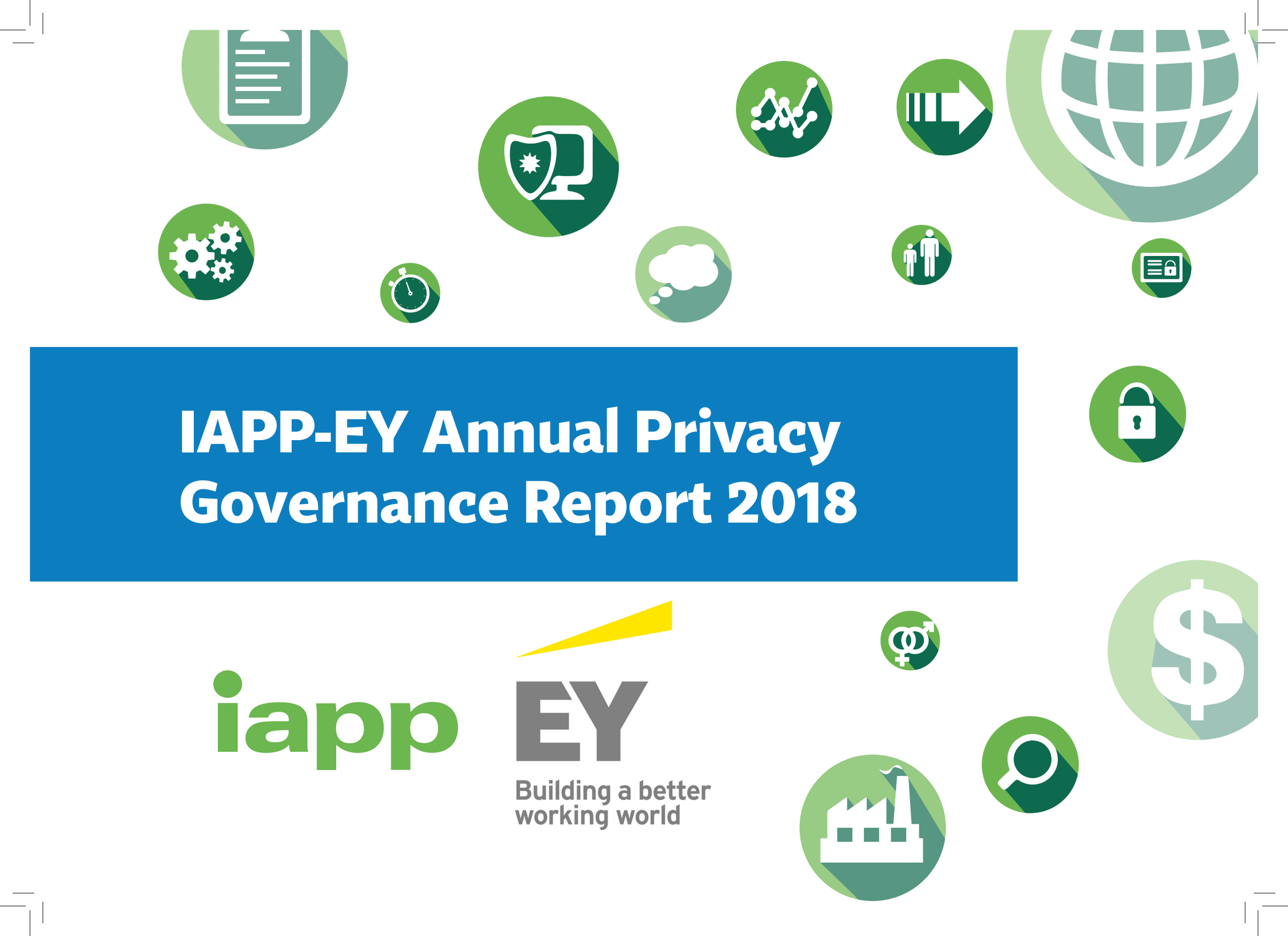
IAPP-EY Annual Privacy Governance Report 2018



iapp

EY

Building a better working world

Executive Summary

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

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

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

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

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

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

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

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

- 25 percent of respondents have changed vendors in response to GDPR and 30 percent say they are considering future vendor changes.
- The most popular cross-border data transfer mechanism — by far — is Standard Contractual Clauses.
- More than half the respondents subject to GDPR (56 percent) say they are far from compliance or will never comply.

