# PRIVACY IN THE WAKE OF COVID-19

## *Remote Work, Employee Health Monitoring and Data Sharing*

EY
Building a better
working world

iapp REPORT

# CONTENTS

EY Building a better working world | iapp

# EXECUTIVE SUMMARY AND REPORT

EY Building a better working world

iapp

# Privacy in the Wake of COVID-19:

## Remote Work, Employee Health Monitoring and Data Sharing

By Müge Fazlıoğlu, Senior Westin Research Fellow

## Executive summary

On Jan. 30, the World Health Organization declared the coronavirus outbreak, which was first detected in Wuhan, China, to be a Public Health Emergency of International Concern, and, on March 11, it declared COVID-19, the disease caused by the coronavirus, to be a pandemic. While many unknowns remain, what can be said with certainty is that the 2019–20 pandemic has already changed social, economic and political realities around the world in profound ways, many of which will take years to fully comprehend.

In addition to the significant human and health costs it has brought about, COVID-19 has led indirectly to an utter transformation of everyday life for most people around the world. The "new normal" is a phrase that has been used during the current crisis to describe newly emerging routines, rituals and rules: sheltering in place; social distancing; a mass shift from a commuter workforce to a remote one; temperature checks at critical entryways and thoroughfares; the increased use of face masks in public spaces; and the replacement of in-person gatherings — from classes to conferences to concerts — by virtual ones.

Considering the rapid and massive changes underway, the IAPP and EY launched a research initiative to gain more insight into the unique ways privacy and data protection practices have been affected by the pandemic. The initial phase of the project included a survey of privacy professionals, taking a deeper look at how organizations, in general, and privacy programs, in particular, are handling the privacy and data protection issues that have emerged alongside COVID-19, such as privacy and security issues related to working from home, monitoring the health of employees, and sharing data with governments, researchers and public health authorities. It also looks at the unique economic impact of the crisis on the privacy profession. A total of 933 respondents completed the survey, and responses were collected between April 8 and 20.

## Key findings

Some of the key findings from this study include:

- Issues related to **employee remote work, employee health monitoring and COVID-19 data sharing** are the top challenges privacy professionals are facing during the coronavirus pandemic.
- Nearly half of organizations (45%) **have adopted a new technology or contracted with a new vendor** to enable remote work due to COVID-19.
- Most employers have **collected data from their employees about personal travel and symptoms,** and 60% is **keeping records of employees diagnosed with COVID-19.**
- About 19% of organizations **have shared the names of employees diagnosed with COVID-19** with other employees or the government.
- Globally, 72% of privacy professionals **expect no or only a small reduction in privacy staff,** while most 81% **expects no or only a small reduction in privacy budgets.**

## Privacy unfazed

While the pandemic is an unprecedented event for most of the current generation, upheaval is not entirely unfamiliar to privacy professionals. The broad extraterritorial scope of the EU General Data Protection Regulation and the swiftness with which the California Consumer Privacy Act entered the scene are just a couple of recent examples of new developments that have taught privacy pros to be adaptable to change.

In the face of a pandemic, privacy professionals have forged ahead in fulfilling their existing legal, regulatory and compliance duties. Indeed, data protection authorities have made clear that fundamental rights and freedoms must continue to be protected during the pandemic and that existing data protection rules, such as the GDPR, continue to be in force. In addition, despite an effort by a coalition of advertising groups to convince the California Attorney General's Office to delay the CCPA's enforcement date of July 1, the enforcement of the law is moving forward as planned.

Along these lines, the results of the survey indicate that privacy has not been sidelined due to COVID-19. For example, most respondents (~60%) said that privacy has "not at all" become less of a priority due to the pandemic, while nearly 30% said it has been de-prioritized only "to a small extent." Yet, privacy has been more sidelined in the industries that have been hardest hit by the COVID-19 pandemic: those working in the hospitality sector (e.g., hotels, restaurants, leisure) were more likely to say the priority of privacy within their organization has been lowered by COVID-19, while those working in software and services were less likely to say so, compared to others.

