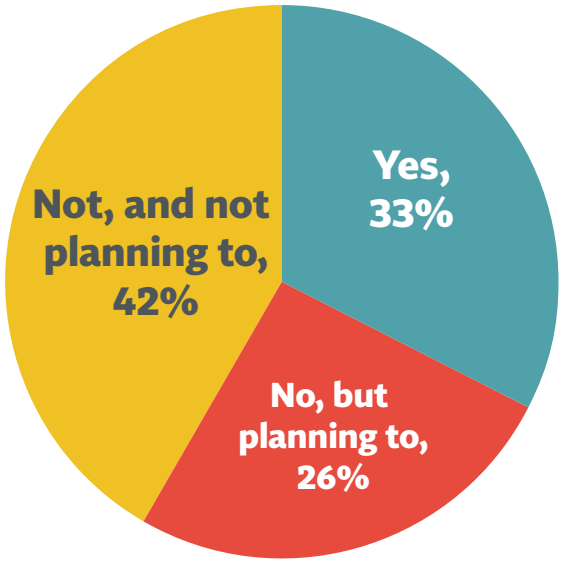
Reporting Structure Changed?



Position of Privacy Leader Elevated?

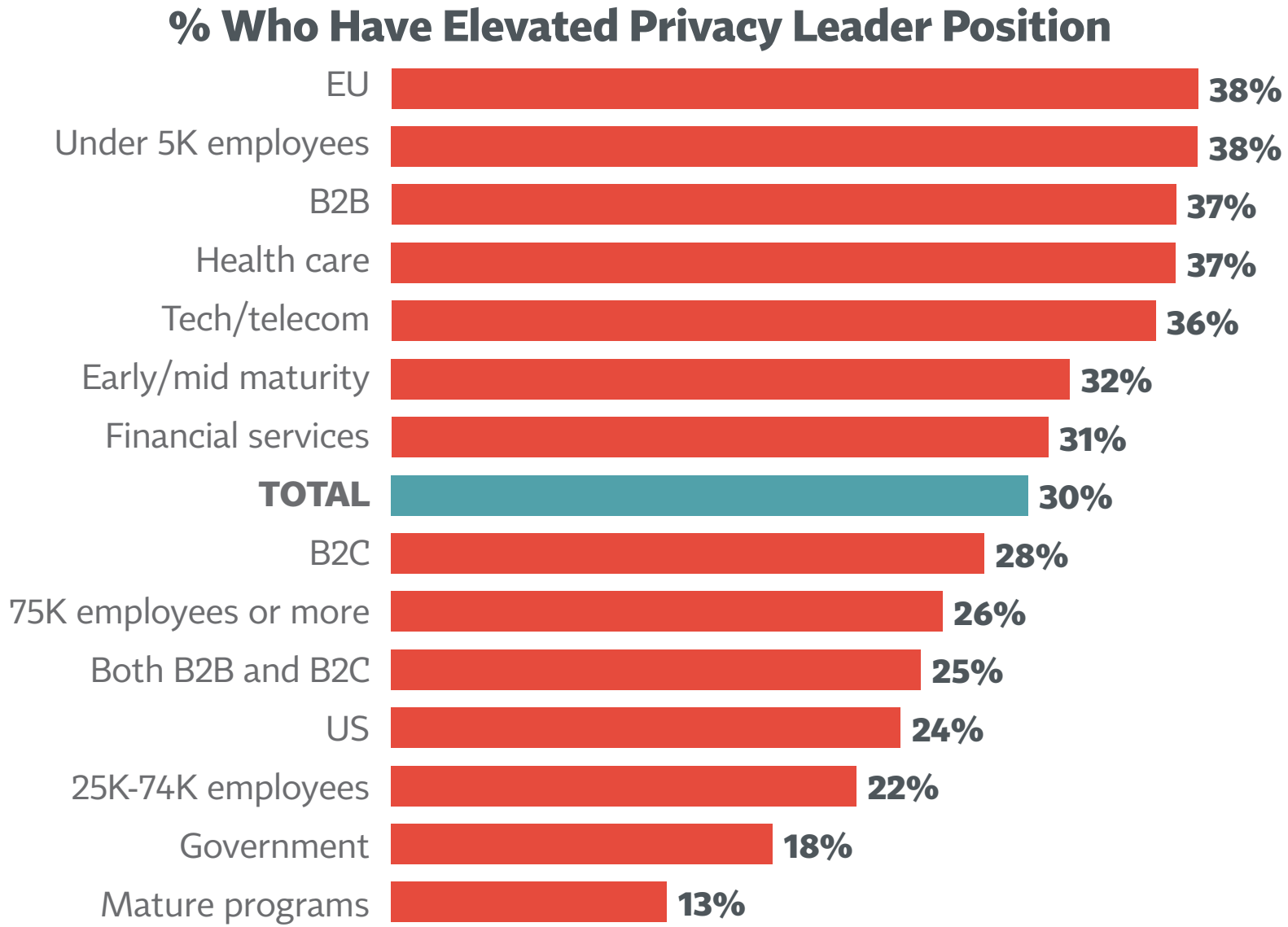


Reporting to Board Changed?



J9: Has your privacy team's reporting structure changed in the last year as part of GDPR compliance efforts?
J10: Have you elevated the position of privacy leader in the last year due to GDPR compliance efforts?
J11: Has reporting of privacy matters to the board of directors changed in the last year as part of GDPR compliance efforts?

Most likely to have elevated the privacy leader position due to GDPR: EU, small firms, B2B, and health/tech



J10: Have you elevated the position of privacy leader in the last year due to GDPR compliance efforts?

The average GDPR-affected firm will need to add about 4 employees to assist with GDPR initiatives

- Among firms with the most employees generally, the number of new hires is 10

Additional Employees Intend To Hire for GDPR
(Base: Falls Under GDPR)

BY EMPLOYEE SIZE

Mean Employees Expected to Hire	TOTAL	<5K	5–24.9K	25–74.9K	75K+
Full-time	2.2	0.6	2.3	1.5	4.9
Part-time	1.7	0.5	1.0	0.8	5.1

Significantly higher than total

J12: How many additional employees does your company intend to hire to assist with GPDR-related activities, if any?

The number of full-time staff that will be added to help with GDPR is directionally highest in financial firms

Additional Employees Intend To Hire for GDPR
(Base: Falls Under GDPR)

BY INDUSTRY

Mean Employees Expected to Hire	TOTAL	Gov't	Finance	Health	Tech
Full-time	2.2	1.2	4.0	2.6	2.3
Part-time	1.7	0.6	2.9	3.7	1.4

J12: How many additional employees does your company intend to hire to assist with GPDR-related activities, if any?

Mature privacy programs expect to hire 9 new employees as a result of GDPR

Additional Employees Intend To Hire for GDPR
(Base: Falls Under GDPR)

BY MATURITY

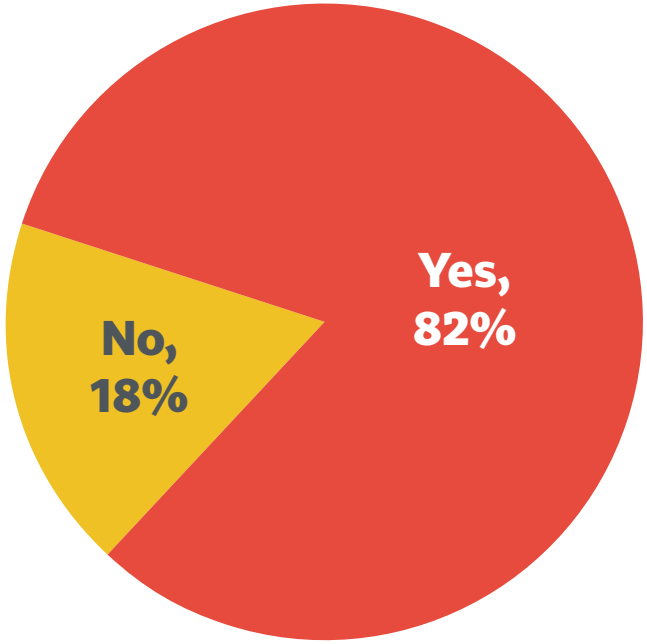
Mean Employees Expected to Hire	TOTAL	Early/Middle Maturity	Mature
Full-time	2.2	1.3	2.5
Part-time	1.7	1.8	6.6

Significantly higher than total

J12: How many additional employees does your company intend to hire to assist with GPDR-related activities, if any?

More than 8 in 10 firms falling under the scope of GDPR say they'll need to adapt products to comply

Expect To Adapt Products and Services
(Base: Falls Under GDPR)



J13: Do you expect your organization will need to adapt current products and services to be GDPR compliant?

Firms report that GDPR will require more than $2M to adapt products, and close to $3M in other expenses

- The mean additional spending expected is comparable between the US and the EU; median figures suggest the "typical" US firm will spend much more

Additional Spending Resulting from GDPR
(Base: Falls Under GDPR)

BY LOCATION

Mean Spending (000)	TOTAL	US	EU
To adapt products and services (base: expect to adapt)	$2,160	$2,885	$1,732
Additional GDPR spending	$2,844	$3,135	$3,173
Median Spending (000)			
To adapt products and services (base: expect to adapt)	$20	$50	$10
Additional GDPR spending	$100	$150	$50

J14_1: How much do you expect to spend to adapt these current products and services to be GDPR compliant?
J14_2: About how much do you think you will spend in your budget to comply with GDPR, not including spending to adapt specific products and services?

Financial and tech firms say they'll need to spend higher amounts than average to be GDPR compliant

Additional Spending Resulting from GDPR
(Base: Falls Under GDPR)

BY INDUSTRY

Mean Spending (000)	TOTAL	Gov't	Finance	Health	Tech
To adapt products and services (base: expect to adapt)	$2,160	$43	$4,123	$258	$3,125
Additional GDPR spending	$2,844	$36	$8,410	$779	$922
Median Spending (000)					
To adapt products and services (base: expect to adapt)	$20	$0	$50	$0	$10
Additional GDPR spending	$100	$0	$100	$250	$50

Significantly higher than total

J14_1: How much do you expect to spend to adapt these current products and services to be GDPR compliant?
J14_2: About how much do you think you will spend in your budget to comply with GDPR, not including spending to adapt specific products and services?

GDPR-related spending is also expected to be highest among the largest firms and most mature programs

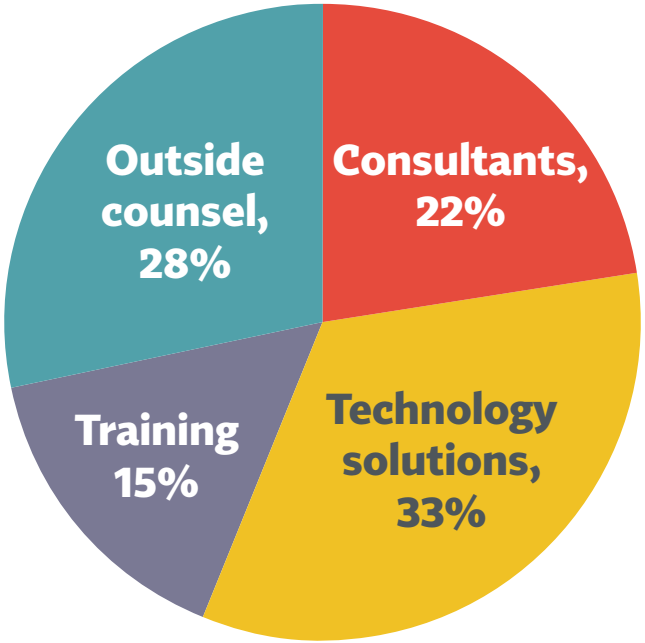
Additional Spending Resulting from GDPR
(Base: Falls Under GDPR)

		BY EMPLOYEE SIZE				BY MATURITY	
Mean Spending (000)	**TOTAL**	**<5K**	**5–24.9K**	**25–74.9K**	**75K+**	**Early/Middle Maturity**	**Mature**
To adapt products and services (base: expect to adapt)	$2,160	$317	$1,218	$1,475	$6,194	$758	$6,725
Additional GDPR spending	$2,844	$241	$1,167	$1,046	$9,581	$946	$7,176
Median Spending (000)							
To adapt products and services (base: expect to adapt)	$20	$10	$1	$200	$100	$100	$500
Additional GDPR spending	$100	$15	$100	$200	$150	$100	$500

J14_1: How much do you expect to spend to adapt these current products and services to be GDPR compliant?
J14_2: About how much do you think you will spend in your budget to comply with GDPR, not including spending to adapt specific products and services?

Among those who will spend more for GDPR, the lion's share will be for tech solutions and outside counsel

Distribution of Additional GDPR Compliance Budget
(Base: Falls Under GDPR, Will Spend More)



J15: About what percentage of that additional budget for GDPR compliance falls into each of these categories?

Share of GDPR compliance budget earmarked for outside counsel is significantly higher in the US than EU

Distribution of Additional GDPR Compliance Budget
(Base: Falls Under GDPR, Will Spend More)

BY LOCATION

% of Budget to:	TOTAL	US	EU
Outside counsel	28%	33%	19%
Consultants	22%	22%	23%
Technology solutions	33%	30%	37%
Training	15%	13%	16%

Significantly higher than total

J15: About what percentage of that additional budget for GDPR compliance falls into each of these categories?

Compliance budget distribution does not differ significantly by industry segment

Distribution of Additional GDPR Compliance Budget
(Base: Falls Under GDPR, Will Spend More)

BY INDUSTRY

% of Budget to:	TOTAL	Gov't	Finance	Health	Tech
Outside counsel	28%	25%	30%	34%	29%
Consultants	22%	30%	22%	29%	16%
Technology solutions	33%	31%	30%	23%	35%
Training	15%	14%	14%	10%	16%

J15: About what percentage of that additional budget for GDPR compliance falls into each of these categories?

In large firms, GDPR budget share for consultants and technology is directionally higher than in small firms

Distribution of Additional GDPR Compliance Budget
(Base: Falls Under GDPR, Will Spend More)

		BY EMPLOYEE SIZE				BY MATURITY	
% of Budget to:	**TOTAL**	**<5K**	**5–24.9K**	**25–74.9K**	**75K+**	**Early/Middle Maturity**	**Mature**
Outside counsel	28%	31%	27%	27%	24%	30%	28%
Consultants	22%	16%	21%	29%	26%	25%	22%
Technology solutions	33%	29%	38%	30%	37%	32%	34%
Training	15%	16%	16%	13%	13%	14%	16%

J15: About what percentage of that additional budget for GDPR compliance falls into each of these categories?

EU firms are more likely to say they'll only be partially compliant and that they're making changes to comply

- Also, privacy leads that are not DPOs are more likely to say they'll be only partially compliant

GDPR Compliance
Segments with Higher Than Average Results

		BY LOCATION		PRIVACY LEAD IS:	
	TOTAL	US	EU	DPO	Not DPO
Expect to be partially GDPR compliant	57%	51%	66%	58%	70%
Elevated privacy leader position	30%	24%	38%	39%	24%
Reporting to board has changed	33%	21%	50%	30%	18%
Privacy reporting structure has changed	29%	21%	39%	30%	11%
Expect to be fully GDPR compliant	40%	45%	33%	42%	28%
Not planning to change privacy reporting	51%	61%	38%	56%	74%
Not planning to change reporting to board	55%	66%	40%	51%	73%
% of additional budget for GDPR is for: **attorneys**	28%	33%	19%	22%	36%

Significantly higher than total

Mature privacy programs are the most confident they'll be fully compliant, without changes needed

GDPR Compliance
Segments with Higher Than Average Results

		BY EMPLOYEE SIZE				BY PROGRAM MATURITY	
	TOTAL	<5K	5–24.9K	25–74.9K	75K+	Early/ Middle	Mature
Elevated privacy leader position	30%	38%	29%	22%	26%	32%	13%
Not planning to elevate privacy leader position	55%	46%	55%	62%	63%	64%	74%
Not planning to change privacy reporting structure	51%	53%	50%	54%	46%	61%	69%
Expect to be **fully** GDPR compliant	40%	36%	33%	46%	45%	26%	61%
Expect to be **partially** compliant	57%	60%	62%	52%	52%	74%	39%

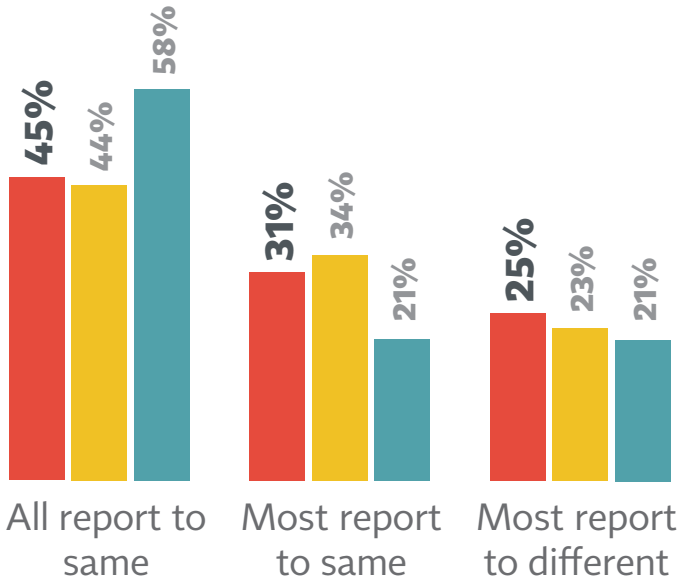
Significantly higher than total

Contents

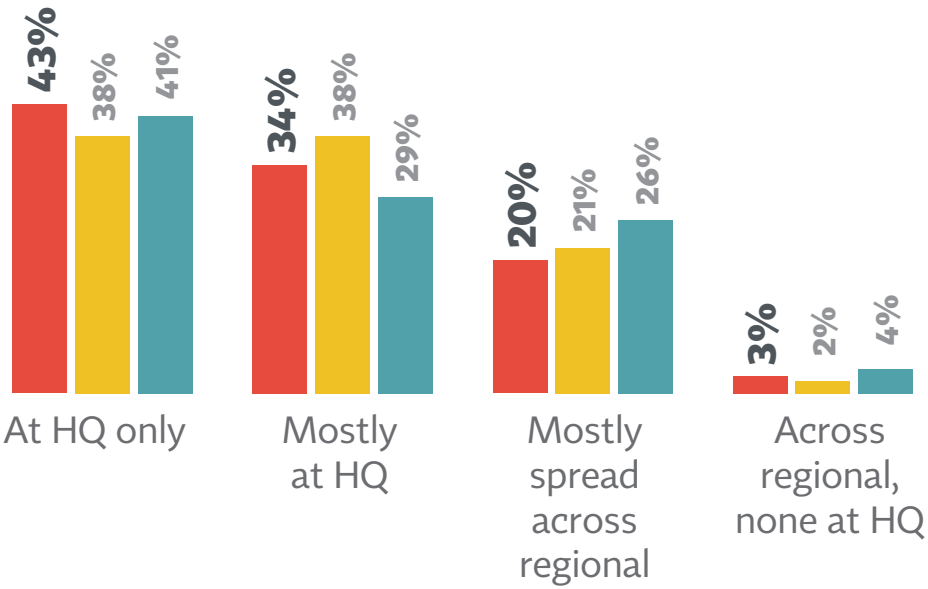
There's been little change since last year in the degree of centralization of the privacy function

- 45% say privacy employees all report to the same people, vs. 44% last year
- However, there's been a directional increase in those saying the privacy function is located only at headquarters, from 38% to 44%

Reporting Structure
Base: Director or Higher



Physical Location of Privacy Function
Base: Director or Higher



F10: Which of the following best describes the reporting structure for you and the colleagues you work with in privacy?
F11: The privacy function of your company is geographically located ...