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

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

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

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

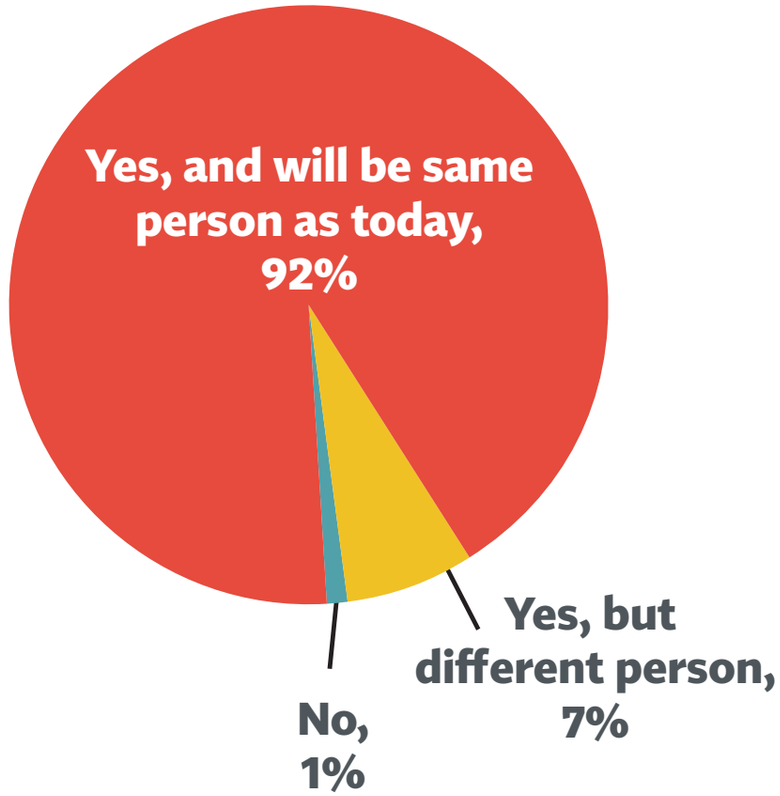
GDPR IN PRACTICE:

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

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

Main Reason for DPO

Will DPO Remain After GDPR?



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

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

Mean Privacy Staffing

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

Significantly higher than total

* Small sample size

NOTE: Outliers over 999 removed.