Yet, while the privacy profession has not wavered in importance, it has undergone significant transformation in response to the crisis. For example, one of the most immediate and impactful effects on global businesses of COVID-19 has been the "stay-at-home" orders and ban on large gatherings issued by various governments and the ensuing shift of the workforce to a remote model. This has undoubtedly affected the types of issues privacy pros have been dealing with and introduced several new privacy and data protection challenges.

## Working from home: new tech in the "new normal"

At the time the survey was conducted in early to mid-April, more than 90% of the organizations surveyed had put in place a policy requiring most, if not all, their employees to work from home. Indeed, only 1% of respondents reported that all or almost all their workforce continues to commute to a physical workplace.

This rapid shift to a WFH model has been one of the biggest business continuity challenges for organizations to deal with. Nearly half (45%) of respondents said that their organization has needed to adopt new technology or contract with new vendors to enable remote work. In some sectors, that number is even higher. For example, about two-thirds of respondents in legal services and academia/education reported adopting new technology to enable WFH. It may be no surprise that schools and universities had the most ramping up to do in the shift to WFH, as the traditional classroom teaching model has been in place for centuries. Meanwhile, a high number of health care organizations and government agencies (60%) have also needed to adopt new WFH tech due to stay-at-home orders.

At the same time, some industries seem to have been better positioned than others to have made this shift to WFH. In particular, the survey results showed that the lowest adoption rates of new WFH technology were in the software and services, technology hardware and equipment, marketing, and materials sectors. It seems likely that, at least for software and services and marketing, companies in these sectors already a WFH model partially in place and thus did not need to adopt any new tools but rather just expand their existing ones.

## Expediting privacy

Some organizations have had to make sacrifices in the scramble to roll out these new tools with efficiency. Indeed, among those who have adopted new WFH technology, around 60% has either skipped or expedited a privacy or security review.

### *Rapid tech rollout*

*Of those that have adopted new tech to enable WFH, 60% has accelerated or bypassed the privacy/security review.*

The large number of organizations that have felt compelled to skip or expedite a privacy or security review for new technologies or vendor agreements indicates the need for guidance on how to conduct an expedited privacy/security review, such as this IAPP checklist.

## Privacy pivots: the risks/threats of working from home

On top of their existing obligations, COVID-19 has also demanded that privacy professionals add an array of new concerns to their plates. When asked about how their priorities have changed in the wake of COVID-19, about half (48%) of privacy professionals said that safeguarding against attacks/threats has become more of a priority for them. Indeed, a recent survey by ISACA found that many companies are seeing an increase in the number of cyberattacks since the pandemic began. In this vein, the U.S. Federal Trade Commission also recently reported that it has received nearly 30,000 fraud complaints related to COVID-19 since January, amounting to some $20 million lost by consumers to these scams.

Given the security vulnerabilities that have been introduced by the diffusion of workforces from centralized corporate networks to multiple home networks with varying degrees of security, the increasing importance of cybersecurity among privacy professionals should come as little surprise.

## Rise in WFH tech

*Two-thirds of organizations in legal services and education/academia and 60% in health care and government have adopted new technology to enable WFH since COVID-19 began.*

Indeed, when asked to identify the top privacy challenges stemming from COVID-19, understanding privacy requirements associated with employee remote work was the top pick, chosen by about half (49%) of respondents. Meanwhile, 38% of respondents said that understanding privacy requirements associated with employee health monitoring and requirements associated with requests to share COVID-19 data were their top privacy challenges. Given that the survey was conducted in early to mid-April, these numbers may be even higher today. Priorities may also have changed since the survey was conducted in April, especially as more and more countries and states have unveiled or begun to executive plans to reopen their economies.