US firms are more likely than EU firms to have their privacy function housed at headquarters

Location of Privacy Function:
Responding: Director or Higher

BY GEOGRAPHY

	US	EU
At HQ only	48%	20%
Mostly at HQ	33%	43%
Mostly regional with some HQ	17%	30%
Regional only	2%	7%

Significantly higher than total

Firms where privacy programs are geographically dispersed tend to be much larger, with higher budgets

Profile of Professionals by Privacy Function Centralization

BY LOCATION OF PRIVACY FUNCTION

Director Level or Above Only

	All at HQ	Distributed
HQ LOCATION		
US	77%	66%
INDUSTRY		
Financial Services	23%	33%
Technology/telecom	36%	26%
CUSTOMER TARGET		
B2B	28%	41%
COMPANY EMPLOYEES		
Mean (000)	8.4	56.5
MATURITY STAGE		
Mature	17%	40%
PRIVACY EMPLOYEES		
Mean full-time or part-time	3.4	21.1
TOTAL PRIVACY SPEND (INCL. OUTSIDE BUDGET)		
Mean (000)	$829	$3,083
PRIVACY LEADER…		
Has non-privacy responsibilities	74%	56%

Significantly higher than total

Those with geographically dispersed programs are also significantly more likely to use a variety of resources

Profile of Professionals by Privacy Function Centralization

BY LOCATION OF PRIVACY FUNCTION

Director Level or Above Only

	All at HQ	Distributed
PRIVACY MATTERS REPORTED TO…		
Entire board	51%	26%
Committee	37%	59%
USES		
Internal audit	64%	81%
PIAs	59%	82%
Vendor management	64%	84%
Data transfer to EU	40%	84%
REQUIRES		
SOC2 Privacy	39%	53%
GDPR		
Has plan to address gaps	41%	68%
Has NOT changed reporting structure	71%	60%
Mean employees to hire due to GDPR (total)	0.8	7.1
CERTIFICATION		
Respondent has CIPP	56%	75%

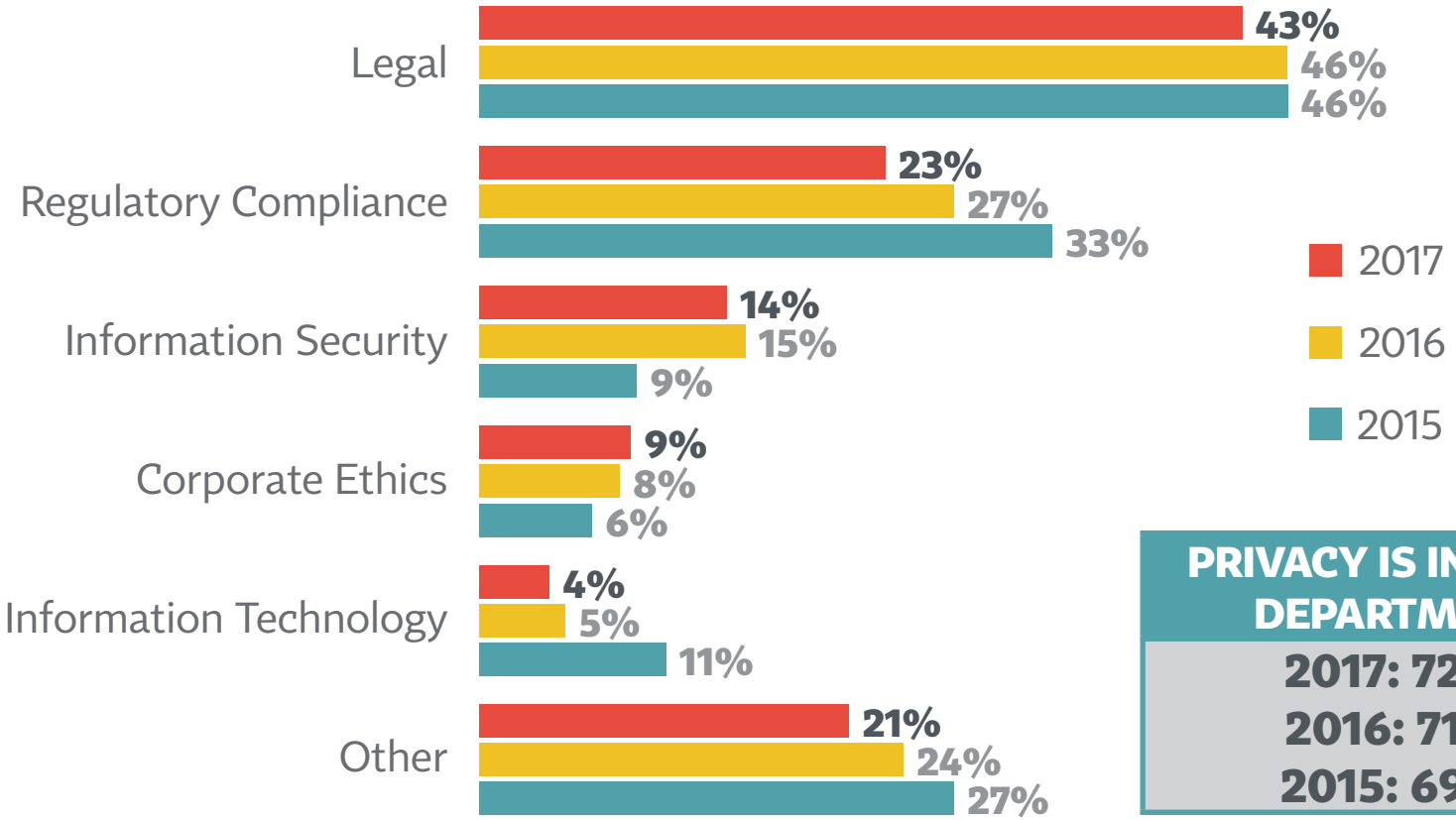
Significantly higher than total

The privacy function is a bit less likely to be based in either legal or compliance than in 2016

- There's been no change in the proportion saying privacy is in the "right" department: 72% in 2017, 71% in 2016

Organizational Location of Privacy Function

Base: Director or Higher



PRIVACY IS IN RIGHT DEPARTMENT
2017: 72%
2016: 71%
2015: 69%

F12: Where within your company is the privacy function located? (Could pick more than one.)

Contents

Privacy leads are most likely to report to General Counsel

- Ranked second and third are the CEO and the firm's Compliance or Ethics Officer

To Whom Top Privacy Person Reports
Base: Director or Higher

F26: Who does the top privacy person report to?

The number of rungs between the privacy lead and the CEO is virtually the same as it was in 2016: 2.3

- However, there's been a directional 5-point increase in the percent of respondents who say they are the privacy lead at their firm

Hierarchical Characteristics

Base: Director or Higher

RUNGS BETWEEN PRIVACY LEADER AND CEO
2017: 2.3 2016: 2.4

FULL-TIME STAFF REPORTING TO RESPONDENT (MEAN)
2017: 4.5 2016: 4.4

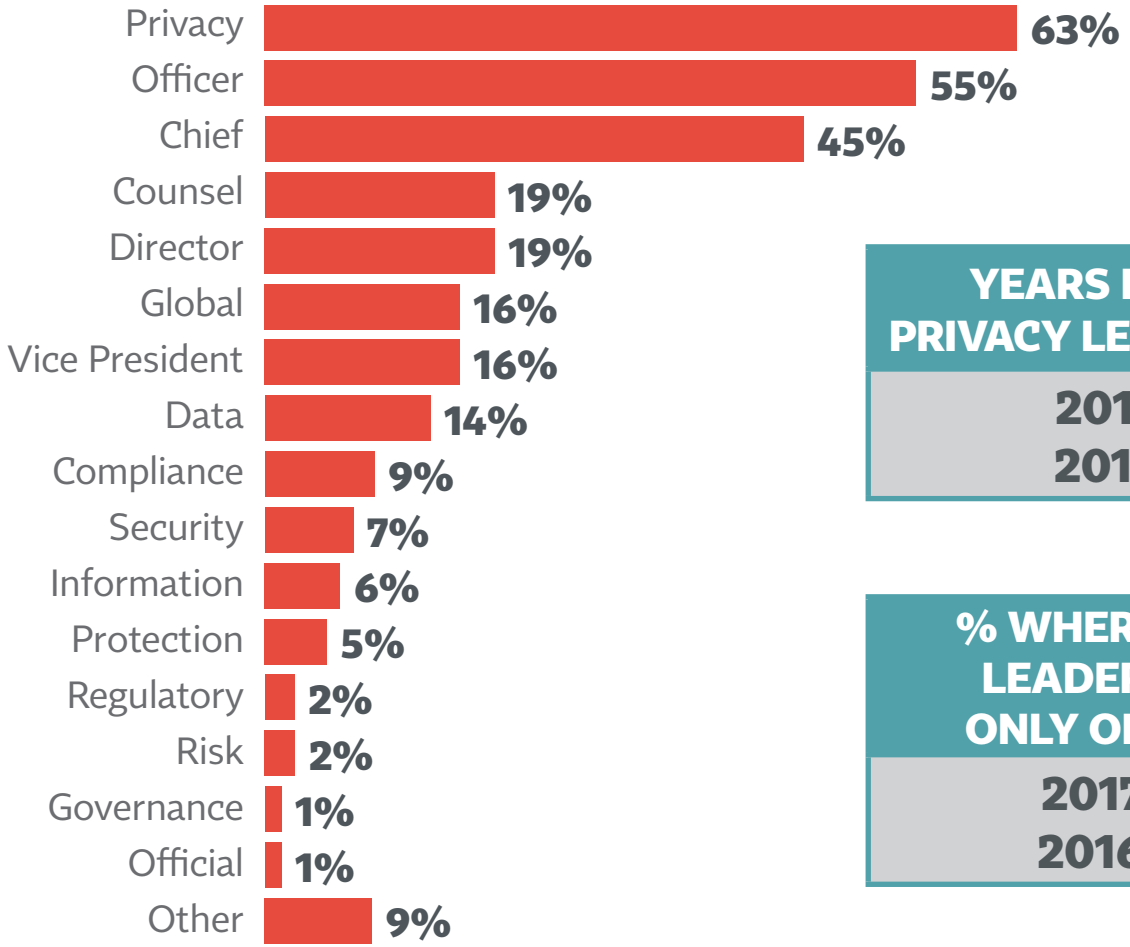
RESPONDENT IS PRIVACY LEAD?
2017: 68% 2016: 63%

F15: How many full-time staff report to you?
F19: How many vertical rungs away from the CEO is the privacy leader
F21: Are you the company's privacy leader, or is that someone else?

Other than “privacy,” “officer” and “chief” are the most common terms in the title of the lead privacy professional

Terms in Title of Privacy Leader

Base: Director or Higher



YEARS HAVE HAD PRIVACY LEADER (MEAN)

2017: 5.8
2016: 6.3

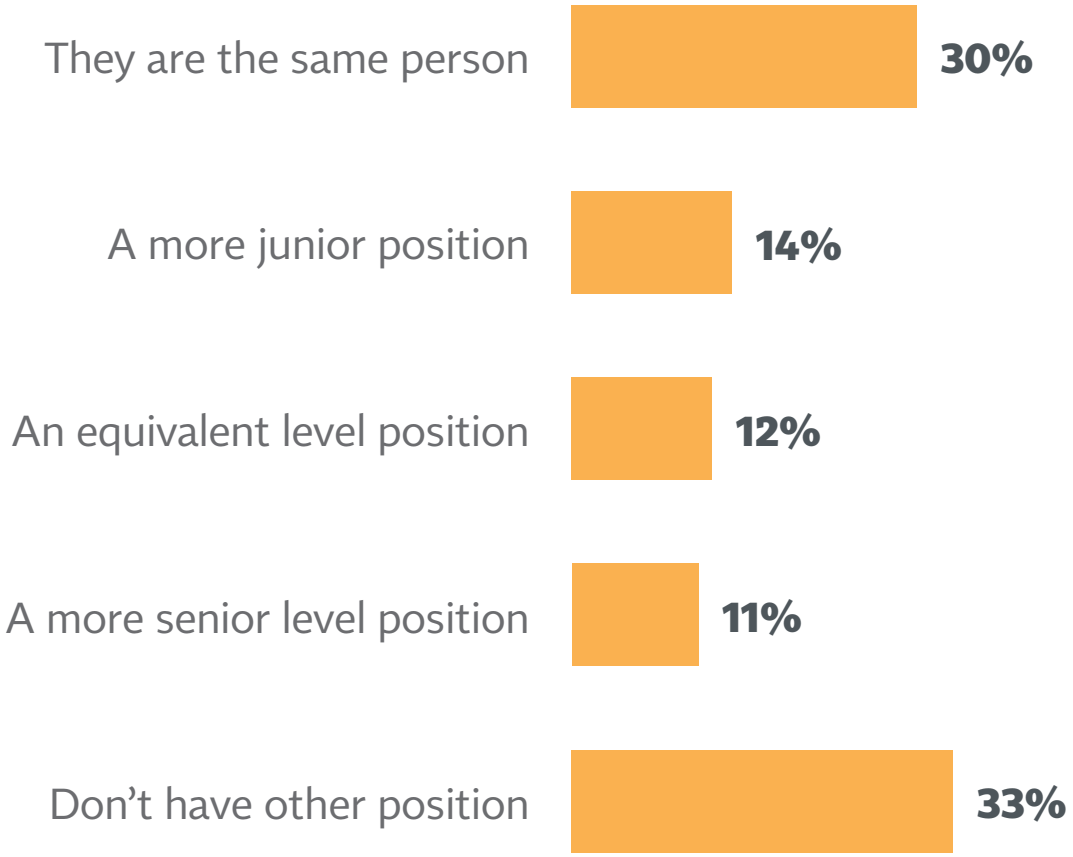
% WHERE PRIVACY LEADER WORKS ONLY ON PRIVACY

2017: 37%
2016: 36%

F18: Which of the following words occur in the official, formal title of the person in rung #1 [or Privacy lead from F22]?
F20: For how many years has your company had a privacy leader or chief privacy officer?
F24: Does the individual designated as your company’s privacy leader have responsibilities other than privacy?

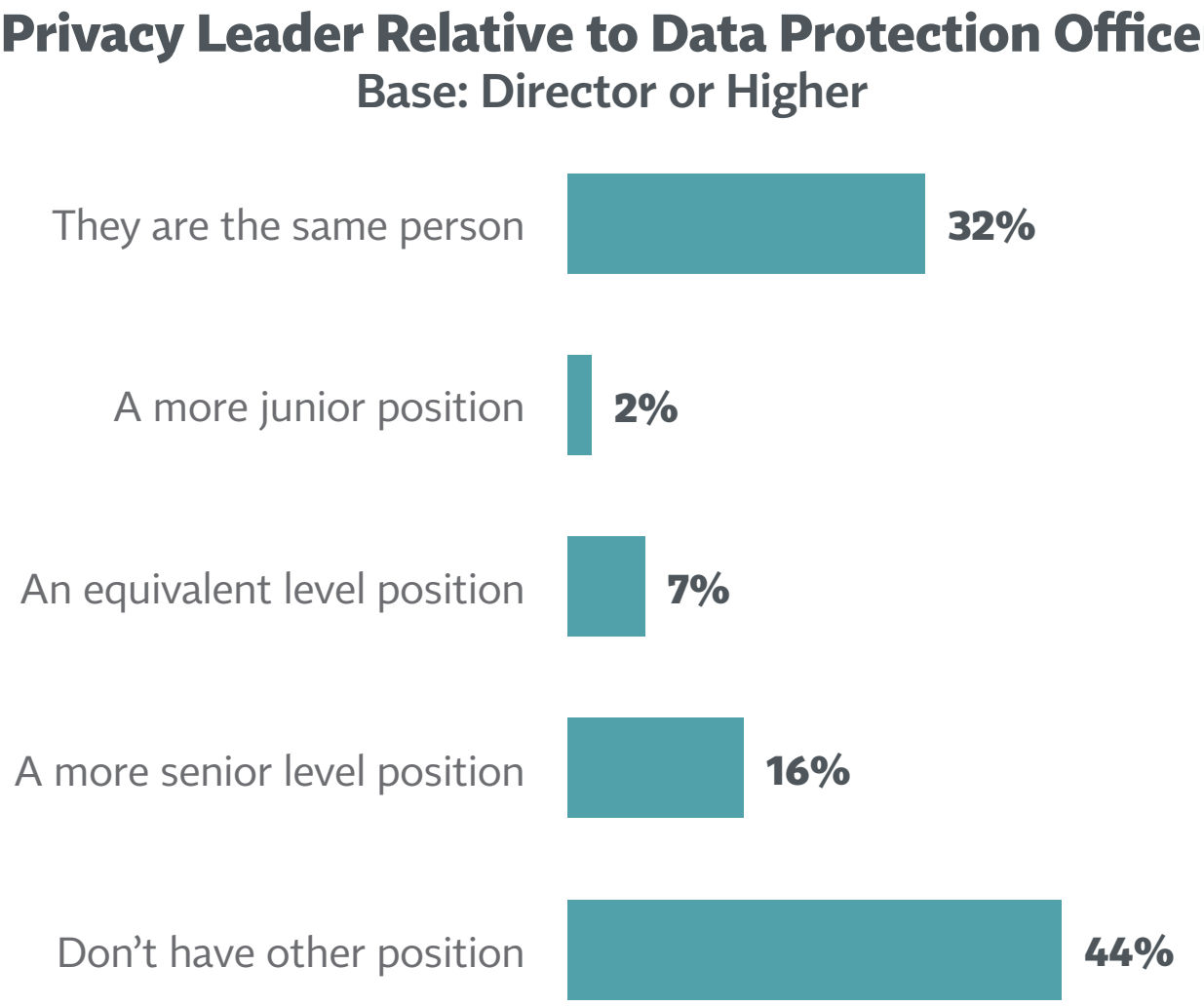
More than a third of organizations have separate lead privacy counsels and heads of privacy operations

Privacy Leader Relative to Chief Privacy Counsel
Base: Director or Higher



F23b: How does the Privacy Leader compare with your company's chief privacy counsel? The Privacy Leader is …

For 76% of organizations, there is either no DPO in place, or the position is held by the privacy leader



F23c: How does the Privacy Leader compare with your company's data protection officer (DPO), if any? The Privacy Leader is …

The CISO is more likely to be above the privacy leader in the company hierarchy

- Still, more than half say the privacy leader is equal to, or above, the CISO

F23a: How does the privacy leader/chief privacy officer compare with your company's chief information security officer or the highest level information security person in the company? The privacy leader/chief privacy officer is …

Unregulated and B2B firms are most likely to have a CPO who is also the DPO

CPO vs. Data Privacy Officer
Responding: Director or Higher

	BY INDUSTRY CATEGORY		BY CUSTOMER TARGET		
	Regulated	Unregulated	B2B	B2C	Both
Same Person	18%	45%	42%	30%	25%
Junior to DPO	3%	3%	1%	3%	2%
Equal to DPO	12%	4%	6%	3%	8%
Senior to DPO	23%	10%	21%	18%	12%
Don't have DPO	43%	38%	29%	46%	52%

Significantly higher than total

EU firms are more likely to say their CPO and CISO are the same; in the US, CPOs tend to be more junior

CPO vs. Chief Information Security Officer

Responding: Director or Higher

BY GEOGRAPHY

	US	EU
Same Person	11%	20%
Junior to CISO	35%	23%
Equal to CISO	41%	39%
Senior to CISO	6%	12%
Don't have CISO	6%	6%

The CPO is especially likely to also have Chief Privacy Counsel responsibilities in unregulated firms

CPO vs. Chief Privacy Counsel
Responding: Director or Higher

	BY INDUSTRY CATEGORY			BY CUSTOMER TARGET		
	Regulated	Unregulated	Gov't	B2B	B2C	Both
Same Person	24%	36%	20%	32%	18%	31%
Junior to CPC	12%	18%	20%	15%	6%	17%
Equal to CPC	18%	5%	20%	4%	7%	18%
Senior to CPC	17%	10%	0%	8%	28%	8%

Significantly higher than total

EU firms are also more likely to say their CPO is also the DPO; US firms are less likely to even have a DPO

CPO vs. Data Protection Officer

Responding: Director or Higher

BY GEOGRAPHY

	US	EU
Same Person	24%	60%
Junior to DPO	3%	0%
Equal to DPO	7%	4%
Senior to DPO	12%	18%
Don't have DPO	52%	18%

Privacy leads who are also DPOs are more likely to work in unregulated, B2B firms

- They're also more likely to work in firms that transfer data across borders and to consider EU GDPR compliance important

Key DPO Characteristics
Higher Than Average Results

BY CPO/DPO STATUS

	CPO Is Also DPO	CPO Is Not DPO
Works in unregulated firm	63%	45%
Works in tech firm	39%	30%
Works in B2B firm	46%	35%
Has CIPP/E	49%	12%
Firm transfers data from EU to US	73%	54%
Program is in early maturity stage	28%	15%
Top 3 Importance: Compliance with EU GDPR	74%	52%
Privacy involvement in ongoing activities: Throughout process	70%	50%

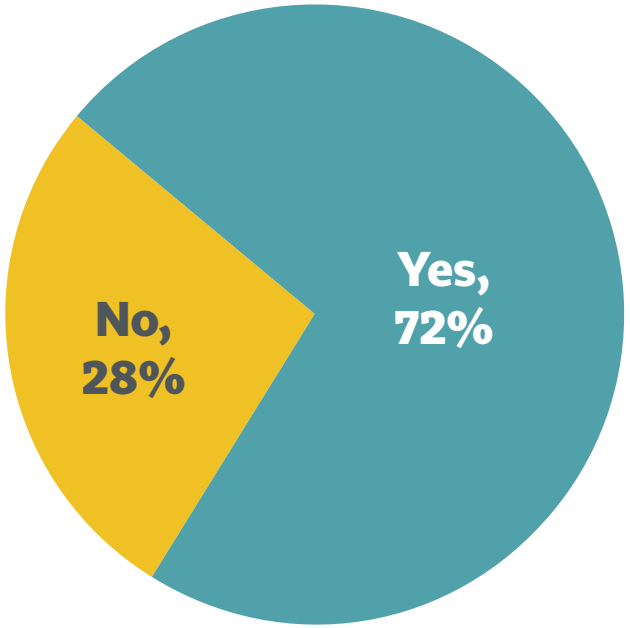
Significantly higher than total

For reporting privacy matters to the board, 2017 results are identical to 2016

- Three-fourths say privacy matters are reported to the board
- In addition, 44% say matters are reported on an ad-hoc basis, while 41% have a regular semi-annual reporting schedule

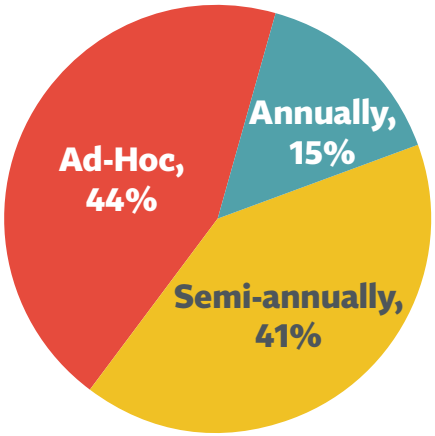
Privacy Matters Reported to Board?

Base: Director or Higher

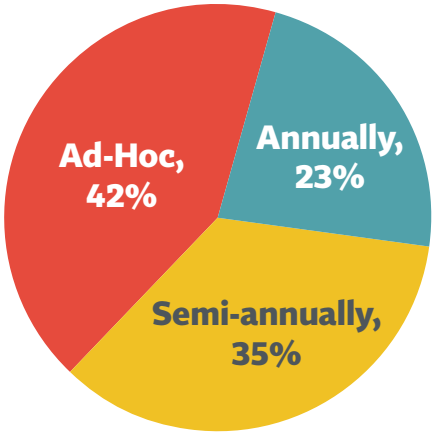


How Often?