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

Mean Privacy Staff Size by Location

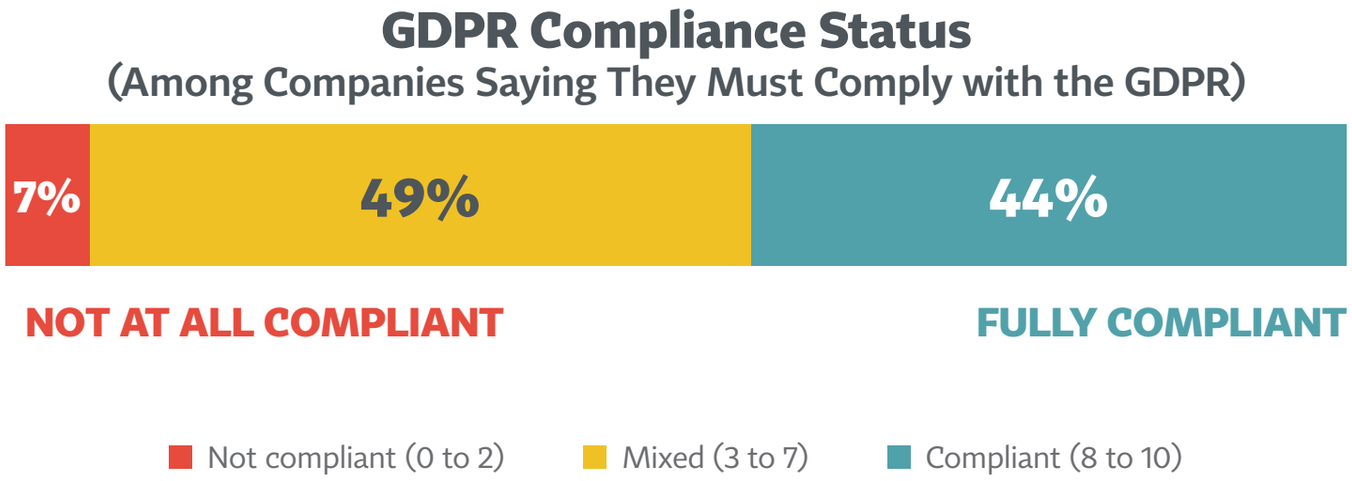
BY HQ LOCATION

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

NOTE: Outliers over 999 removed.

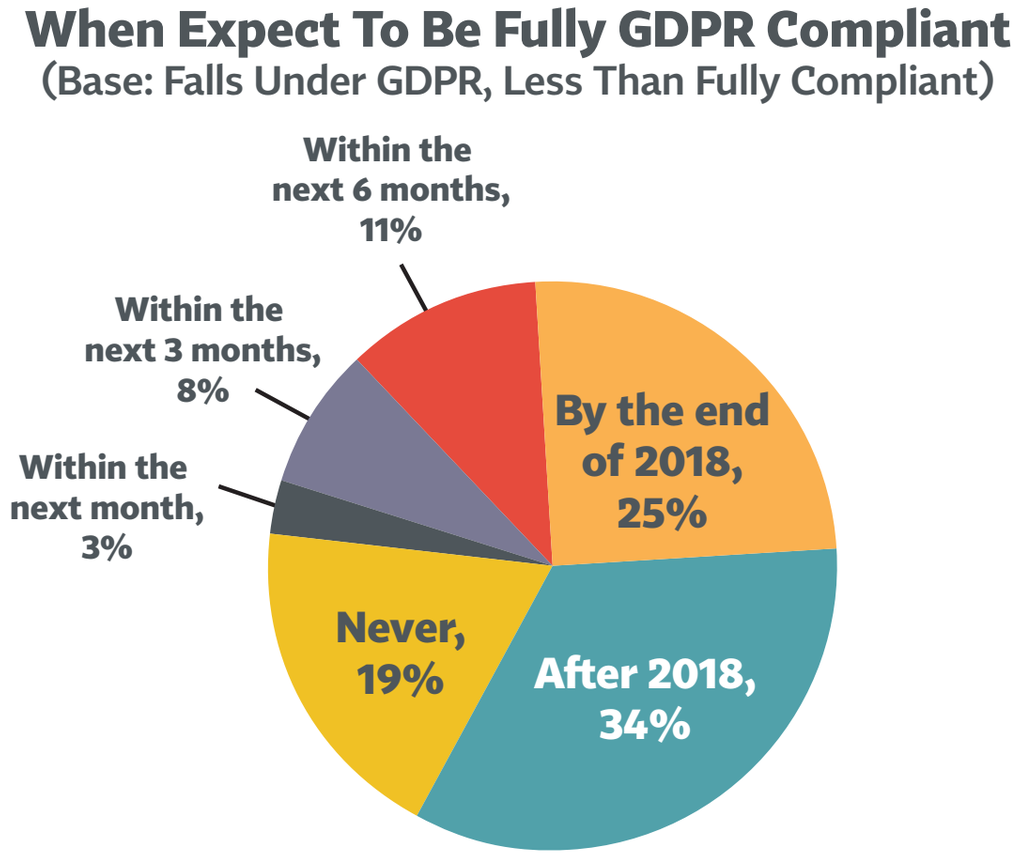
Just 44% of GDPR-affected firms consider themselves fully compliant or close to it