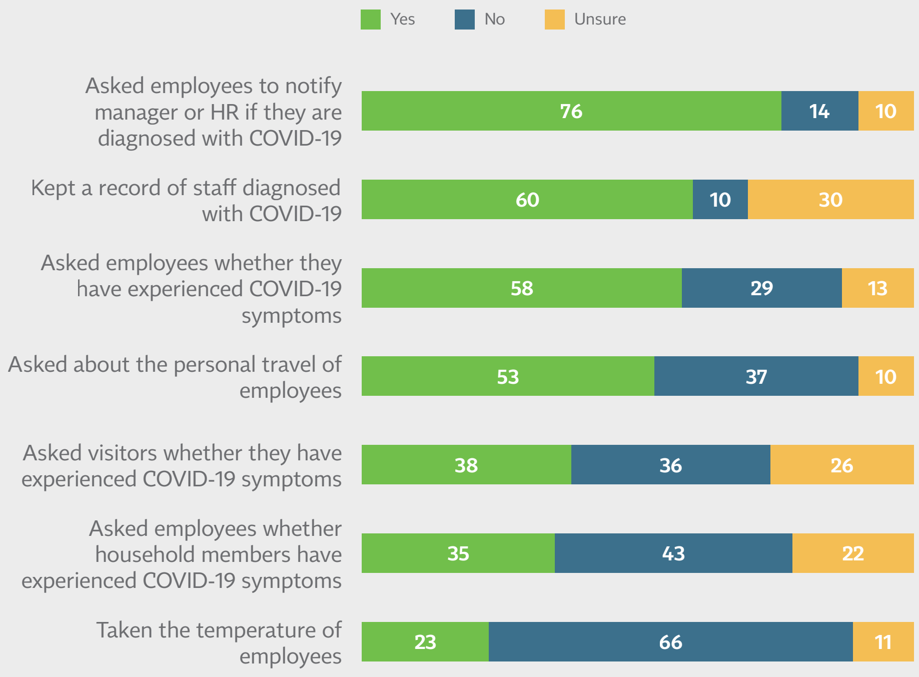
# The rising risks of processing employee health data

A new and important issue has arisen that will undoubtedly require privacy professionals to work closer with HR within their organizations: the monitoring of employee health. While employee monitoring has long been on the radar of privacy pros, COVID-19 has thrown a new ratchet into the mix, as employers seek to identify and quarantine workers who become ill and contagious.

To better understand the types of data organizations are collecting about employee health in their efforts to make workplaces safe, respondents were also asked about what specific types of data their employer is collecting about its employees. The results indicate that most employers are processing the health information of employees, such as asking employees about whether they have experienced any COVID-19 symptoms (58%), have done any personal traveling recently (53%), and whether any members of their household have experienced COVID-19 symptoms (35%). Almost a quarter (23%) have also taken their employees temperatures.

In addition, more than three-quarters of respondents said their employer has required employees to inform their manager or HR if they are diagnosed with COVID-19, and 60% is keeping records of which employees have been diagnosed with COVID-19.

## Types of health data employers are collecting in response to COVID-19



## Public-private partnerships: COVID-19 data sharing

Given the urgency and importance of combatting the pandemic, many companies have been receiving requests to share data around COVID-19. In line with certain basic data protection principles, such as necessity, minimization and proportionality, more aggregated/anonymous data is being shared than identifiable data. In fact, nearly twice as many organizations (30%) have been asked to share aggregated/anonymous data as have been asked to share identifiable data (16%).

*Overall, about 19% of organizations have shared the names of staff diagnosed with COVID-19 with a third party.*

It is worth noting that in their guidance released around COVID-19, several DPAs, as well as the European Data Protection Board, have urged entities to share data in aggregated form, and several have advised against revealing the names of employees who have tested positive for COVID-19 to third parties unless there is a specific justification for doing so.

Yet, some organizations are sharing the names of staff who have been diagnosed with COVID-19 with other employees or with government authorities. In total, around 19% has done so. Since respondents were not asked the reason for such sharing, it is difficult to know if such data was shared to protect the health and safety of other individuals or for a different purpose.