Base: Matters Reported to Board



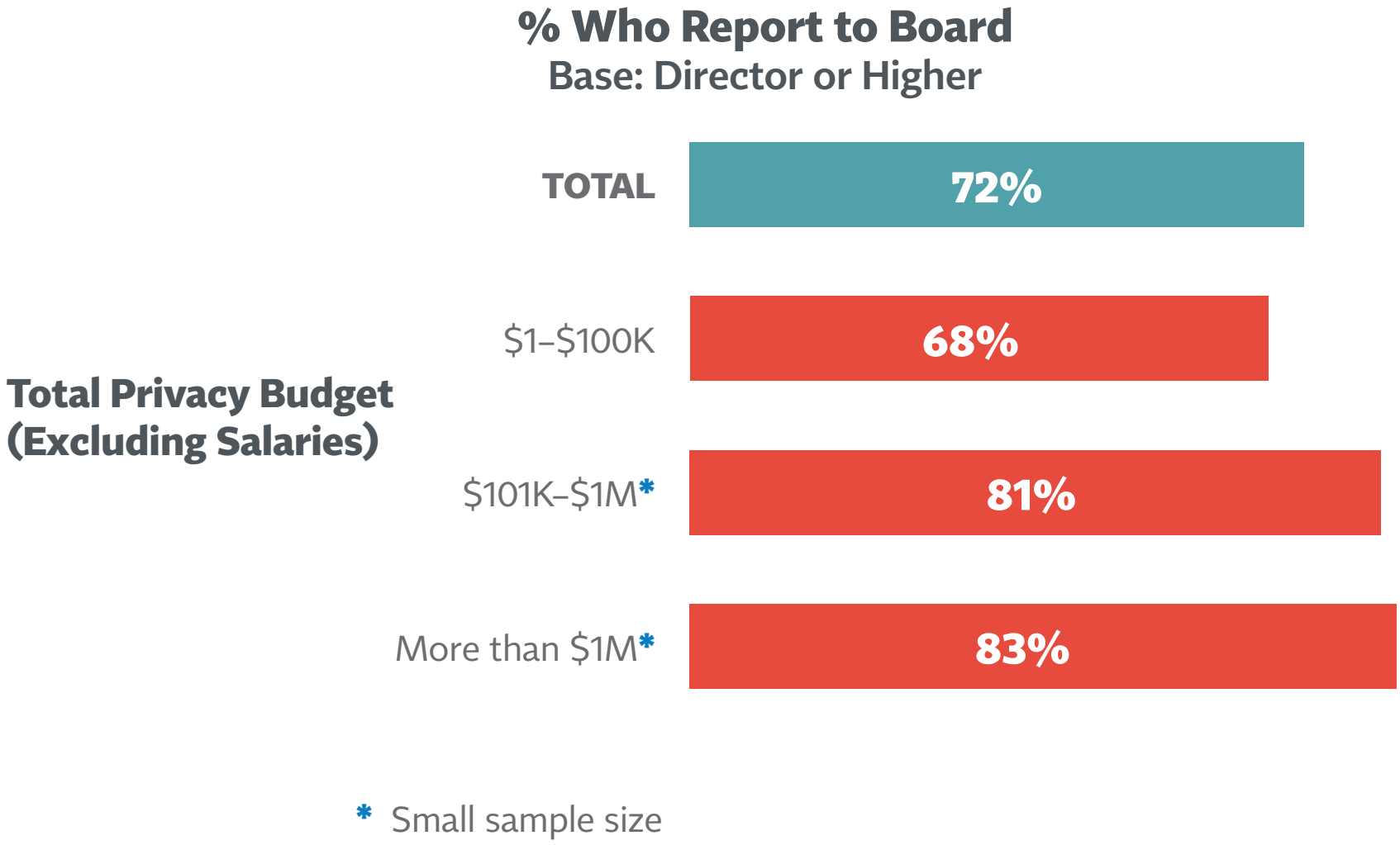
2017



2016

F27: Are privacy-related matters at your organization reported to the board of directors or the board level generally?
F28: How often are privacy matters reported at the board level?

Firms with privacy budgets over $100K are most likely to say privacy matters are reported to their board



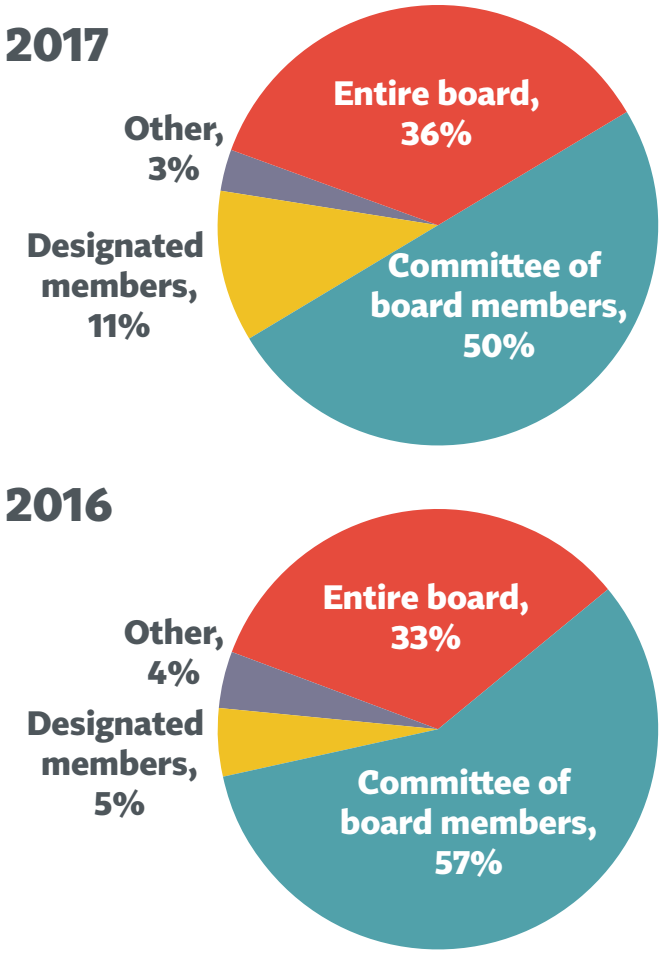
F27: Are privacy-related matters at your organization reported to the board of directors or the board level generally?

Board reporting is typically to a committee, and General Counsels/CPOs are most likely to do the reporting

- The percent saying reports come from the Chief Risk Office has jumped since 2016

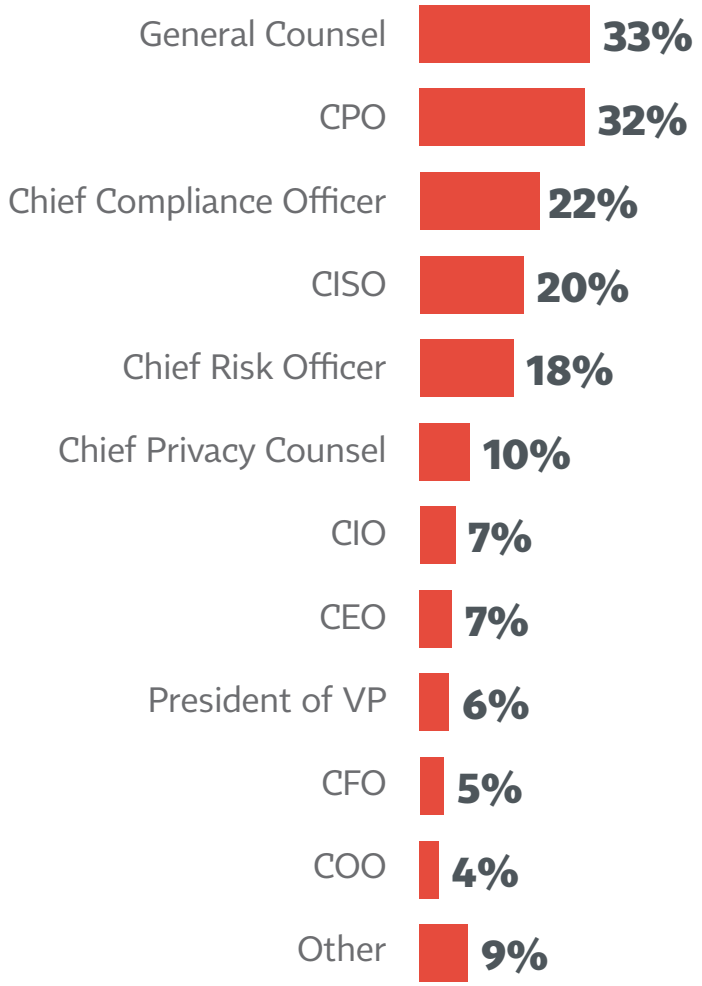
To Whom at Board Matters Reported

Base: Matters Reported to Board



Who Does Reporting

Base: Matters Reported to Board



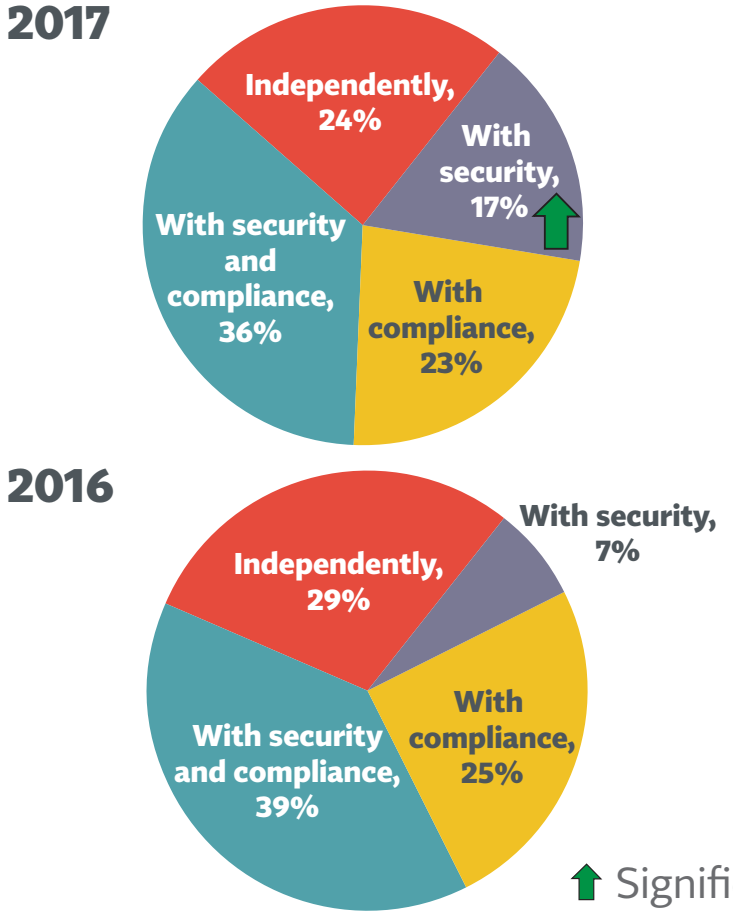
F29: Who at the board level are privacy matters reported to?
F32: Who at least sometimes reports privacy matters at the board level?

Data breaches have been supplanted by substantive privacy governance issues as top Board topic

- Privacy operations is also now being reported alongside security operations more often than in 2016

How Privacy Topics Treated with Board

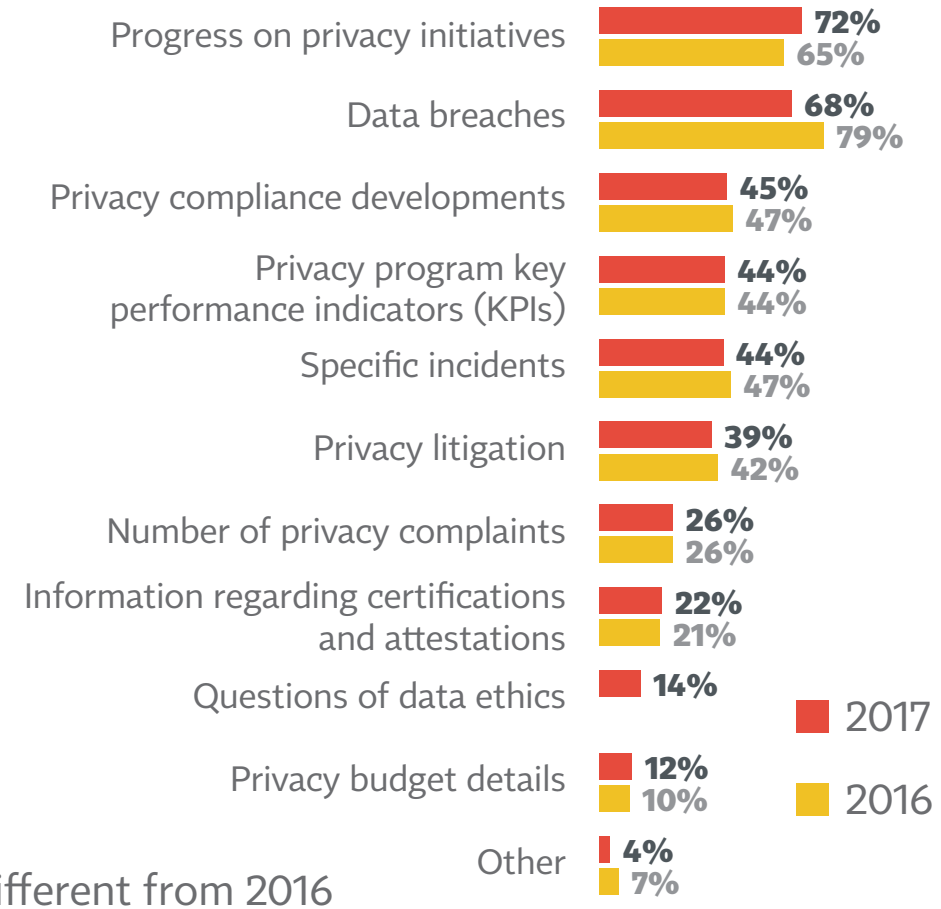
Base: Matters Reported to Board



↑ Significantly different from 2016

Specific Topics Reported

Base: Matters Reported to Board



F30: Privacy matters are reported to the board…
F31: What privacy topics are reported at the board level?

Independent reporting of privacy matters to the board is less common in regulated firms

How Matters Reported to Board
Responding: Director or Higher

	BY INDUSTRY CATEGORY			BY CUSTOMER TARGET		
	Regulated	Unregulated	Gov't	B2B	B2C	Both
Independently	14%	31%	34%	25%	25%	22%
With security	16%	17%	66%	12%	26%	17%
With compliance	29%	20%	0%	16%	10%	33%
With both	41%	32%	0%	46%	39%	28%

Significantly higher than total

EU firms are directionally more likely to say privacy matters are reported to the board independently

How Matters Reported to Board
Responding: Director or Higher

BY GEOGRAPHY

	US	EU
Independently	21%	31%
With security	18%	22%
With compliance	24%	6%
With both	38%	42%

Contents

Compliance and breach risk prevention are the strongest reasons for having a privacy function

- 2017 sees a directional increase in "meeting client expectations" as a reason

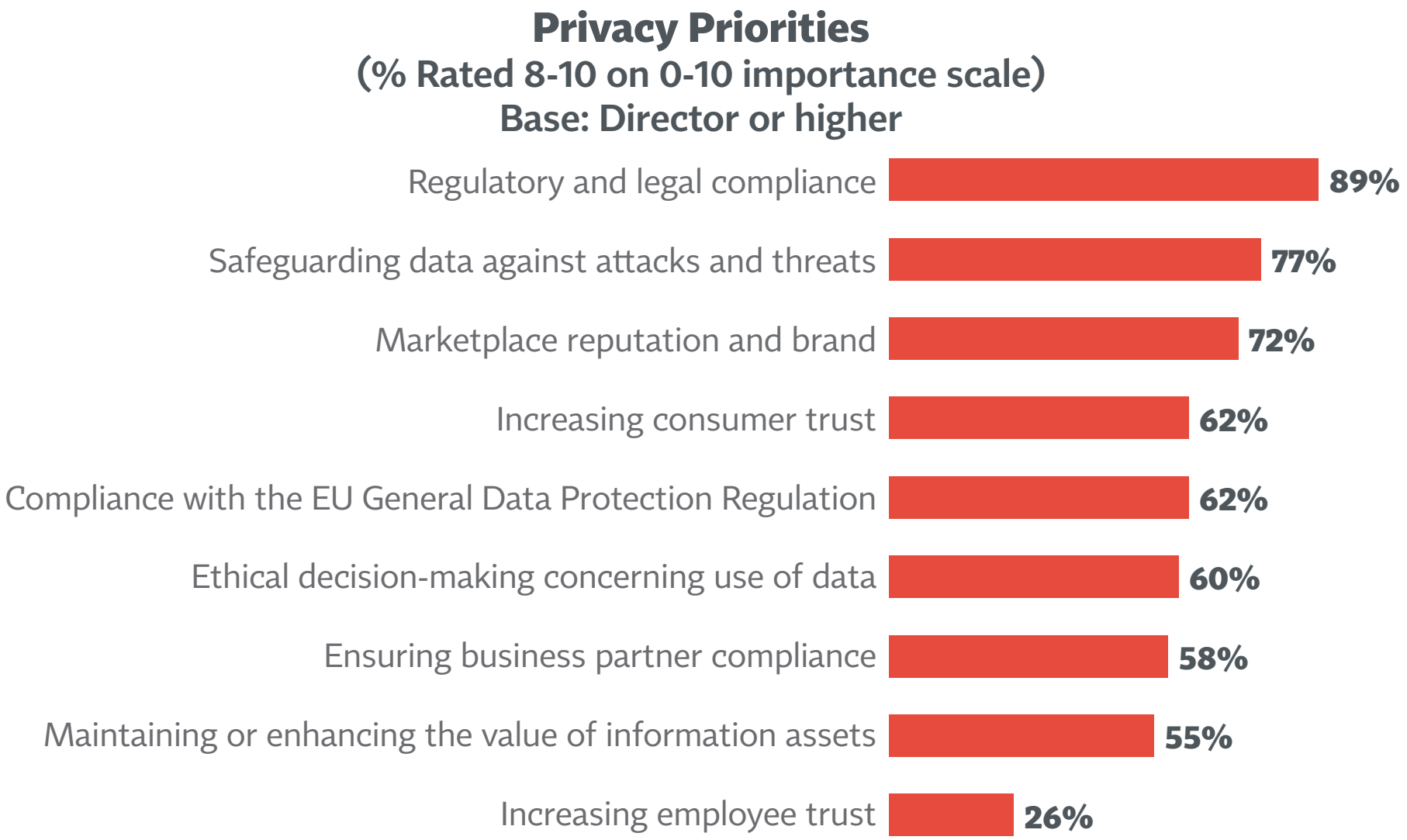
Reasons for Having Privacy Function

Base: Director or Higher

CATEGORIES	2017	2016	2015
Compliance	95%	93%	93%
Brand	88%	84%	88%
Corporate Citizen	48%	45%	50%

E6: Which of the following would you say are the main reasons that the leadership of your company supports and funds a privacy function?

As was true in 2016, regulatory and legal compliance is most likely to be rated as the firm's top privacy priority



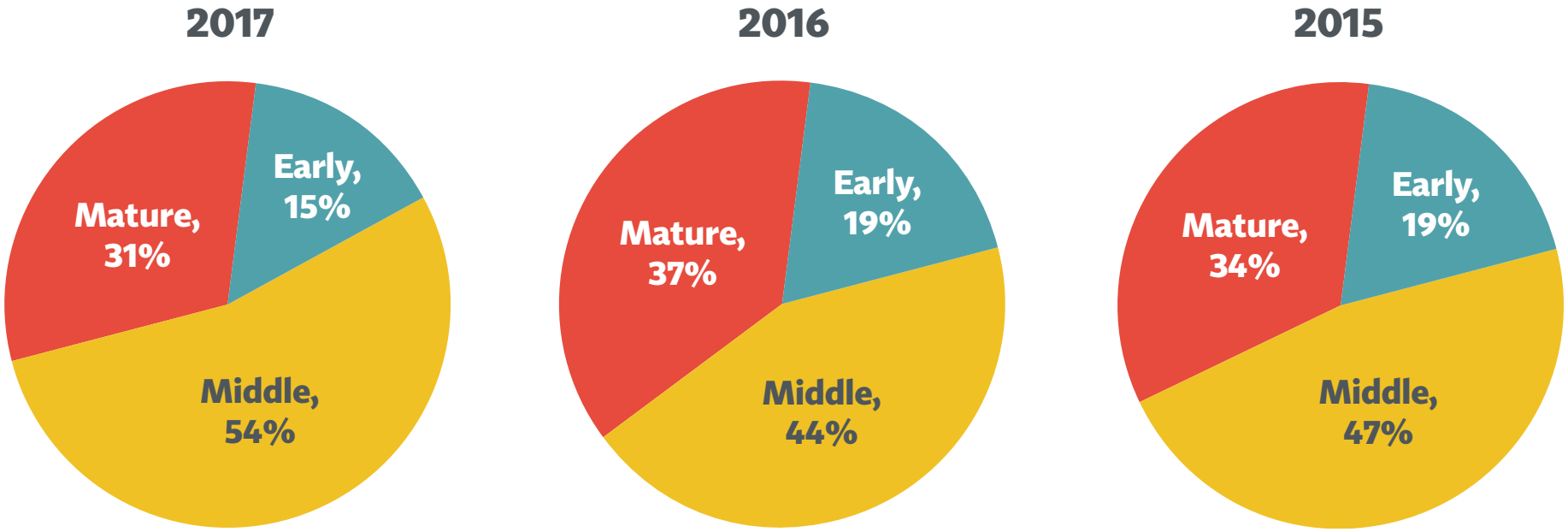
E5: Please rate each for its importance to your company.