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



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

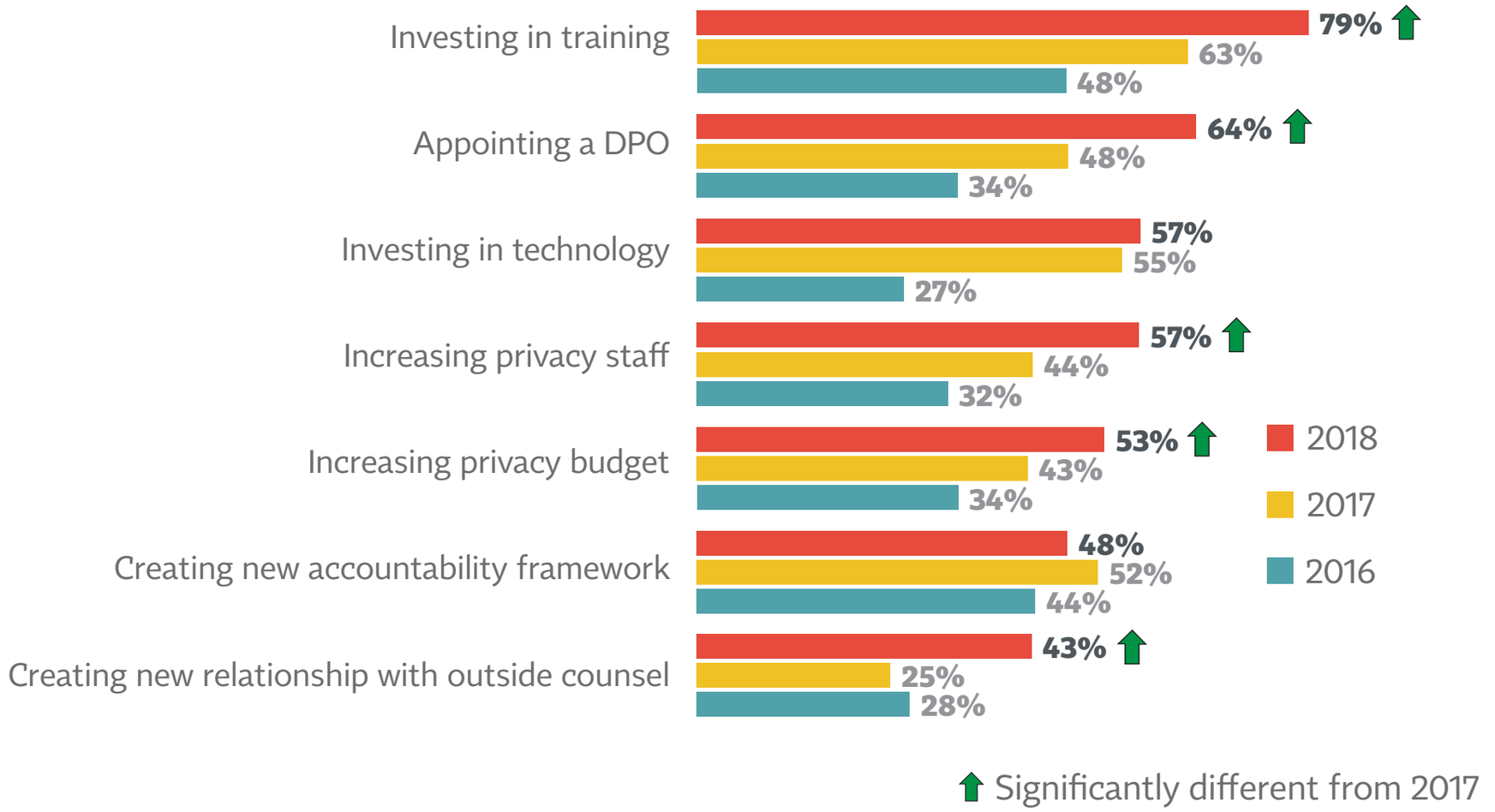
For those less than compliant, one-third say they won't reach compliance until after 2018; 19% say "never"