In addition, due to their nature, businesses in some sectors have done more sharing than others. Around 40% of organizations in the aerospace and defense sector have shared the names of staff who have tested positive for COVID-19, while 26% of organizations in the health care sector have done the same. There were also differences between organizations of different sizes: While only 6% of smaller organizations (1 to 250 employees) have shared the names of staff who have COVID-19, more than a quarter (26%) of large organizations (5,001 to 25,000 employees) have.

## Privacy programs brace for economic downturn

Alongside significant losses to human life and health consequences, the pandemic has generated untold economic turmoil for many. The stoppage of business activity that characterizes the "Great Lockdown" or "Great Shutdown" has already been described by the IMF as the worst economic downturn since the Great Depression, "much worse" than the financial crisis of 2008–09. Inevitably, some of the economic fallout from the pandemic will affect the organizations for which privacy professionals work. Yet, as fewer than 1% of those surveyed said that their privacy programs would be discontinued, the overwhelming majority feel that their privacy programs are positioned to survive in the long-term. Some sectors will likely get through the crisis unscathed or become even stronger than they were before, while others may see some degree of drawdown in their privacy programs.

## Privacy staffing mostly unaffected, though hardest-hit sectors already seeing cuts

***COVID-19 impact***

*Privacy pros in the U.K., compared to elsewhere, expect to see more cuts to their program staff.*

*Privacy pros in the EU and Canada expect to see the smallest privacy budget cuts.*

Regarding future expectations about the size of their privacy teams, 62% of privacy professionals expect to see no reduction in staffing. While 21% remains unsure, the rest are expecting a privacy staff reduction ranging from small (10%) to fair or large (7%). Yet, while most privacy teams will likely emerge from the crisis unscathed, some already are feeling the squeeze. Indeed, while less than 1% of the overall sample expects their privacy program to be eliminated, that number is 7% in the hospitality sector and 5% in the business services sector. In addition, respondents in the U.K. were more likely than those anywhere else to expect a fair to large reduction in privacy staff (16% said so).

It is also worth recalling here, however, that the survey was conducted in early to mid-April, when the picture of job losses was less clear than it is today, as the full gravity of the economic crisis continues to unfold. As of May 11, for example, more than 33 million Americans had filed for unemployment benefits over the past seven weeks.

## Canadian, EU privacy pros expect fewer budget cuts

Regarding expectations about changes in privacy budgets going forward, the results paint a similar picture. About half (48%) said the budget for their privacy program will not be reduced at all, with the other half expecting various degrees of cuts, depending on the industry. While 18% overall said they expect their privacy budget to be reduced by a fair or great extent, 34% of privacy pros working in the transportation sector and 32% of those in the business services sector expect to see a fair to large budget reduction.

Some geographic differences also emerged regarding budget expectations, with respondents in the EU and Canada less likely to expect large budget cuts than respondents elsewhere.

## Conclusion

This report focuses on privacy and data protection issues related to COVID-19 to provide insight into the impact the pandemic is having on the privacy profession. The implications of the present crisis for the privacy profession cannot be overstated, as so many things have changed — from how employees work to how employers monitor them to how private companies and governments share data around the world.

While there is no letting up with the compliance work around existing global privacy laws, responding to data subject requests and conducting privacy and security reviews and data protection impact assessments, these new challenges and priorities around teleworking and teleconferencing, processing employee health data, and sharing data with third parties have taken on novel importance.

Privacy is here to stay, but it will likely reemerge on the other side of the crisis in a different form, a “new privacy,” permanently transformed by it as so many other aspects of life have been.

## Sample demographics

About 75% of respondents worked in the private sector, 13% worked in government and another 12% worked for a nonprofit or education institution. Respondents were spread relatively evenly throughout small and large organizations — approximately half worked for organizations with 5,000 or more employees, and the other half for organizations with fewer than 5,000 employees, with 30% working for organizations with fewer than 1,000 employees.

Regarding geographic distribution, the sample was diverse and broadly reflected the distribution of the IAPP membership. Respondents represented organizations based in more than 80 countries, with about half of respondents being located outside the U.S. About 10% was based in Canada, 8% in the U.K., 6% in the Netherlands and 3% in Germany. More than 9% of the sample came from outside the U.S. and Europe.