2017 shows a 10 point increase in programs describing themselves as in the "middle" of the privacy function lifecycle

- However, the average firm has still only had a dedicated privacy function for 6.4 years, similar to 2016

Privacy Function Lifecycle Stage

Base: Director or Higher



YEARS WITH PRIVACY (MEAN)	2017: 6.4 2016: 6.5 2015: 6.7

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

Companies that are both B2B & B2C are more likely to consider their privacy program "mature"

Privacy Maturity Stage
Responding: Director or Higher

	BY INDUSTRY CATEGORY			BY CUSTOMER TARGET		
	Regulated	Unregulated	Gov't	B2B	B2C	Both
Early	13%	17%	30%	15%	25%	12%
Middle	49%	57%	60%	65%	56%	46%
Mature	38%	26%	10%	19%	20%	42%

Significantly higher than total

Companies with the highest privacy budgets are also the most likely to have mature programs

Privacy Maturity Stage
Responding: Director or Higher

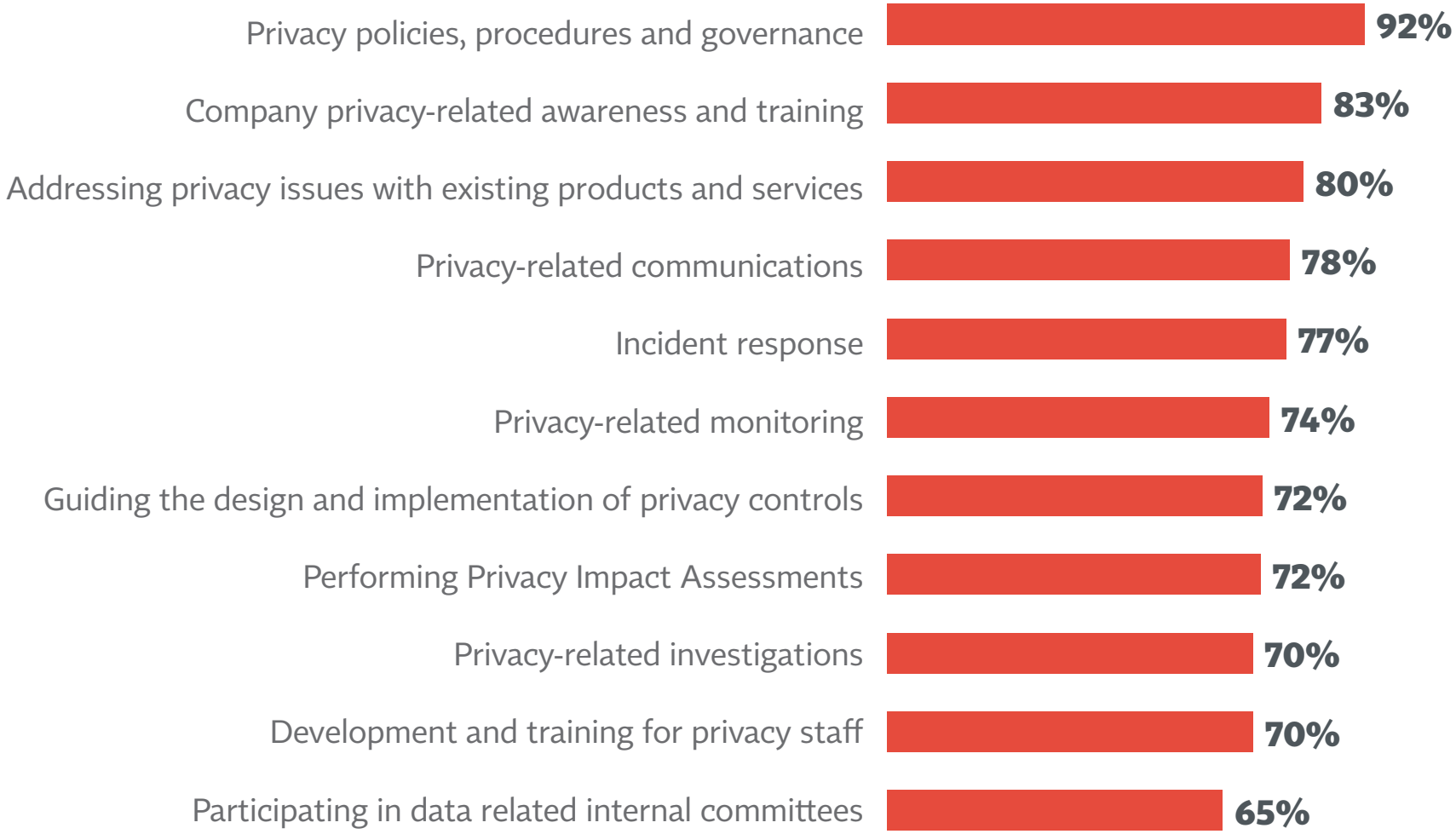
BY PRIVACY BUDGET
(Excluding Salaries)

	$1-$100K	$101K-$1 million	More than $1 million
Early	14%	13%	6%
Middle	63%	58%	42%
Mature	23%	29%	51%

Significantly higher than total

Privacy's range of responsibilities, led by policies, procedures, and governance, is annually consistent

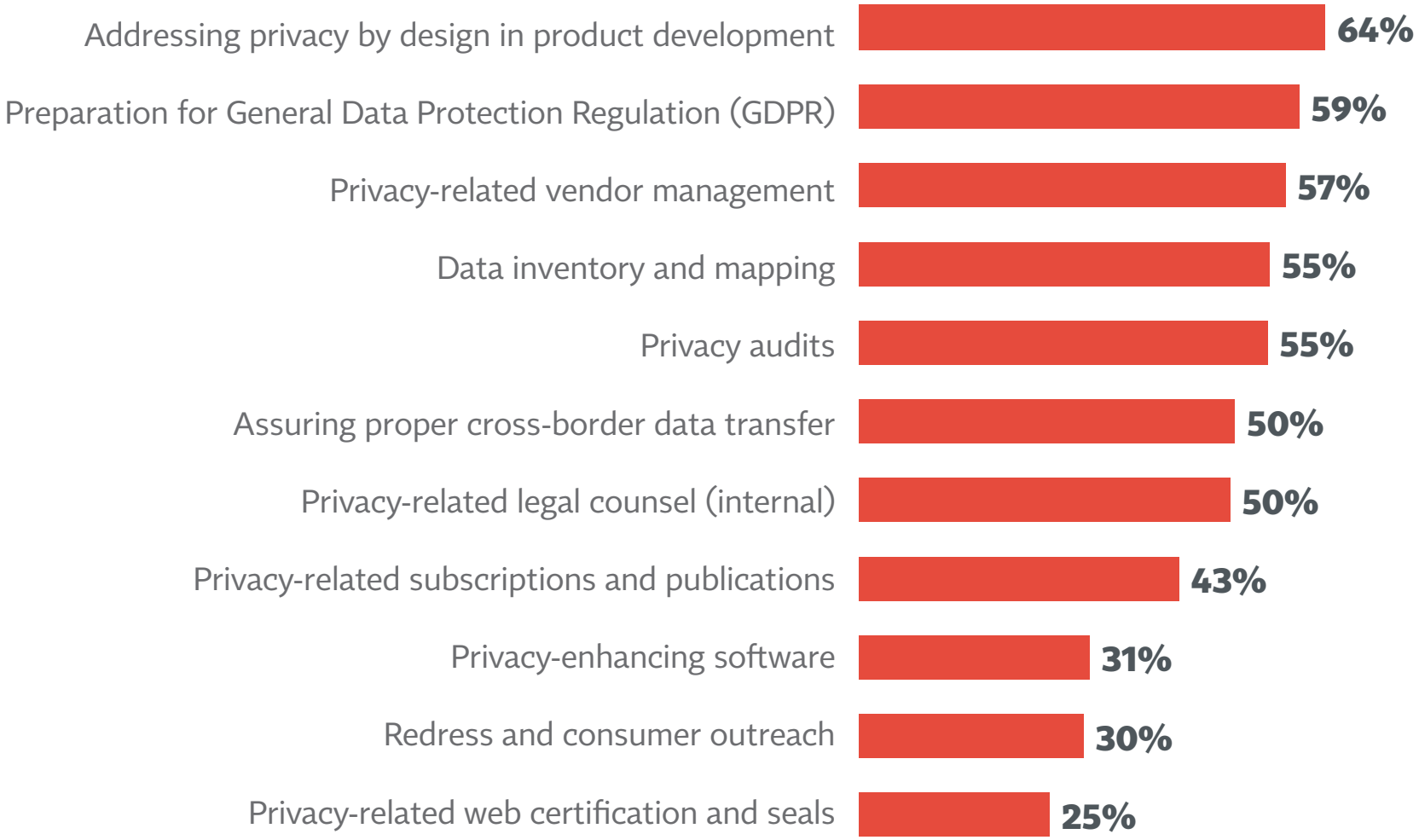
Top Privacy Team Responsibilities
Base: Director or Higher



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

GDPR preparation and cross-border data transfer are now responsibilities for more than half of privacy teams

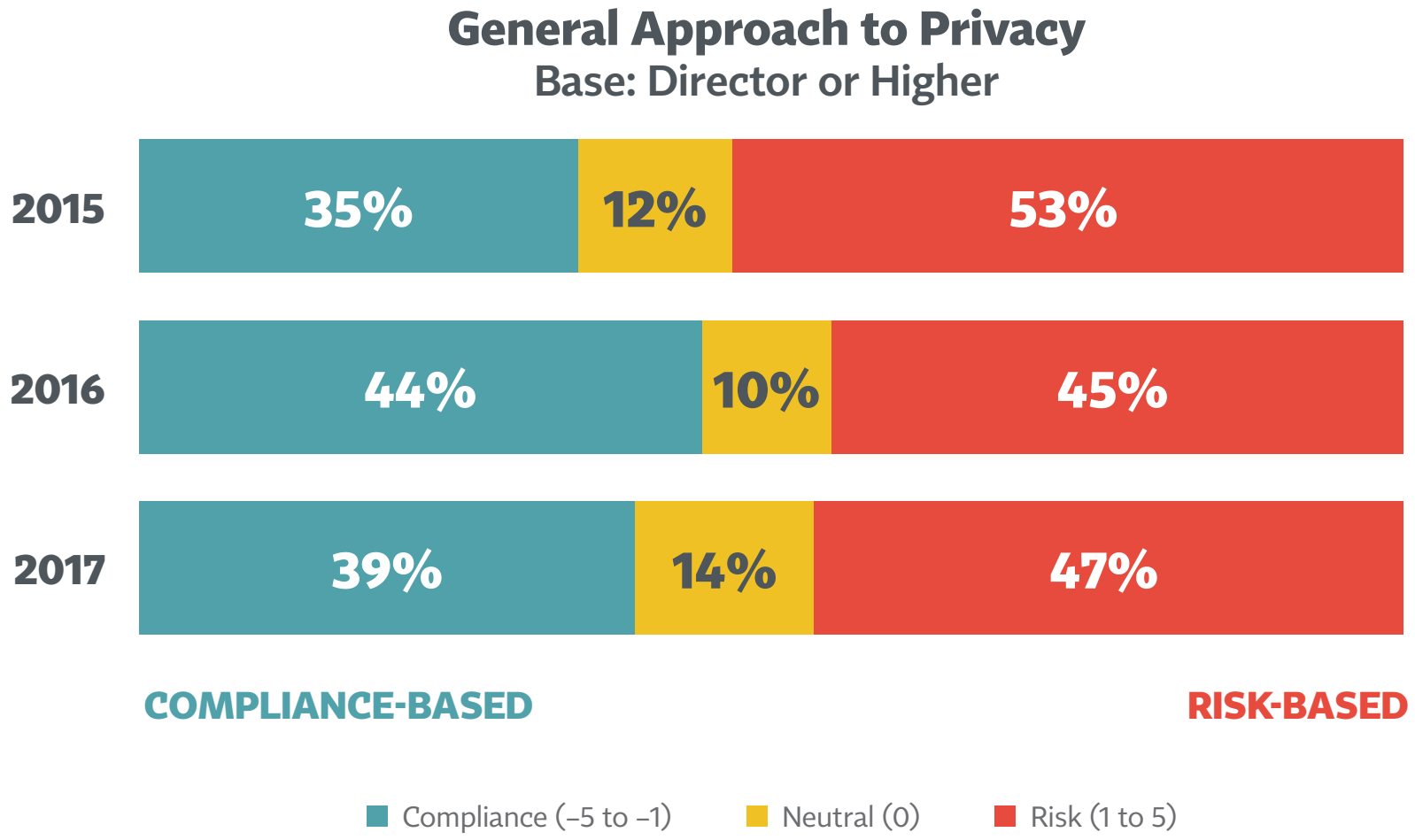
Secondary Team Responsibilities
Base: Director or Higher



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

Privacy professionals in 2017 report a slight shift away from a compliance focus, toward a risk focus

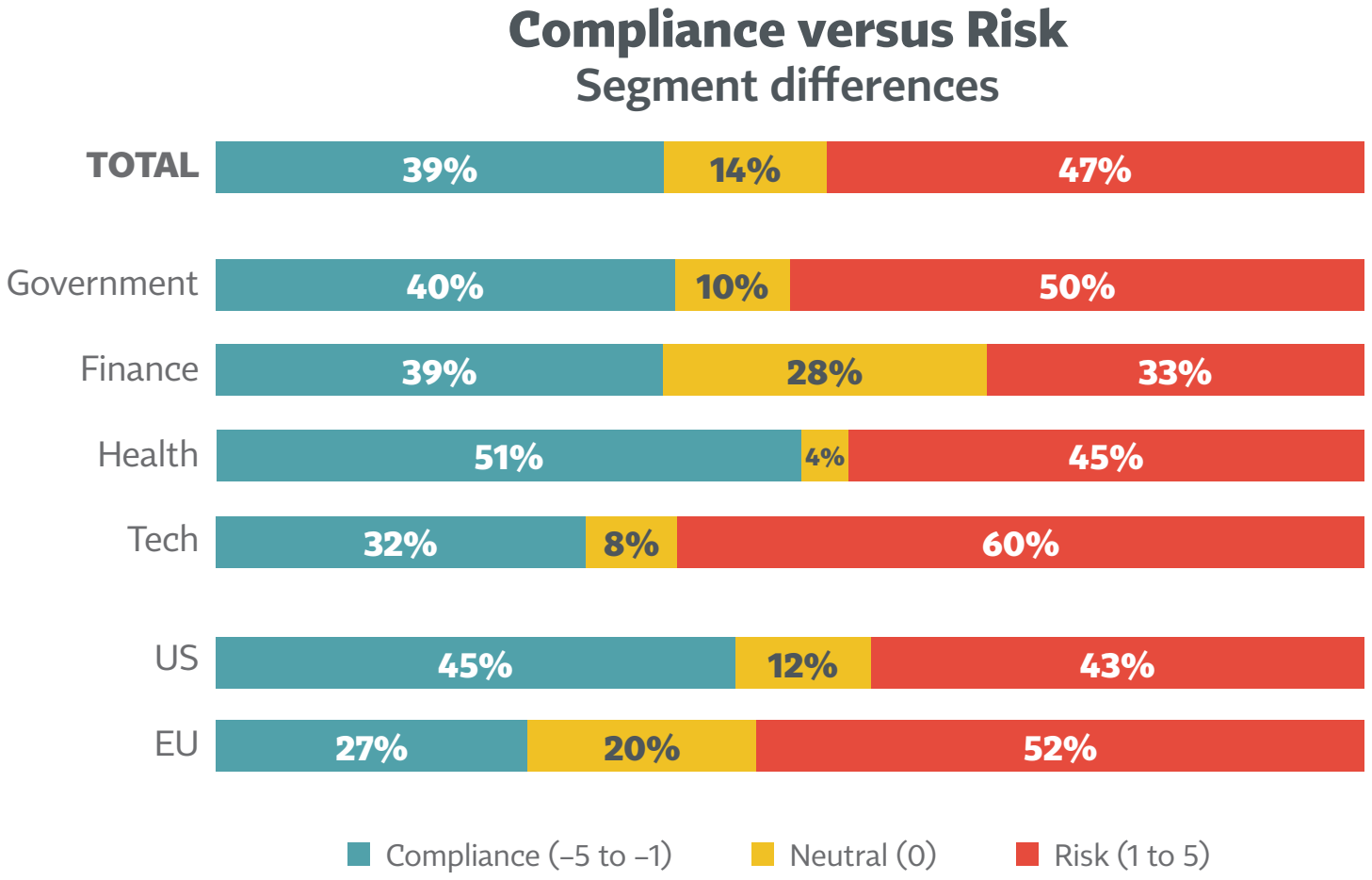
- Note that most professionals cluster toward the center on this scale: 63% are within plus or minus 2 points of the midpoint



E8: Please use the slider below to indicate where your company falls on this spectrum between compliance-based or risk-based.

Tech and EU firms are the most likely to be risk-focused in their privacy functions

- Health care and US firms are more likely than others to focus on regulatory compliance



E8: Please use the slider below to indicate where your company falls on this spectrum between compliance-based or risk-based.

EU firms are more likely than US firms to cite compliance as a reason for having a privacy function

- Compliance and data breaches are the main reasons for privacy in finance and health care firms, while tech firms use privacy more for client and competitive reasons

Privacy Group Responsibilities:
Segments with Higher Than Average Results

BY GEOGRAPHY

	US	EU
Main Reasons for Privacy: Increase revenues	15%	6%
Main Reasons for Privacy: Compliance with EU GDPR	50%	75%

BY INDUSTRY

	Finance	Health	Tech
Main Reasons for Privacy: Compliance	98%	100%	89%
Main Reasons for Privacy: Reduce the risk of data breach	85%	81%	66%
Main Reasons for Privacy: Meet client expectations	65%	69%	84%
Main Reasons for Privacy: Competitive differentiator	24%	19%	39%
Main Reasons for Privacy: Increase data value	18%	16%	35%

Significantly higher than total

Compliance (including for GDPR) is an especially strong reason for large firms to have a privacy function

- As in 2016, those in mature privacy functions are more likely to cite a variety of reasons for having a privacy practice

Privacy Group Responsibilities:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Main Reasons for Privacy: Compliance	85%	91%	96%	100%
Main Reasons for Privacy: Compliance with the EU General Data Protection Regulation	44%	48%	65%	75%
Main Reasons for Privacy: Competitive differentiator	36%	17%	23%	20%

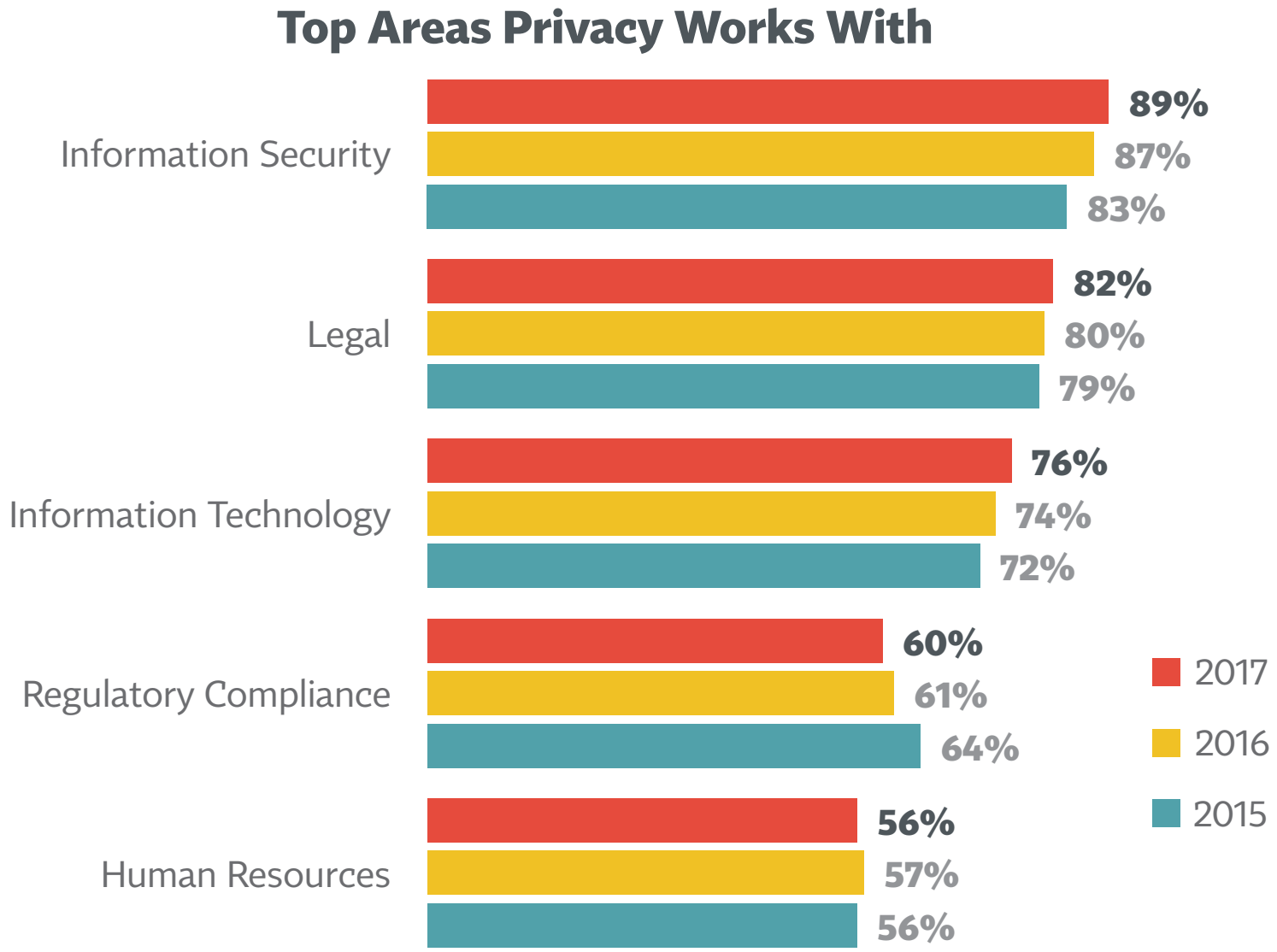
BY PRIVACY LIFESTAGE

	Early/ Middle	Mature
Main Reasons for Privacy: Meet consumer expectations	56%	72%
Top 3 importance rating: Increasing consumer trust	57%	74%
Top 3 importance rating: Ethical decision-making concerning use of data	54%	75%
Top 3 importance rating: Maintaining or enhancing the value of information assets	48%	72%