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

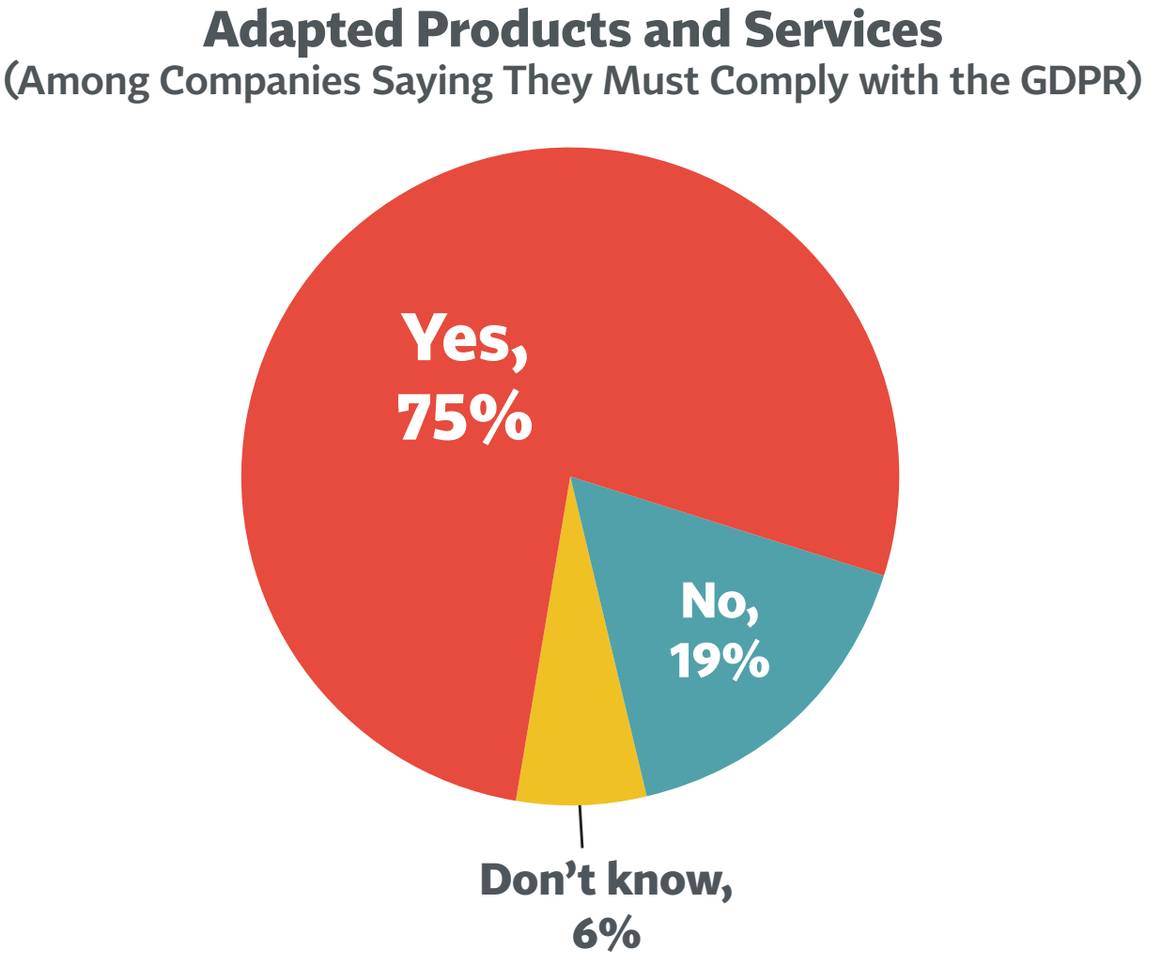
With 2018 being the GDPR compliance year, we see large increases in preparation steps across the board

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



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

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



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