Respondents also came from a variety of job sectors, more than 30 in total. The largest group came from the software and services industry (15%), followed by the health care industry (11%) and government (8%). Banking (6%), education and academia (6%), and insurance (6%) were the next most prominent industries within the sample, reflecting the broad swath of the economy in which privacy professionals work.

Respondents were also asked whether their place of employment met the definition of an "essential business" in the context of COVID-19 according to federal, state or local government guidelines. Given that the term "essential business" may be defined differently from country to country (or even from state to state), respondents were asked to self-identify their organization. More than half (53%) said their organization was an essential business, 37% said it was not and 10% was unsure. Thus, the sample represented a broad range of businesses and industries that have been affected by the crisis to varying degrees.

## Research objectives

- To understand how organizations are responding to the **COVID-19 outbreak** and **declaration of a public health emergency** around the world.
- To take a deeper look at how practices around **data collection and sharing** have been affected by COVID-19.
- To examine the impact of the pandemic on the **staffing and budgets of privacy programs**.

## Methodology

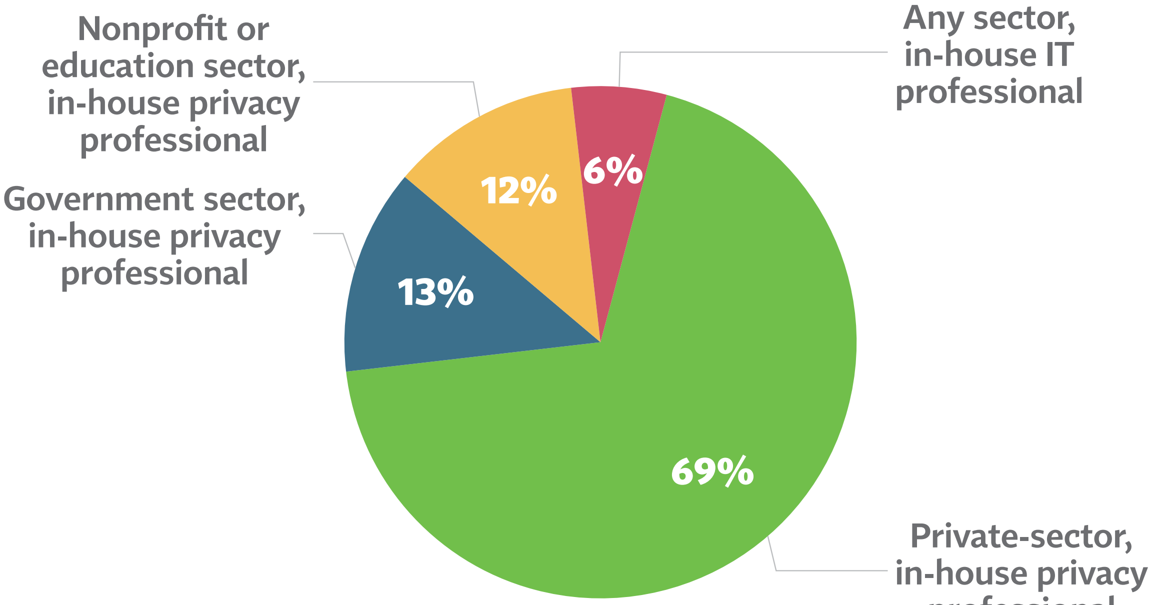
- The target population for the survey was **in-house privacy** and **IT professionals**.
- Subscribers to the **IAPP's Daily Dashboard** were sent a survey invitation and reminder by email in early **April**.
- A **call to action** was published on the IAPP's website and shared on social media.
- Responses to the survey were collected between **April 8 and 20, 2020**.
- A total of **933** respondents completed the survey.