Significantly higher than total

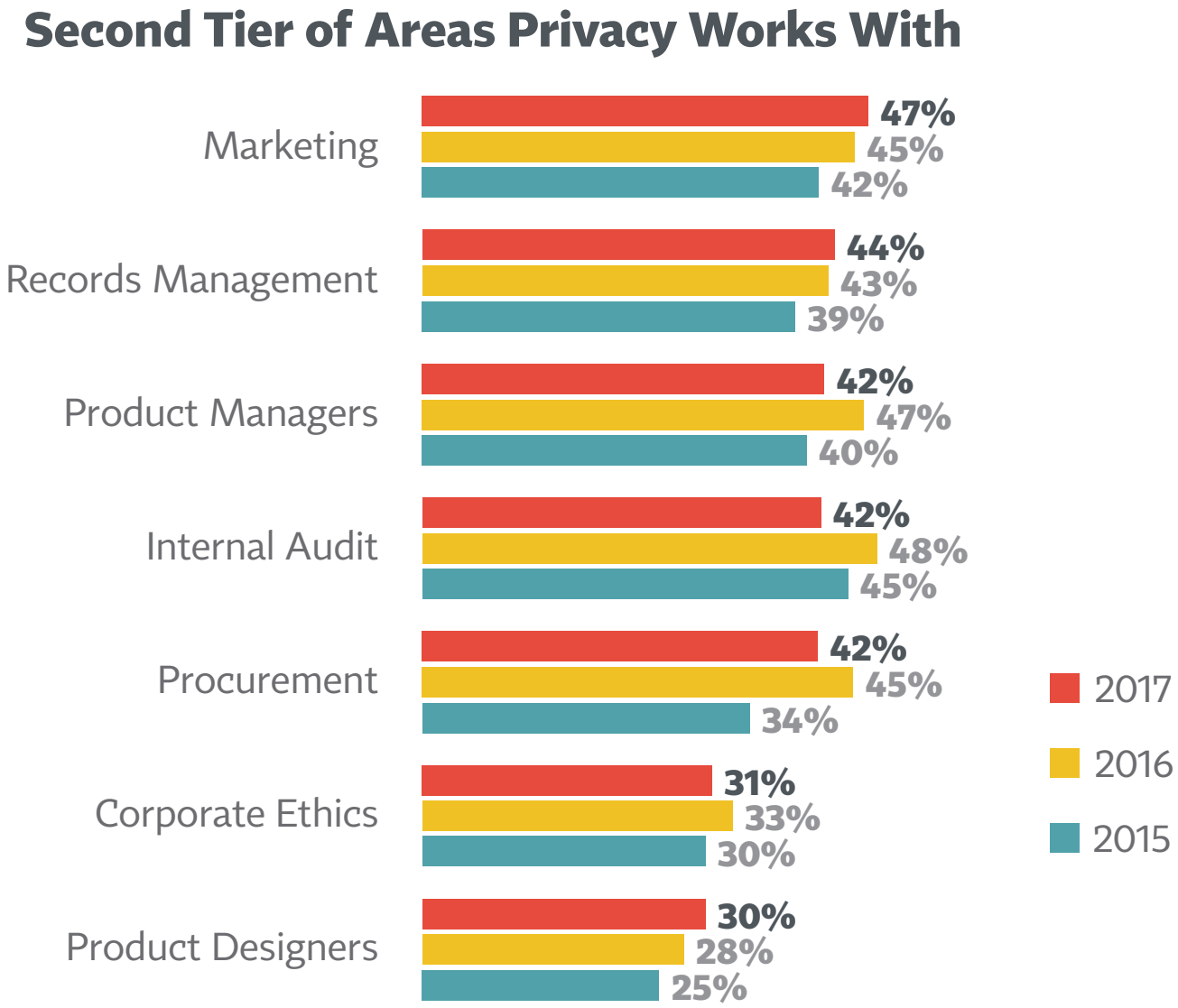
Contents

We've seen incremental increases since 2015 in the percent saying privacy works with IS, legal, and IT



G1: First, thinking about your day-to-day work, with which of the following functions do you interact on a regular basis?

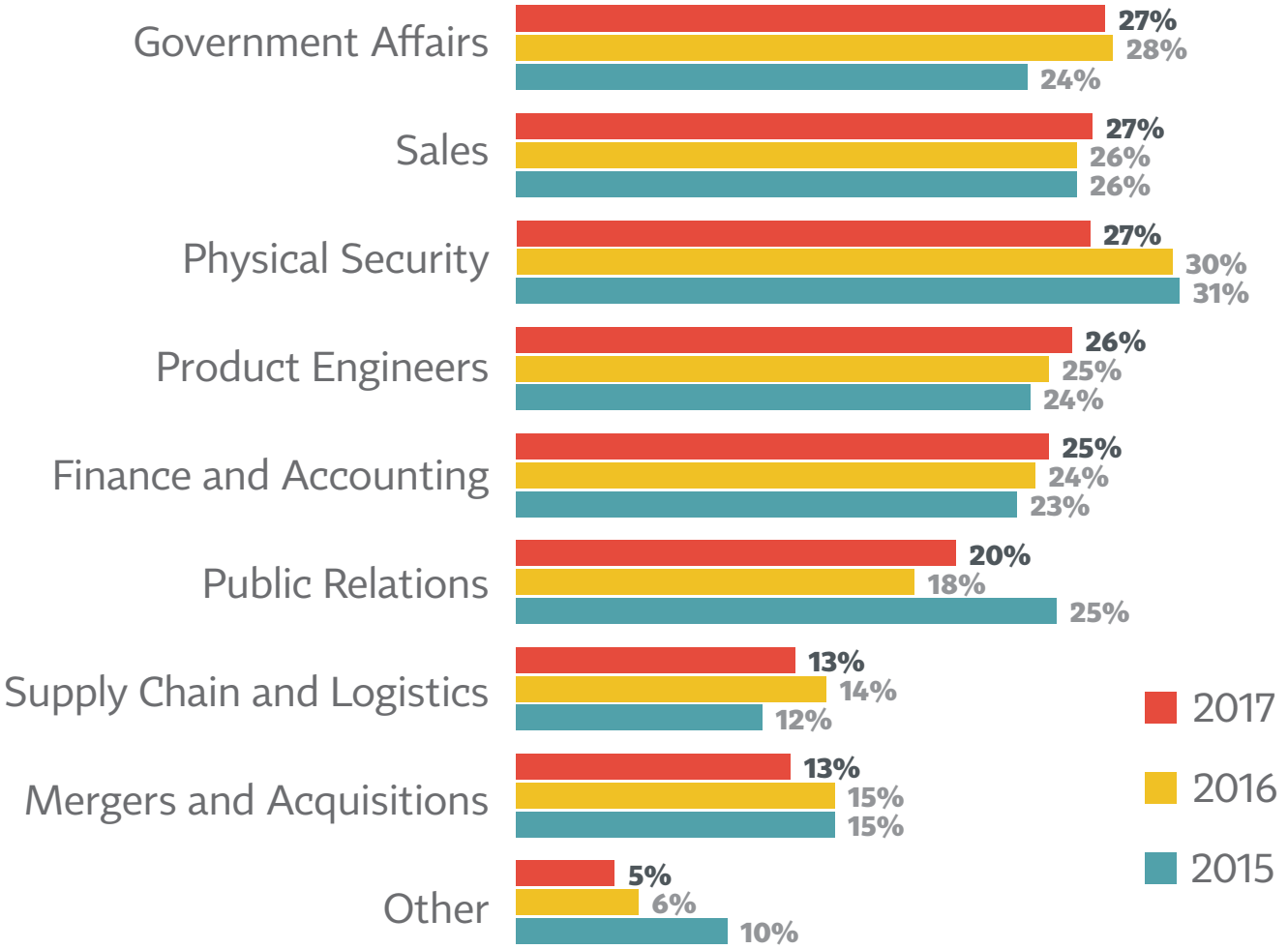
Marketing and Records Management are two functions seeing directional increases since 2015



G1: First, thinking about your day-to-day work, with which of the following functions do you interact on a regular basis?

As we've seen in past years, privacy functions are least likely to work with supply chain and M&A groups

Areas Privacy Is Least Likely to Work With

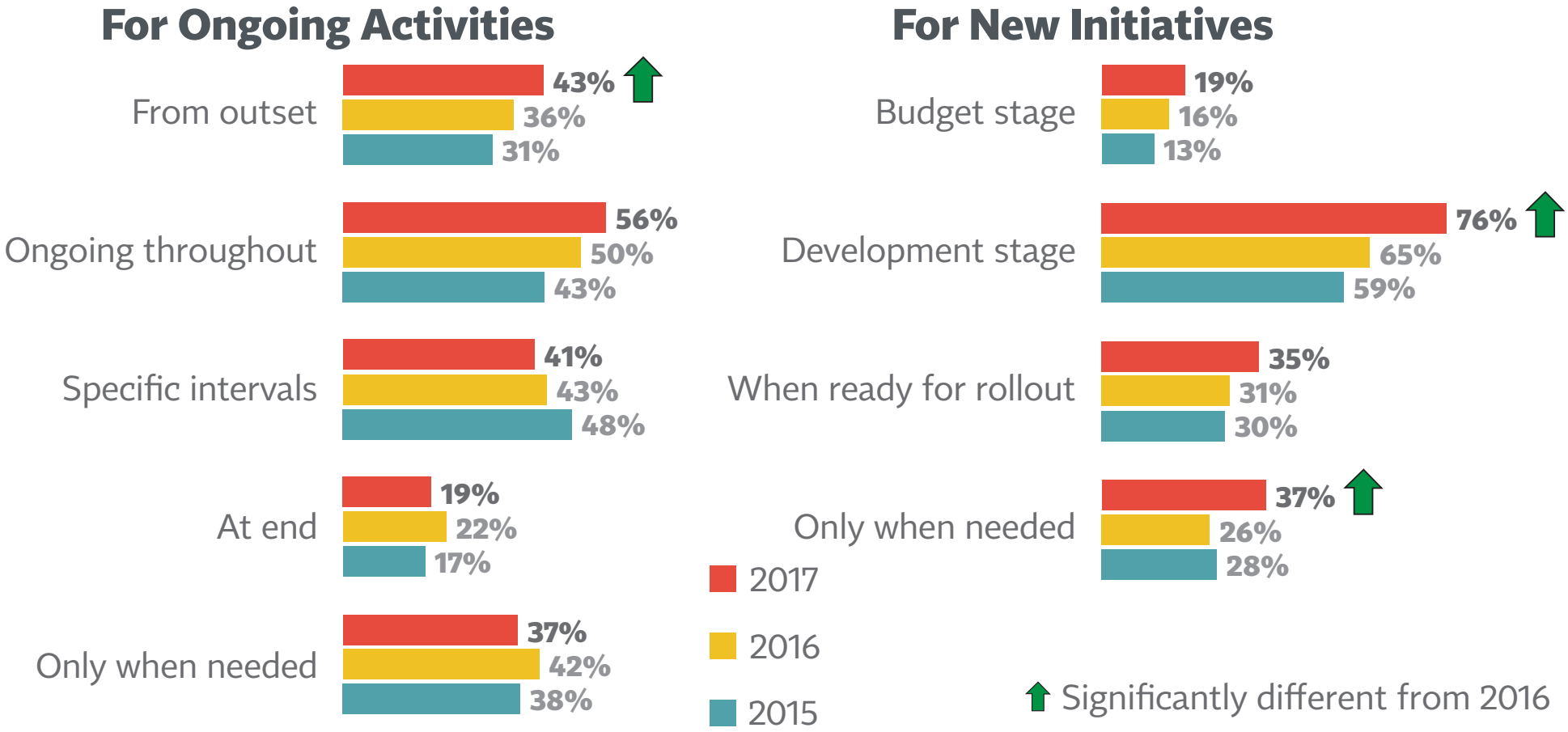


G1: First, thinking about your day-to-day work, with which of the following functions do you interact on a regular basis?

2017 sees significant increases in those saying that privacy is involved "at the outset" of ongoing activities

- For new initiatives, we see an 11 point jump in those saying privacy is involved at the development stage: to 76%

Privacy Involvement in Initiatives

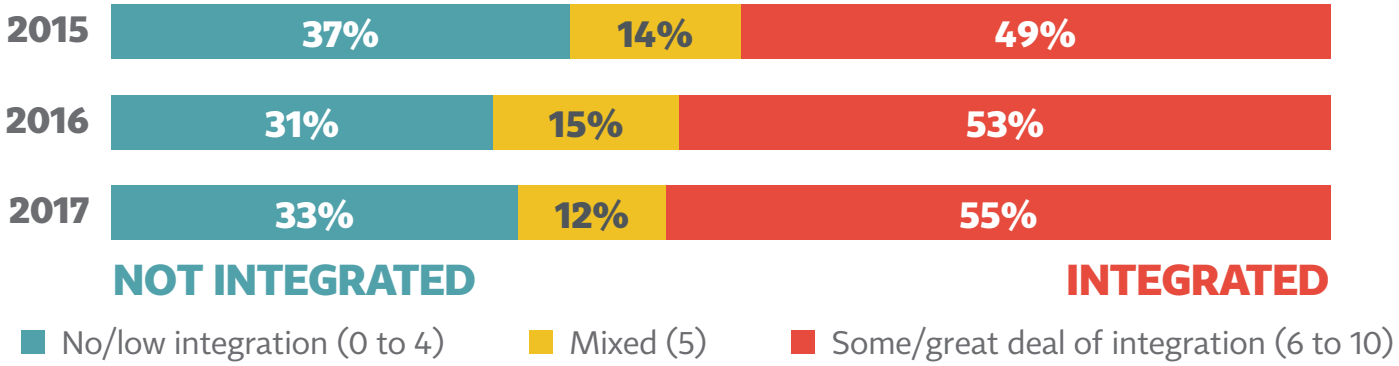


G5: In a general sense, for ongoing activities within your company that may involve privacy-related information, representatives of the privacy function are involved …
G6: Now thinking about new projects or initiatives established by your company that may involve privacy-related information, representatives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

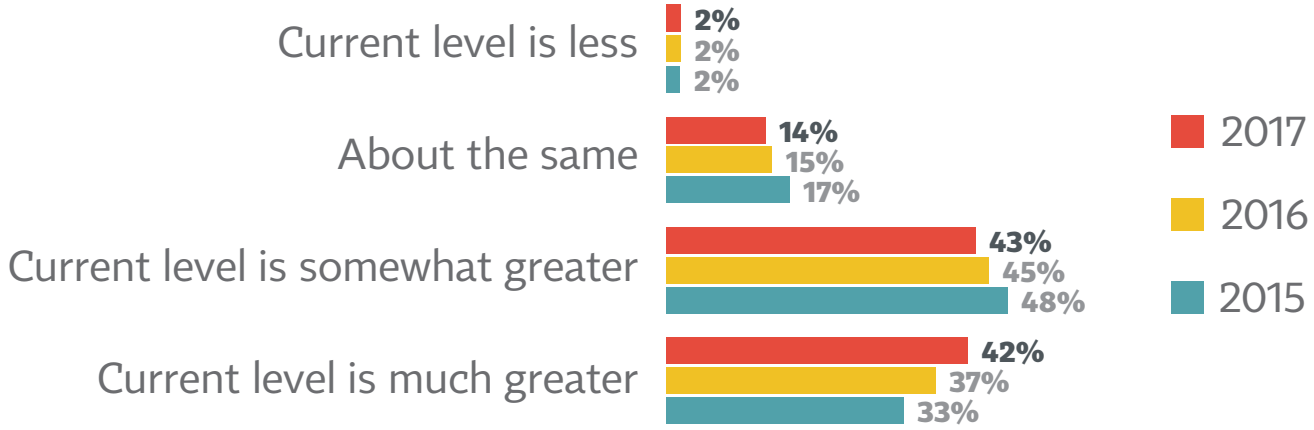
Increases continue for those saying privacy is involved in planning/implementation to at least some extent

- Plus, 42% say integration is "much greater" today than a few years ago, up 5 points

Privacy Integration in Planning and Implementation



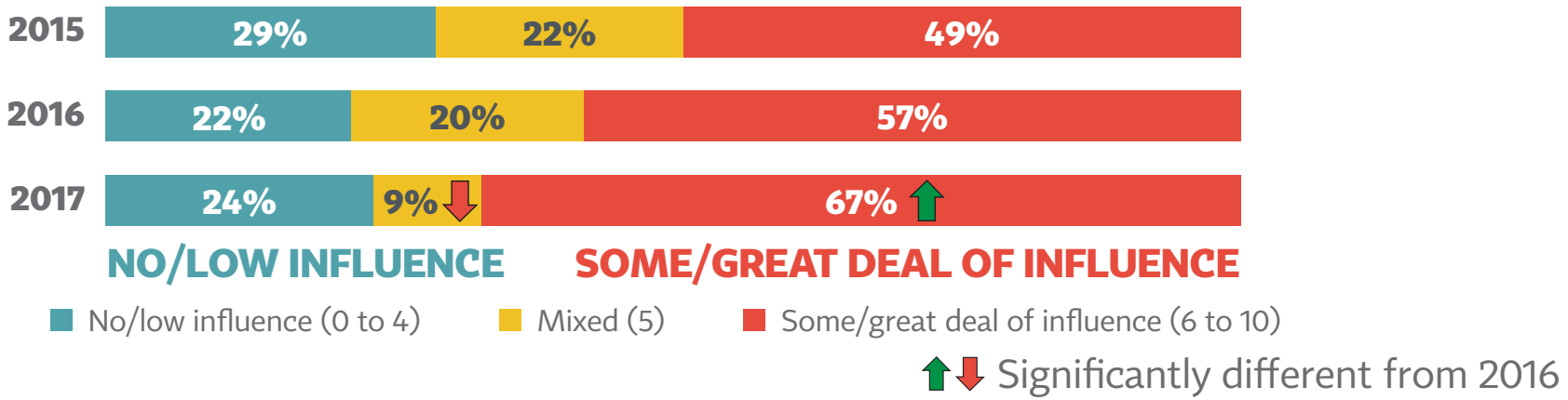
Current Integration Level vs. A Few Years Ago



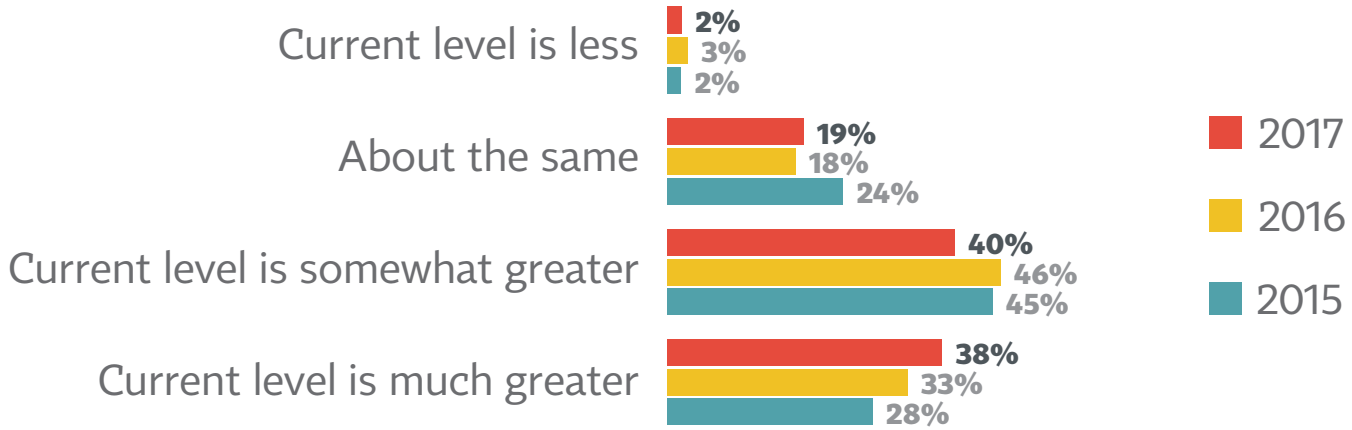
G7: To what extent would you say those in the privacy function of your company are integrated into the planning and implementation of initiatives that involve privacy-related information?
G8: This level of integration is …

After an 8-point jump, the percent saying privacy has influence on initiative planning is up another 10 points

Privacy Influence on Planning and Implementation



Current Influence Level vs. A Few Years Ago



G9: How would you describe the degree of influence those in the privacy function of your company have over planning and implementation of initiatives?
G10: This level of influence is …

The largest firms and mature privacy functions are the most likely to say privacy is involved from the start

Privacy Group in Business Context:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Ongoing activities: Involved at the outset	42%	37%	38%	55%
New initiatives involvement: At rollout	32%	31%	31%	49%

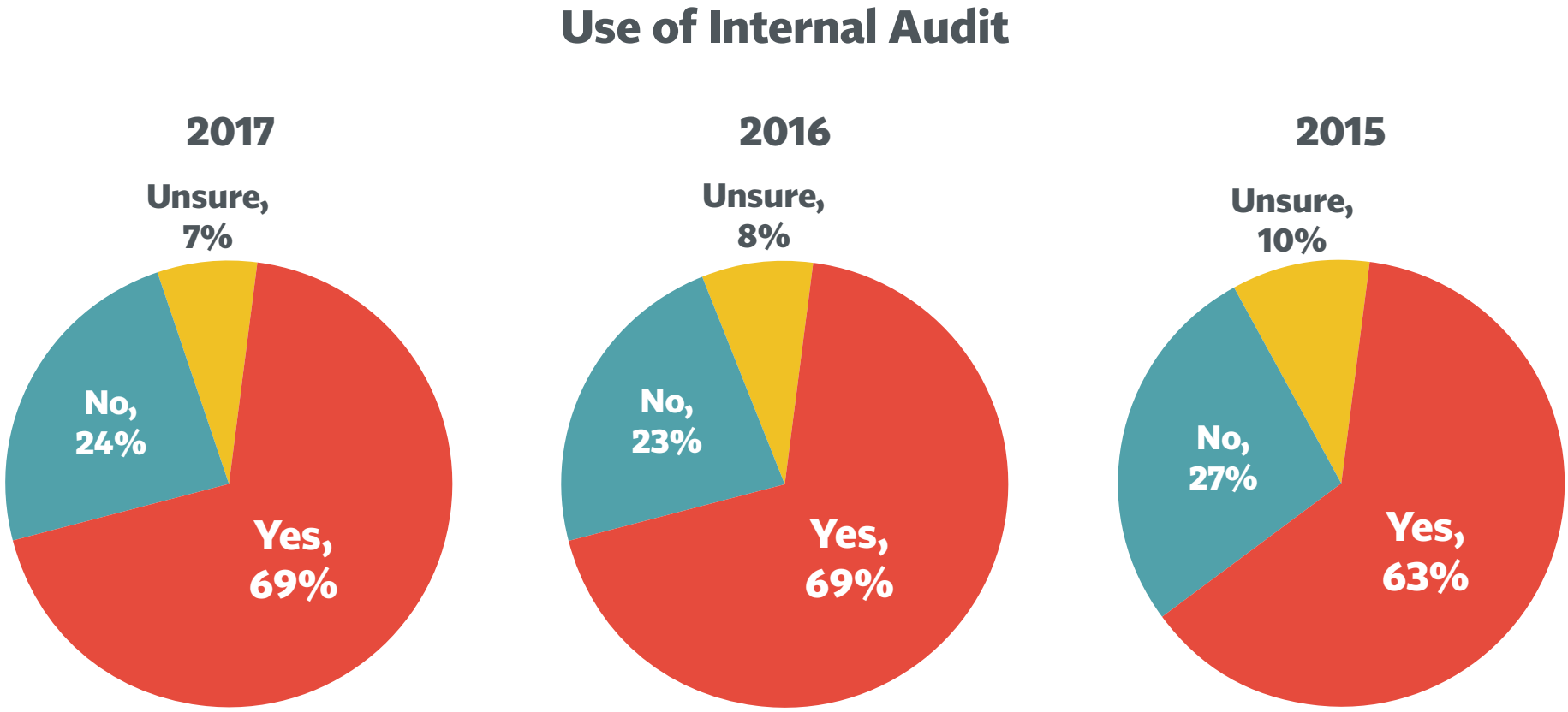
BY PRIVACY LIFESTAGE

	Early/Middle	Mature
New initiatives: Involved at development stage	76%	90%

Significantly higher than total

Contents

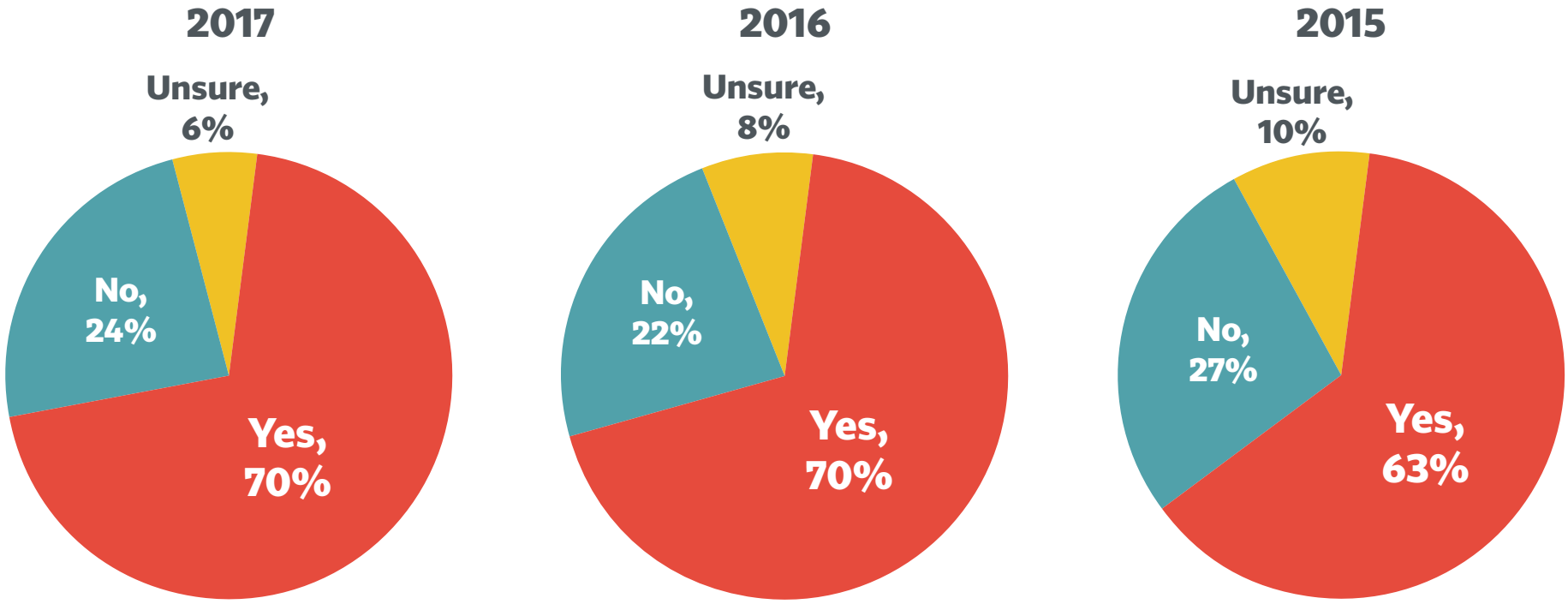
Use of Internal Audits has remained unchanged from 2016



H2: Does your company use internal audit for privacy audits?

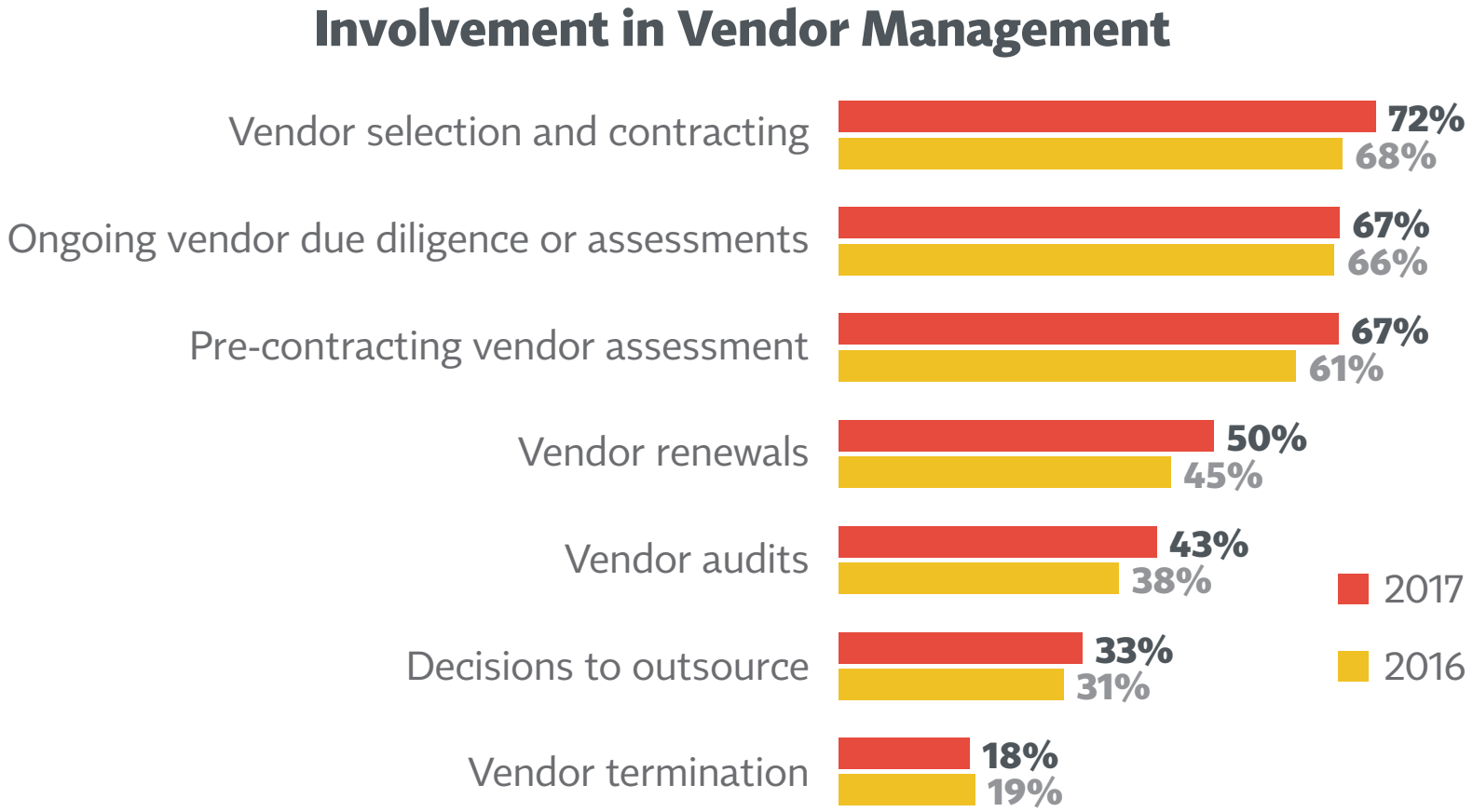
Vendor Management Program use has also stayed the same since last year

Have Vendor Management Program



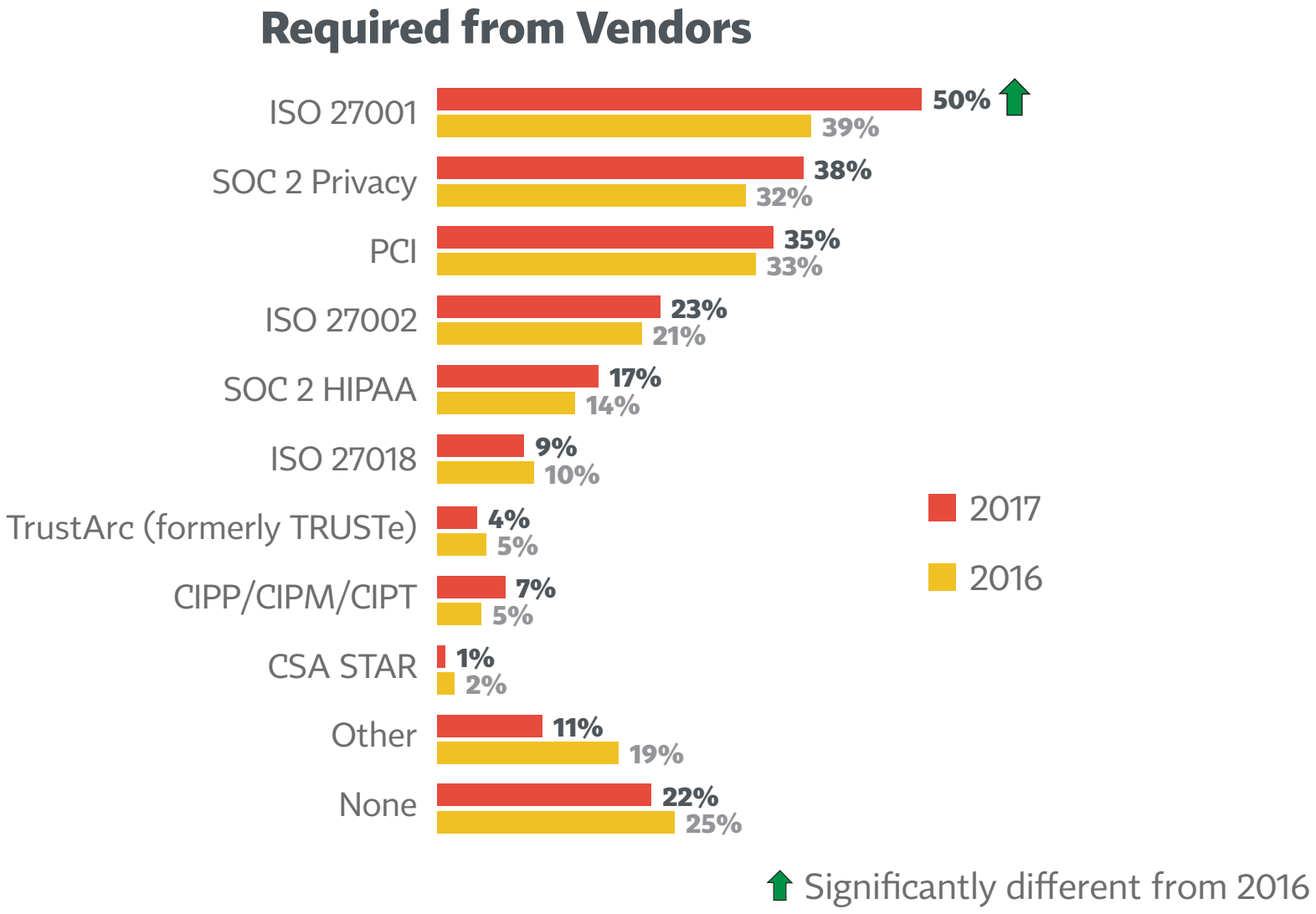
H7: Does your company have a vendor management program designed to ensure the privacy and/or security practices of vendors will not threaten the integrity of your company's privacy standards?

As part of the Vendor Management process, privacy is most involved in selection, due diligence, and assessments



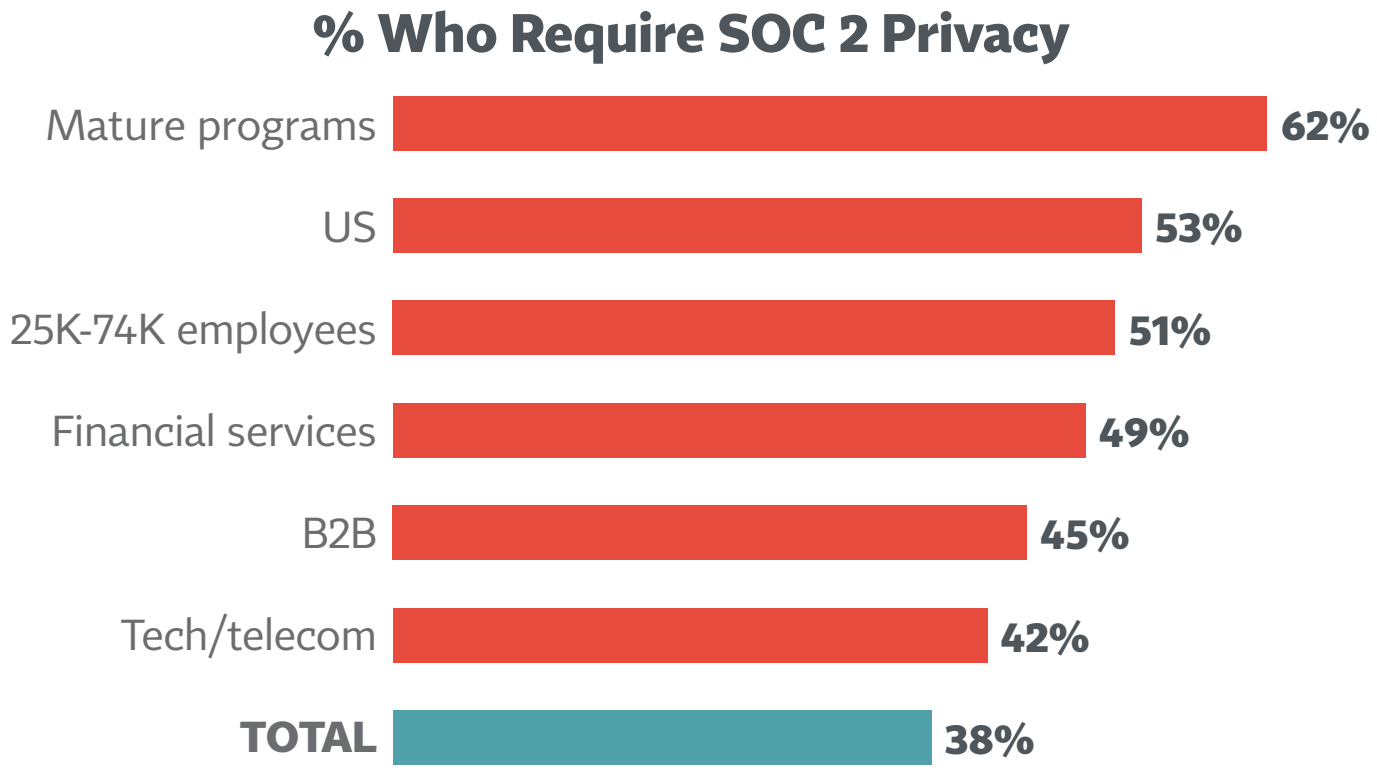
H7d: Which stages of the vendor management lifecycle is the privacy function involved in?

ISO 27001 certification, most likely to be required in 2016, is even more likely to be a requirement in 2017



H7g: Which, if any, third party audits or certifications does your organization require from vendors?

Mature programs, along with US and upper-mid-sized firms, are most likely to require SOC 2 Privacy



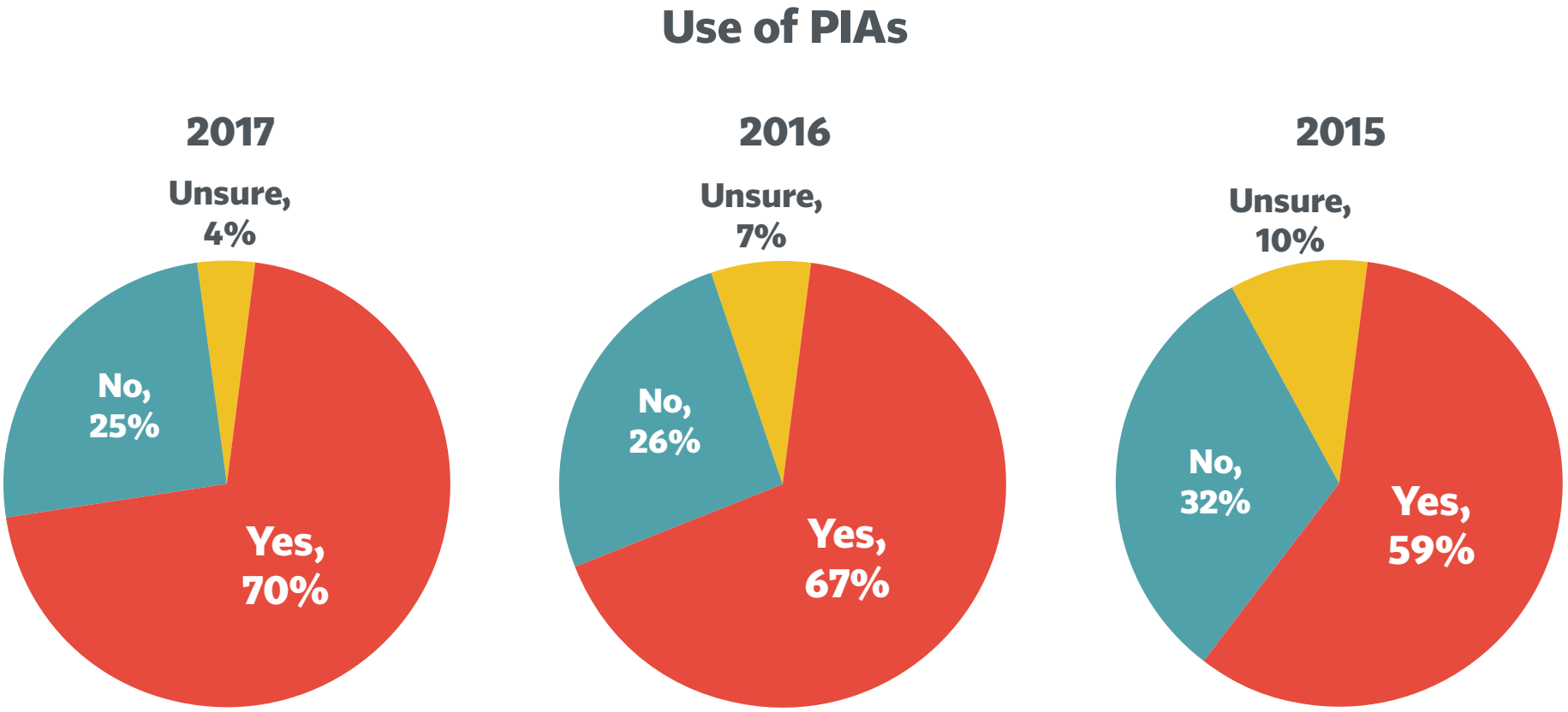
ISO 27001 is much more common in unregulated firms, and firms are more likely to require it than in 2016

Audits and Certifications
Responding: Director or Higher

			BY INDUSTRY CATEGORY		BY CUSTOMER TARGET		
	2017	2016	Regulated	Unregulated	B2B	B2C	Both
ISO 27001	50%	39%	50%	60%	54%	45%	50%
SOC2 Privacy	38%	32%	41%	39%	45%	28%	37%
PCI	35%	33%	28%	40%	22%	43%	43%
ISO 27002	23%	21%	26%	23%	20%	23%	26%
SOC 2 HIPAA	17%	14%	18%	17%	20%	9%	19%
ISO 27018	9%	10%	8%	9%	13%	6%	7%