# DEMOGRAPHICS

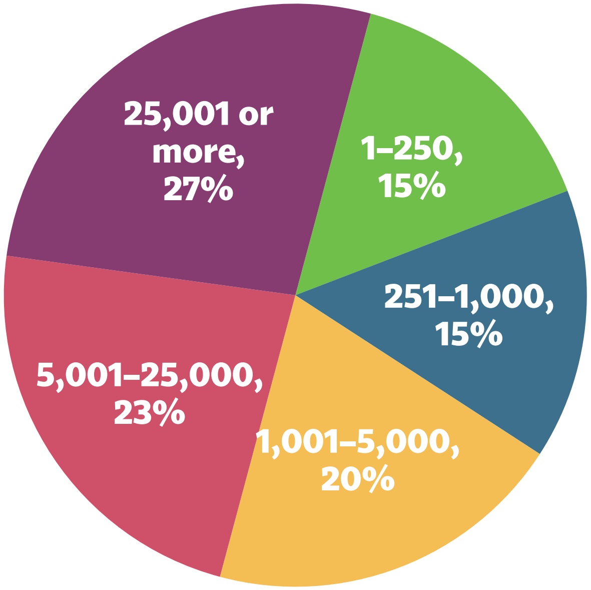
EY Building a better working world | iapp