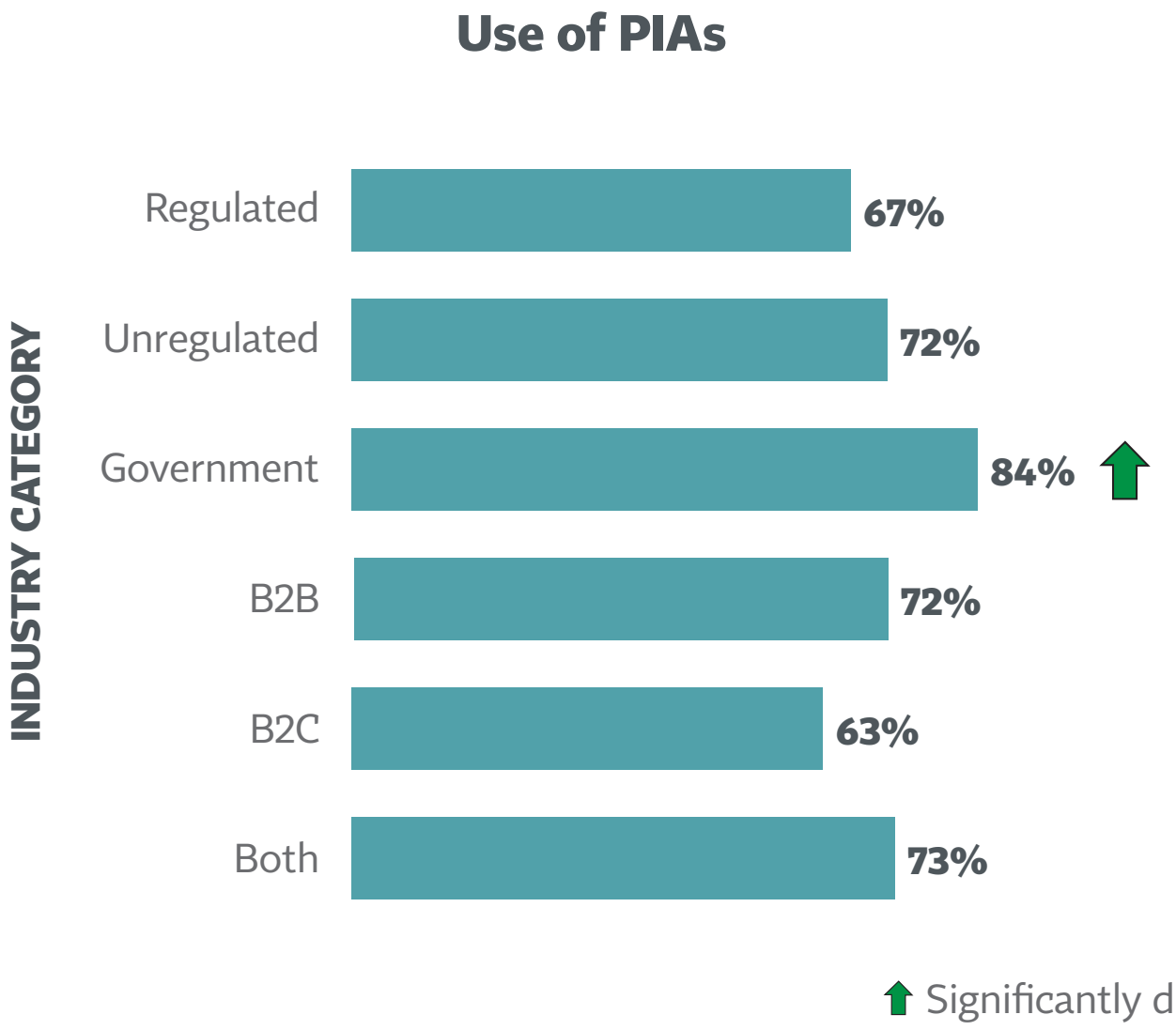
Significantly higher than total

Use of Privacy Impact Assessments is up directionally from 2016, to 70% of respondents



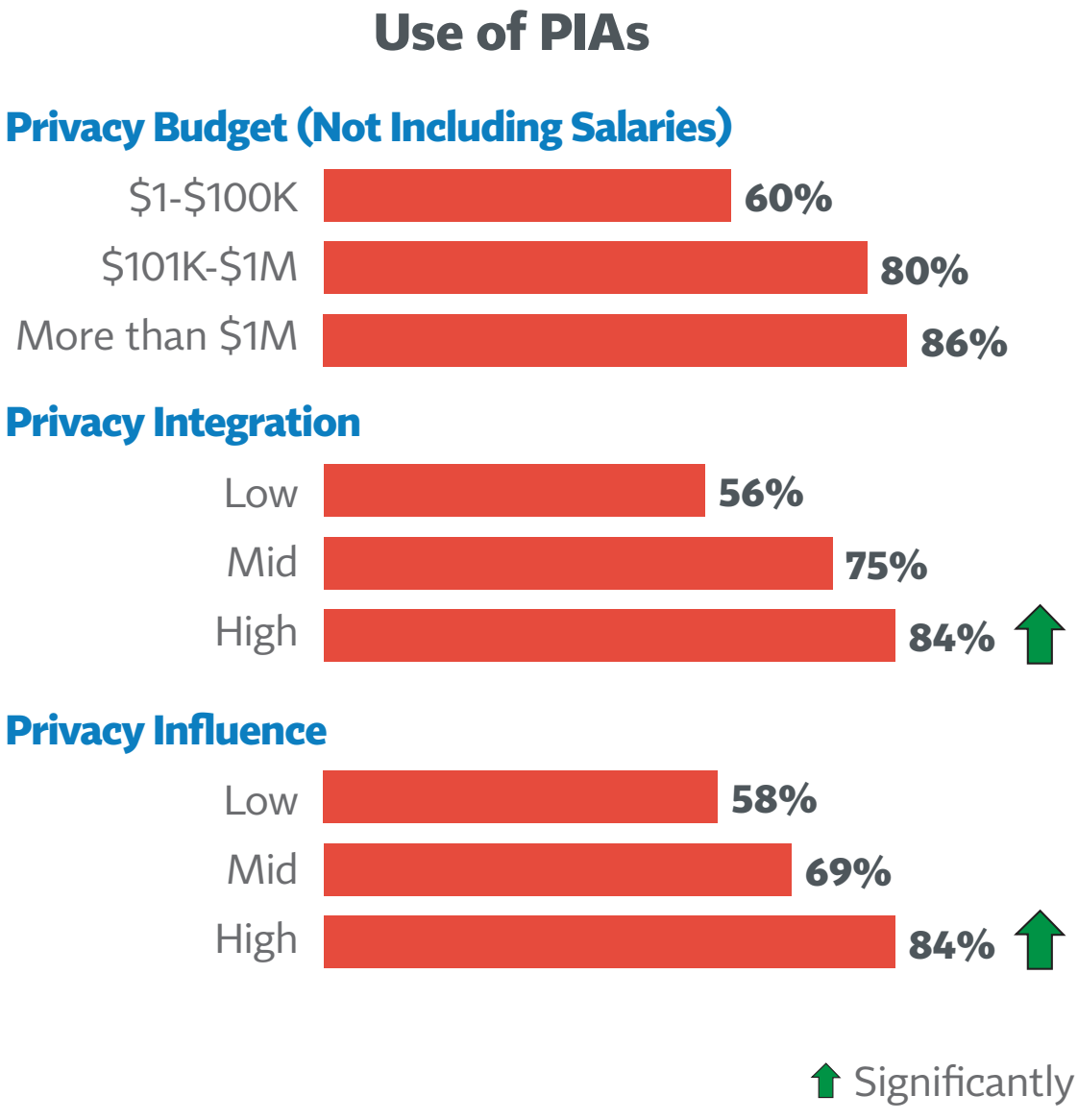
H16: Does your company use Privacy Impact Assessments (PIAs)?

Privacy Impact Assessments are most often used in government agencies



H16: Does your company use Privacy Impact Assessments (PIAs)?

PIAs are also common in firms with high privacy budgets and in firms with strong privacy integration



H16: Does your company use Privacy Impact Assessments (PIAs)?

Financial firms are more likely than average to use Internal Audit or have Vendor Management Programs

- US firms are more likely to have Vendor Management and require SOC 2 certification; EU firms are more likely to use PIAs and require ISO 27001

Internal and External Resources:
Segments with Higher Than Average Results

BY GEOGRAPHY

	US	EU
Vendor management program	74%	71%
Privacy Impact Assessments	63%	79%
Stages of vendor management cycle privacy is involved in		
Decisions to outsource	25%	45%
Vendor selection and contracting	68%	80%
Third party audits required		
ISO 27001	46%	68%
SOC 2 Privacy	53%	11%
SOC 2 HIPAA	23%	8%

BY INDUSTRY

	Gov't	Finance	Health	Tech
Internal audit	58%	85%	67%	69%
Vendor management program	48%	88%	71%	75%

Significantly higher than total

Larger firms and mature programs are more likely to use all of these tools

Internal and External Resources:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Internal audit	58%	69%	78%	83%
Vendor management program	56%	75%	81%	85%
Privacy Impact Assessment	60%	65%	83%	88%

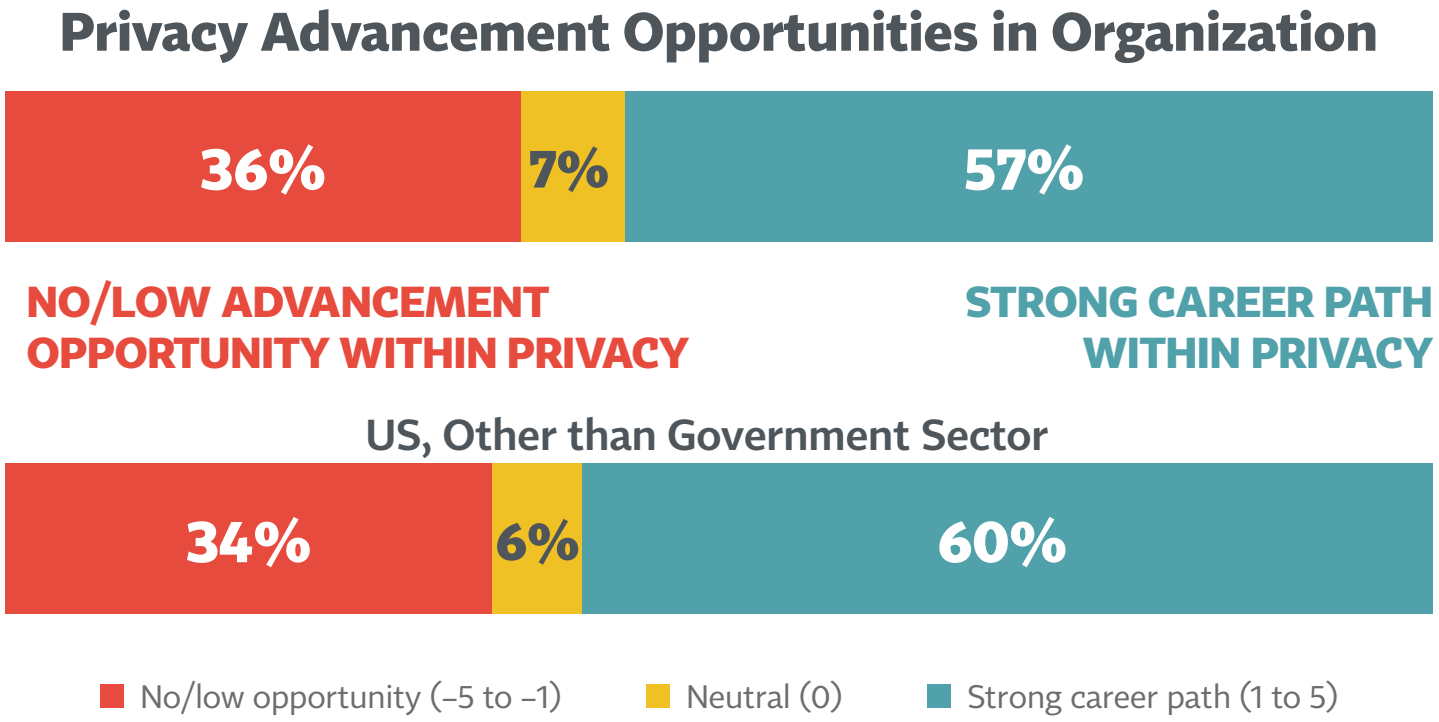
BY PRIVACY LIFESTAGE

	Early/Middle	Mature
Internal audit	67%	89%
Vendor management program	69%	89%
Privacy Impact Assessments	64%	90%
Third party audits required		
SOC 2 Privacy	41%	62%

Significantly higher than total

Contents

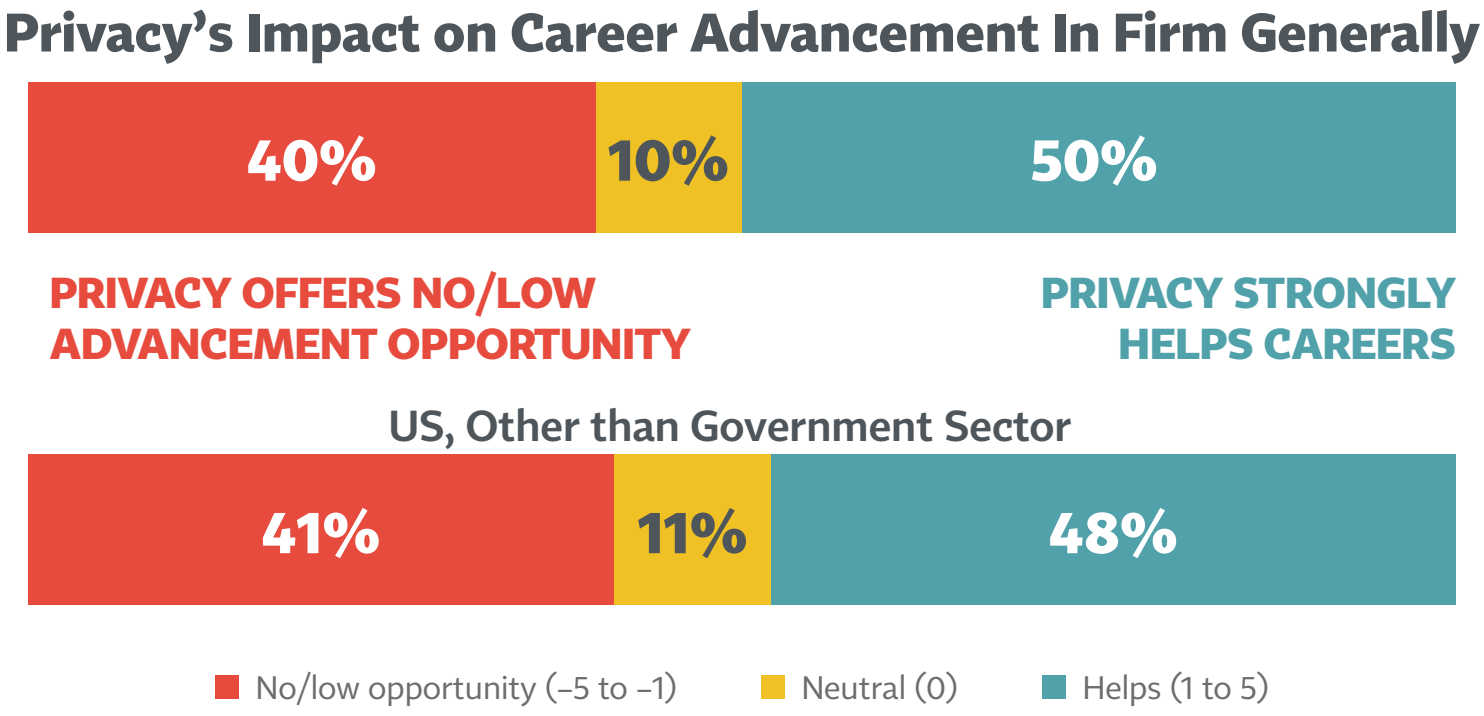
About 6 in 10 give a positive rating to privacy as a career track in their firm, unchanged from 2016



E9: Please use the slider below to indicate the extent to which you view privacy as a career track at your organization.

Half say that working in privacy helps one's general career chances within their firm

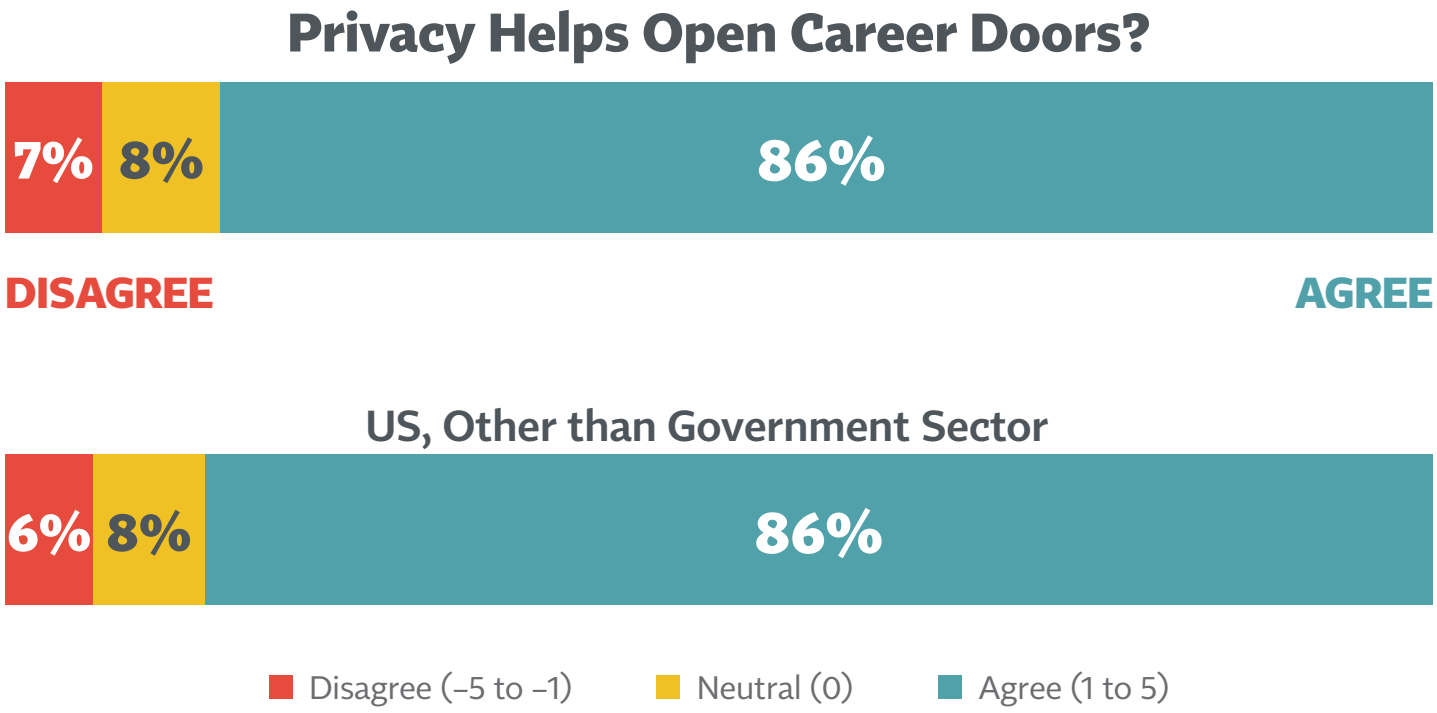
- That proportion is actually down a directional 8 points from last year. In addition, the 40% saying privacy offers low opportunity is a significant 13 points higher



E10: Again, please use the slider below to indicate the extent to which privacy roles can advance careers at your company in general (that is, not necessarily within the privacy program).

As was the case in 2016, close to 90% say privacy opens doors for career opportunities generally

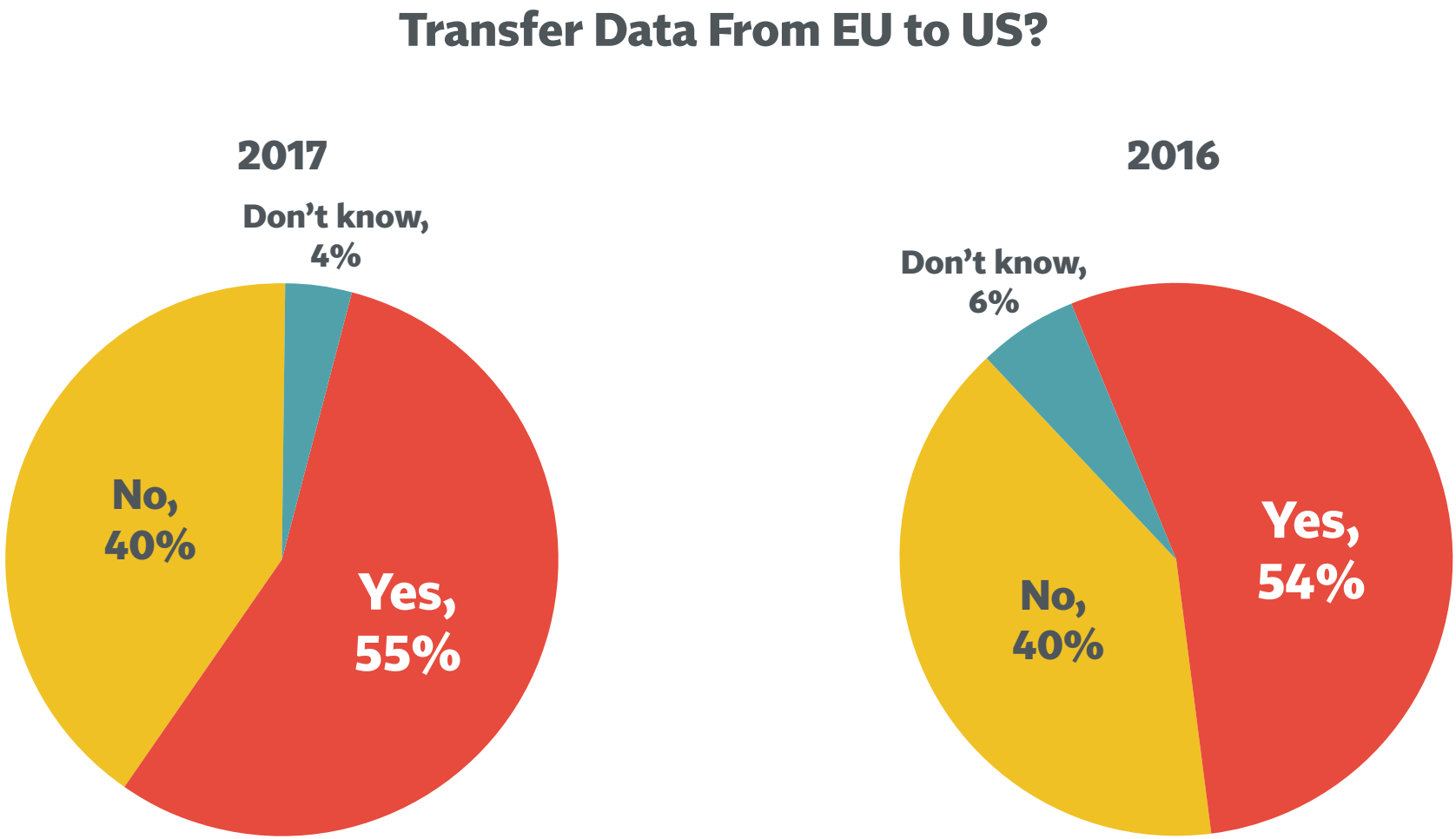
- That is, career opportunities **outside** one's own firm



E11: Please indicate the degree to which you agree or disagree with the following statement: Doing well in privacy will open doors for better and better job opportunities in the marketplace.

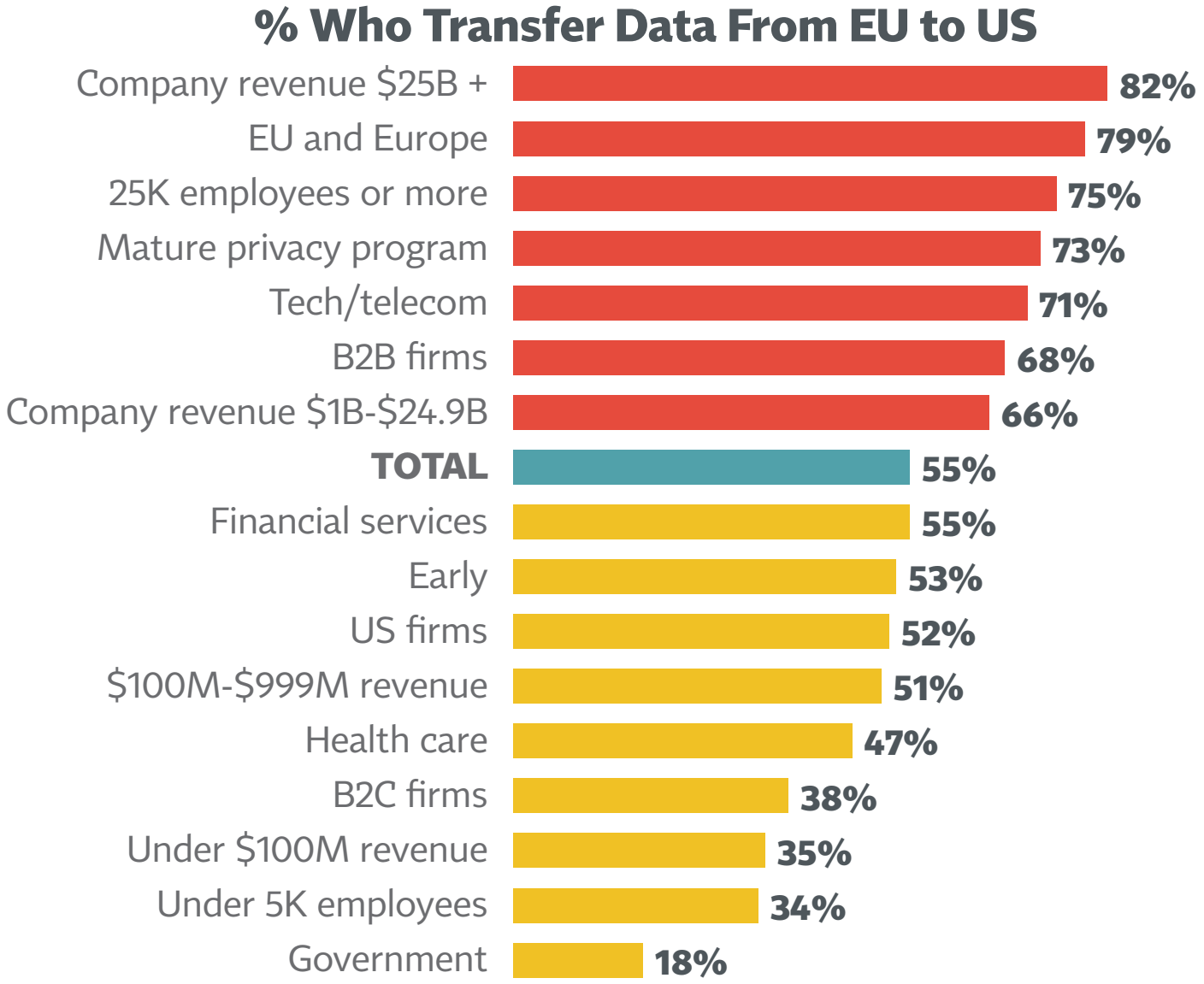
Contents

A bit over half of firms transfer personal data from the EU to the US, statistically unchanged from last year



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

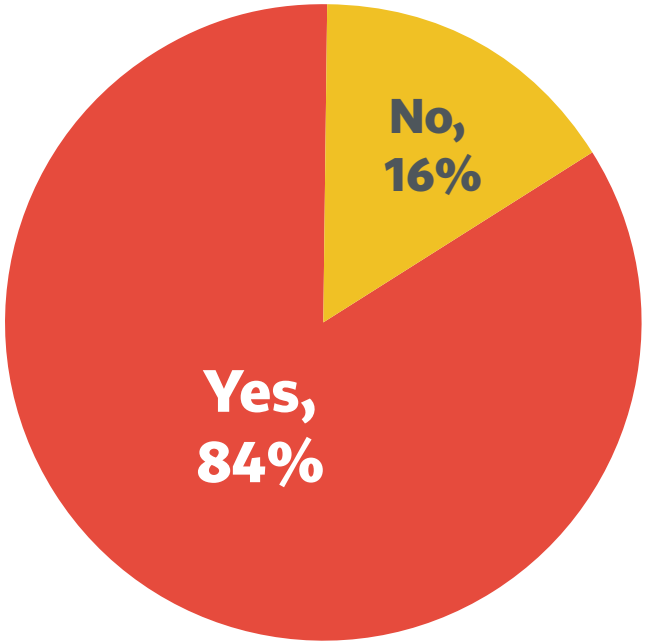
Cross border data transfer is most common in the largest firms, in the EU, and in mature privacy programs



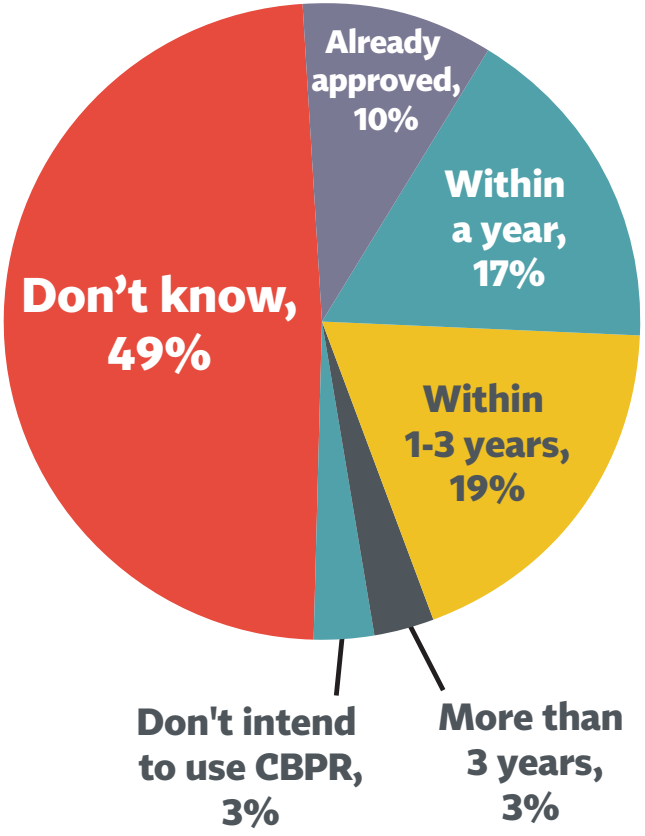
J1: Does your organization transfer personal information from the European Union to the United States?

Only 16% of firms will apply for CBPR; of those, nearly half don't know when they'll get application approval

Will Apply for CBPR?



When Expect Approval?

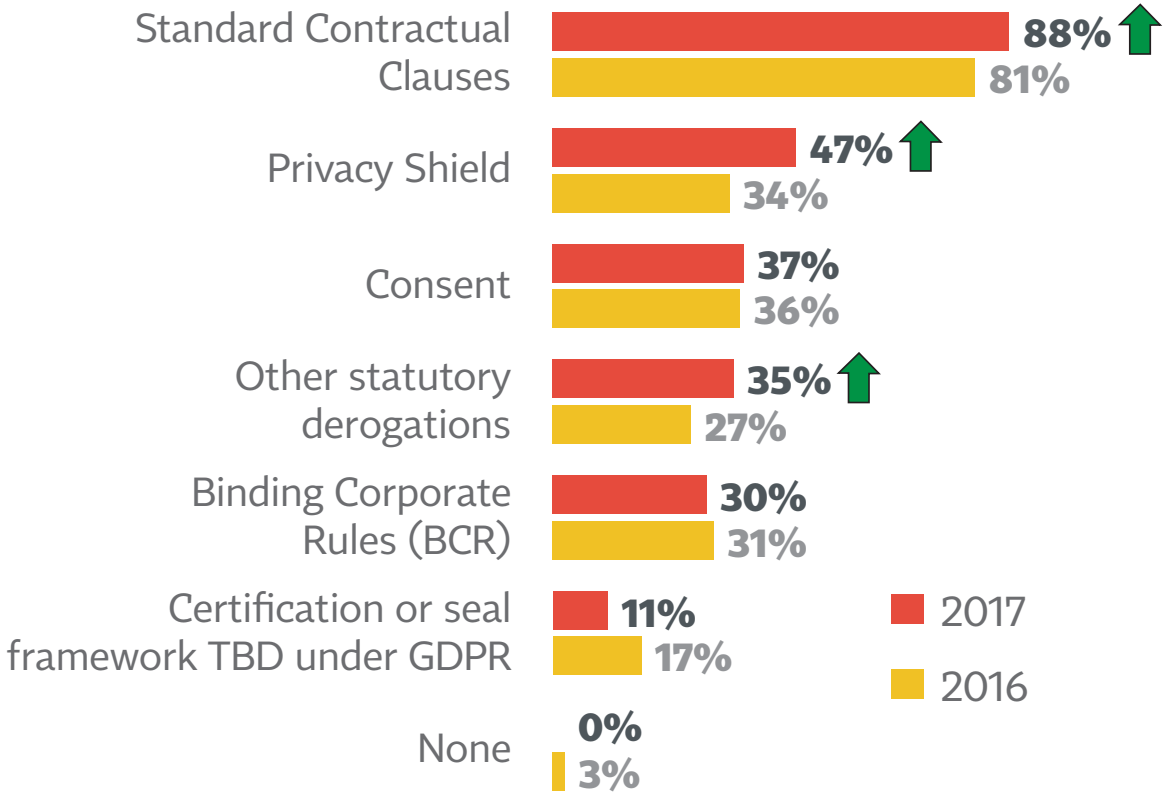


J9: Will your organization apply for Cross Border Privacy Rules (CBPR) to transfer data in the APEC region?
J10: When do you expect your CBPR application to be approved?

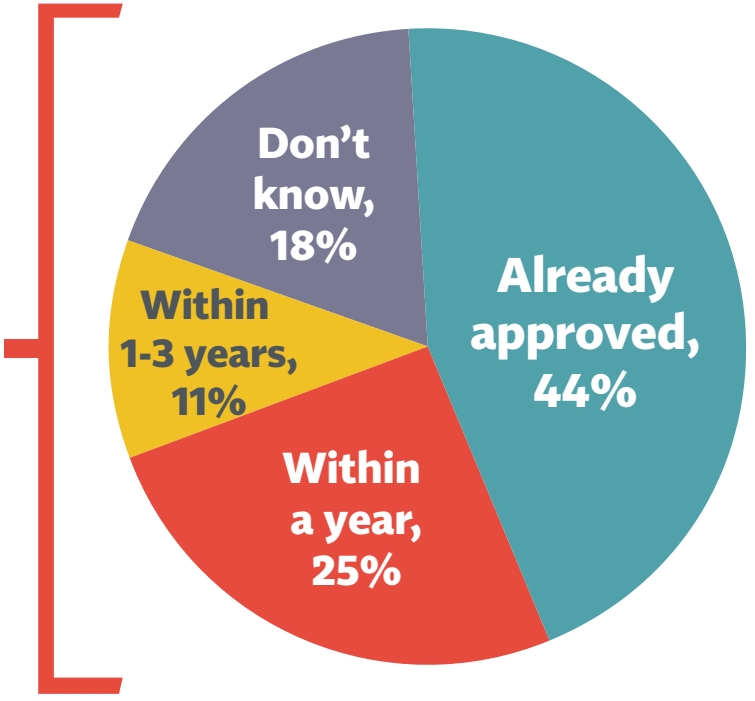
Standard contractual clauses are the most cited mechanism for data transfer

- This year shows increases in use of Privacy Shield and other derogations. It also shows a decrease (from 51%) in those saying BCR has already been approved

Data Transmission Mechanisms



Expected BCR Approval



↑ Significantly different from 2016

J5: What mechanism(s) does your company intend to use to transmit data to the US?
J6: When do you expect your BCR application to be approved?

EU firms are directionally more likely to intend to use BCR and Adequacy as mechanisms to transfer data

Mechanism for Data Transfer
Base: Transfer Data

Mechanisms	US w/o Gov't, Finance, Health	EU w/o Gov't, Finance, Health
Standard Contractual Clauses	90%	93%
Privacy Shield	49%	53%
Consent	41%	25%
Binding Corporate Rules (BCR)	23%	38%
Certification or seal framework TBD under GDPR	10%	10%
Adequacy	11%	34%
Other statutory derogations	34%	33%

J5: What mechanism(s) does your company intend to use to transmit data to the US?

BCR is a more commonly intended mechanism among the largest companies

Mechanism for Data Transfer
Base: Transfer Data

	Employee Size, US and EU, Without Gov't, Finance, Health			
	<5K	5–24.9K	25–74.9K	75K+
Standard Contractual Clauses	88%	95%	90%	89%
Privacy Shield	67%	44%	33%	55%
Consent	41%	35%	38%	27%
Other statutory derogations, such as fulfillment of contract	33%	31%	38%	35%
Binding Corporate Rules (BCR)	28%	26%	10%	45%
Adequacy	28%	23%	10%	14%
Certification or seal framework to be determined under GDPR	14%	5%	10%	12%

J5: What mechanism(s) does your company intend to use to transmit data to the US?

Contents

Do you run a cloud service? Better get GDPR ready

- Respondents place a high importance on GDPR compliance when selecting a cloud vendor

GDPR Compliance Importance in Choosing Cloud Service
(Mean Score on 0-10 Scale: 0=Not Important; 10=Critically Important)

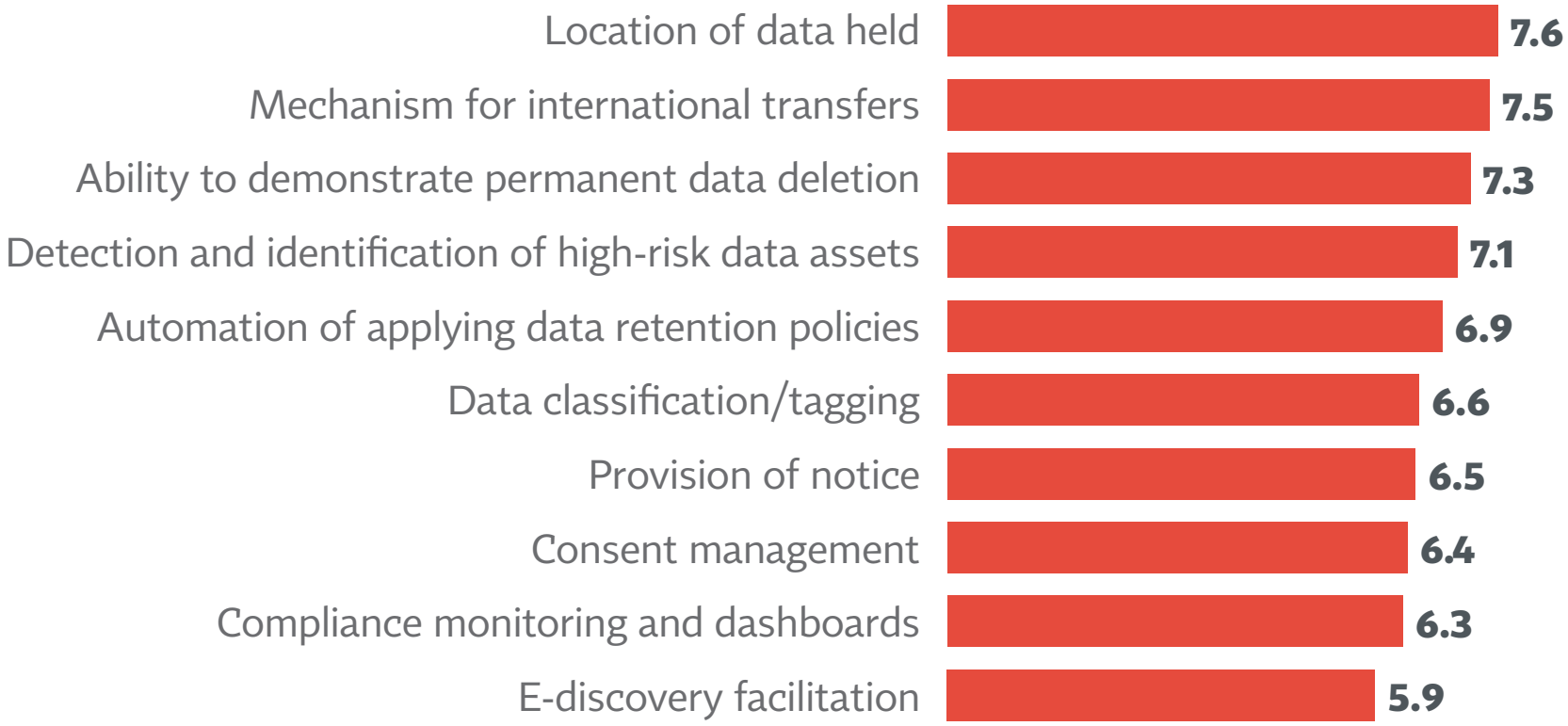
IMPORTANCE RATING
7.5

J18: How important is GDPR compliance when choosing cloud-based computing services?

Three factors are most important for cloud provider decisions…

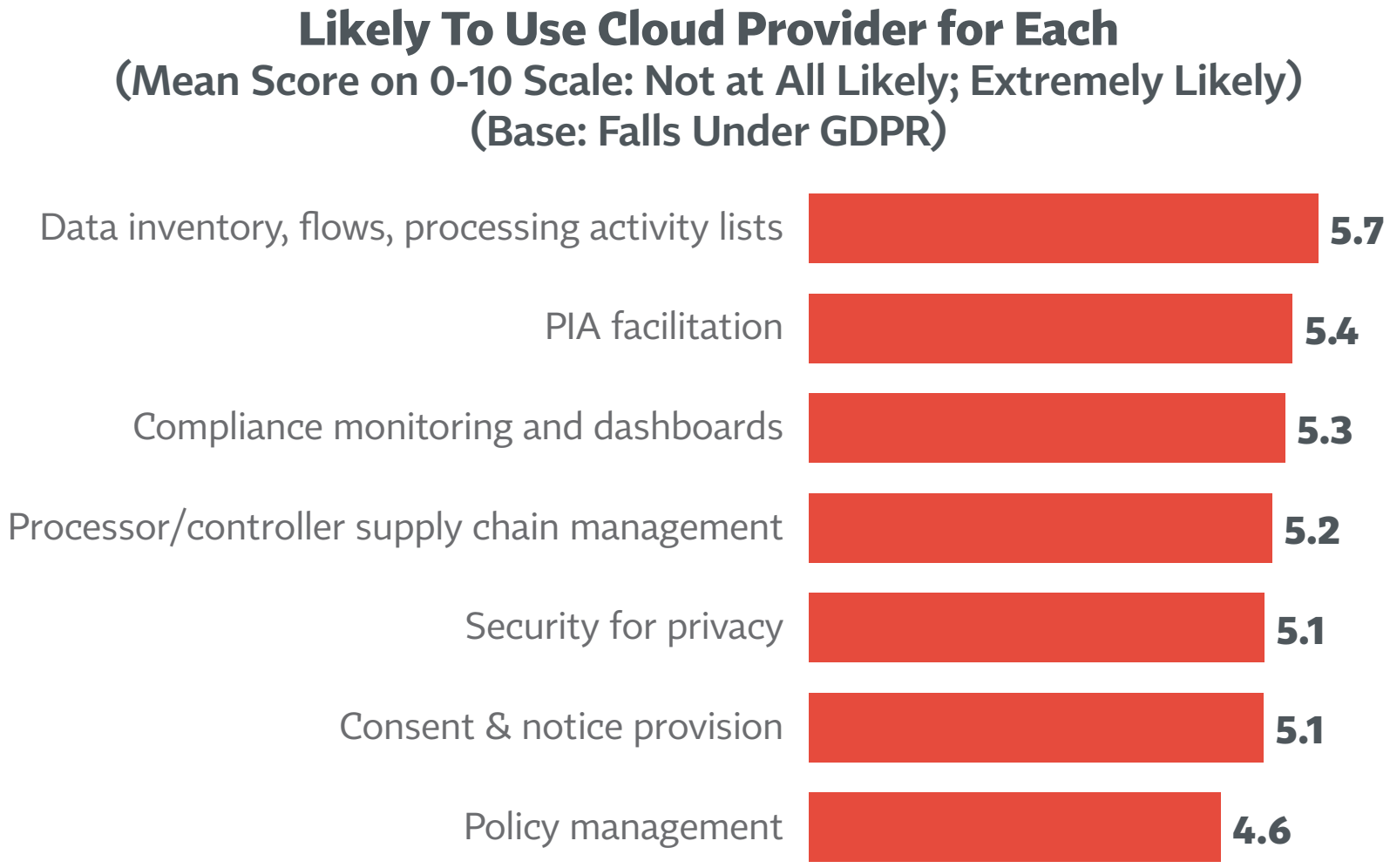
- Data location, transfer mechanism, and data deletion confirmation

Importance of Factors in Selecting Cloud Provider
(Mean Score on 0-10 Scale: 0=Not Important; 10=Critically Important)
(Base: Falls Under GDPR)



J19: Specifically, how important is each of the following factors in considering a cloud service provider?

Firms are lukewarm in their likelihood to use cloud providers for any of the GDPR applications tested



J20: How likely would you be to use a cloud-based service for each of the following? Use a scale of 0 to 10 where 0 means not at all likely and 10 means extremely likely.