# Most respondents work in the **private sector** at **large companies**.

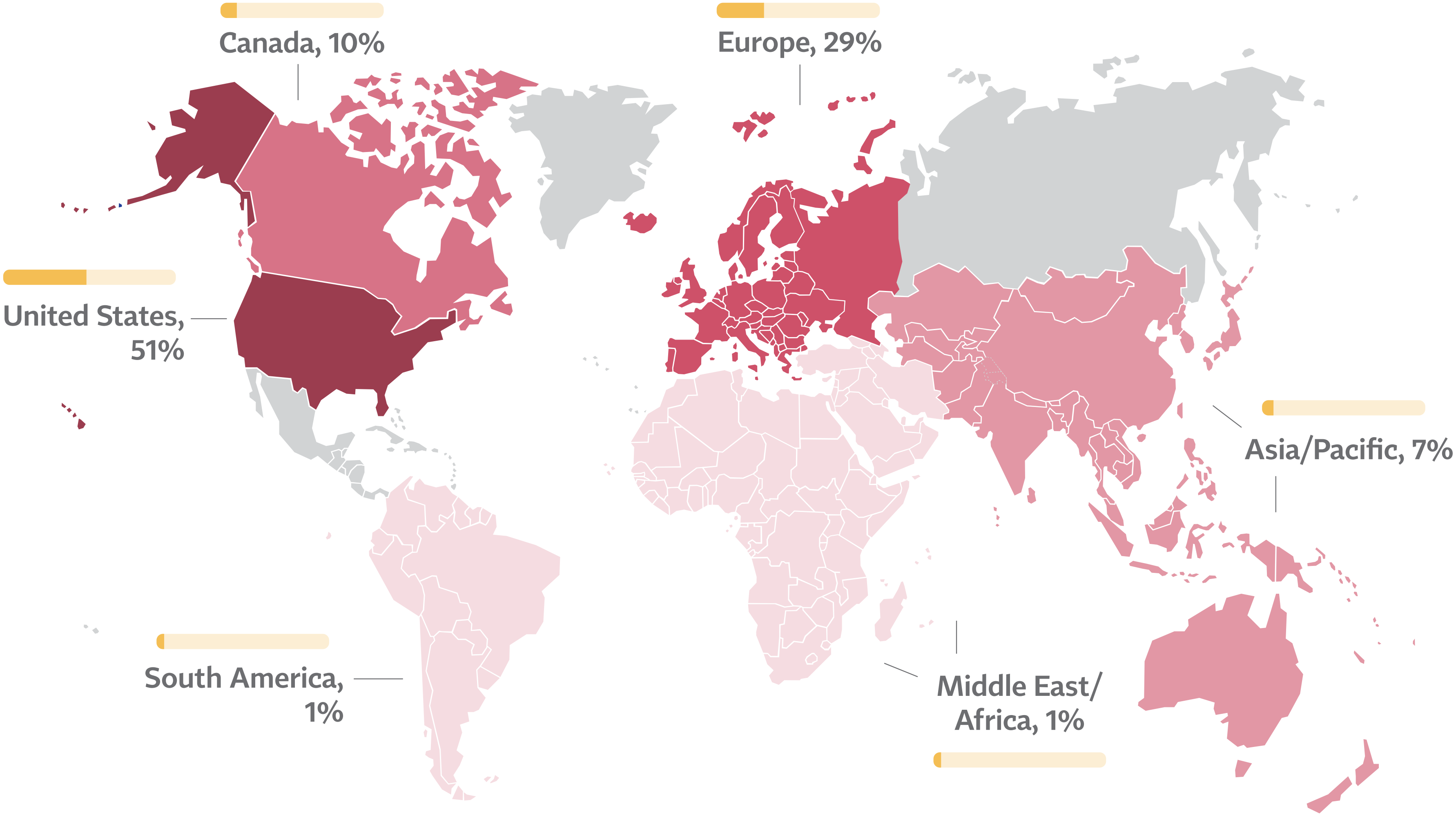
## Role



## Company size

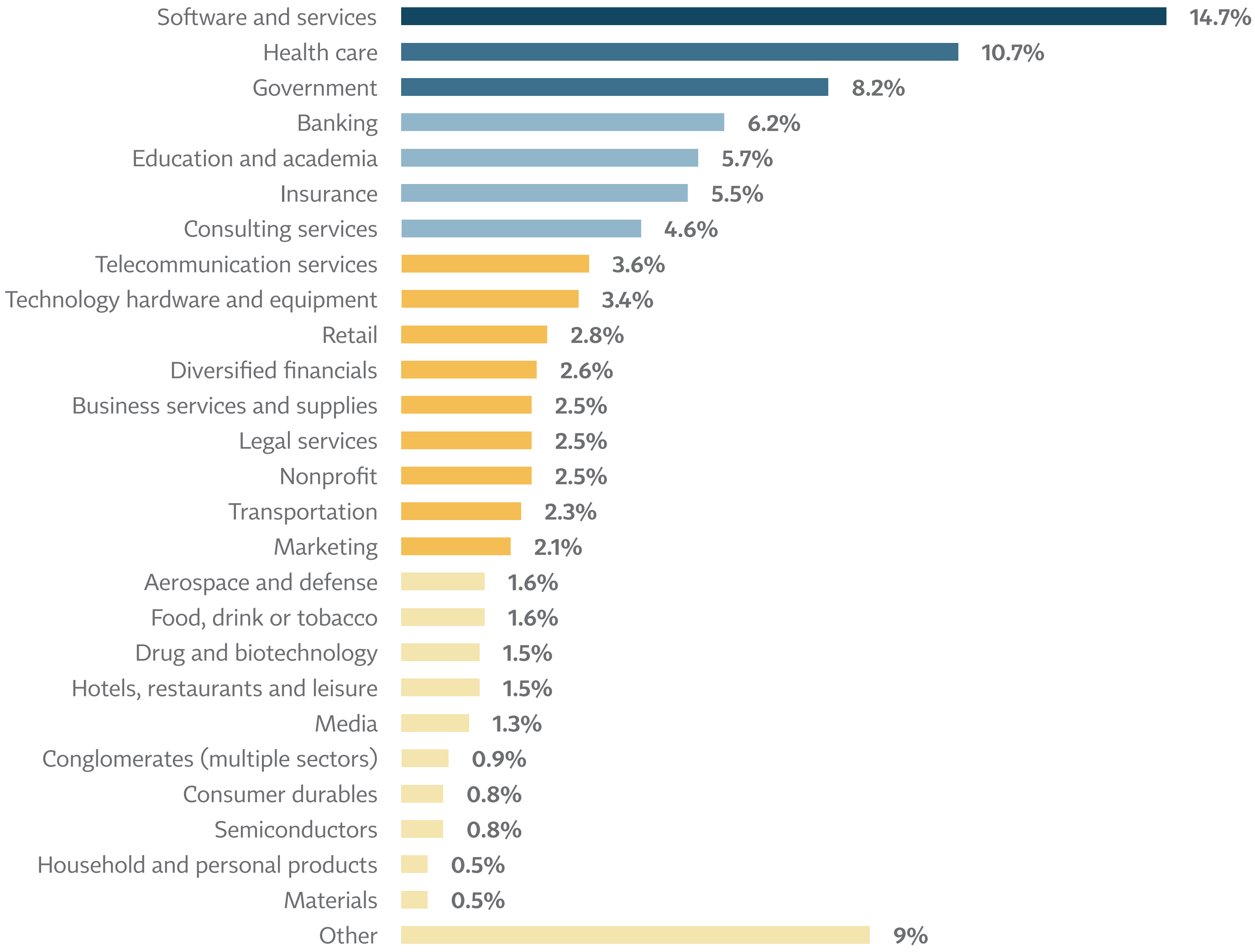


# The **geographic distribution** of respondents spanned the globe.



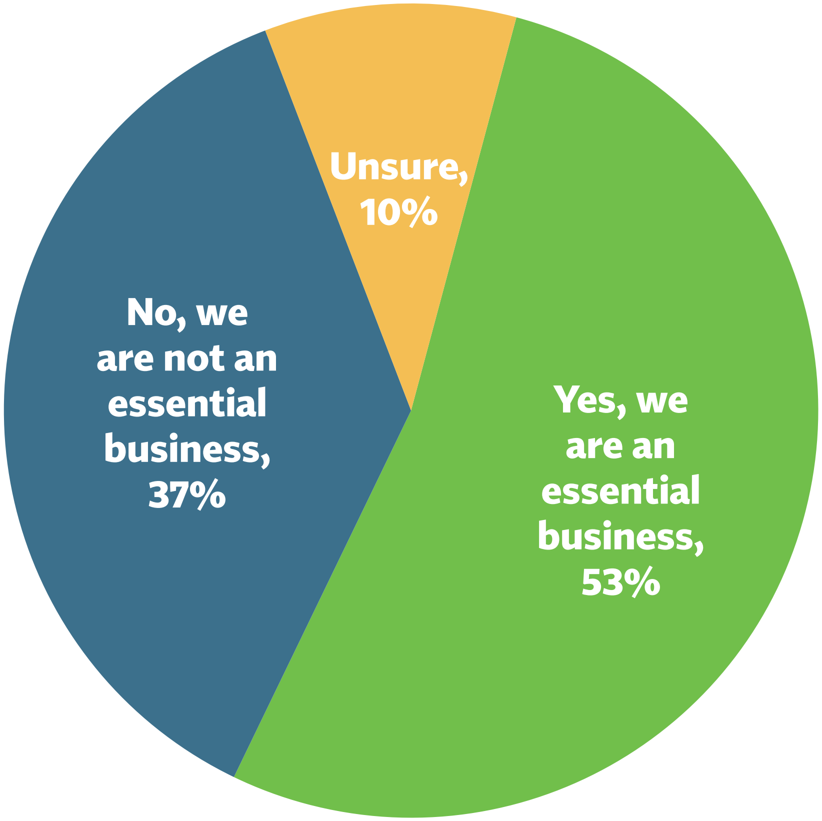
*Question: What is the primary location of your organization's headquarters?*

# **Software and services, health care and government** were the most prevalent **job sectors**.



# **More than half** of respondents work for an organization that has been designated an **“essential business.”***

## “Essential business” designation



*Question: Has your organization been designated an “essential business” according to federal, state or local government guidelines?*

* *The phrase “essential business” was not defined in the survey, recognizing that the types of businesses allowed to remain open during the COVID-19 pandemic have varied greatly across and within countries. Rather, the survey asked respondents to answer based on federal, state or local government guidelines.*

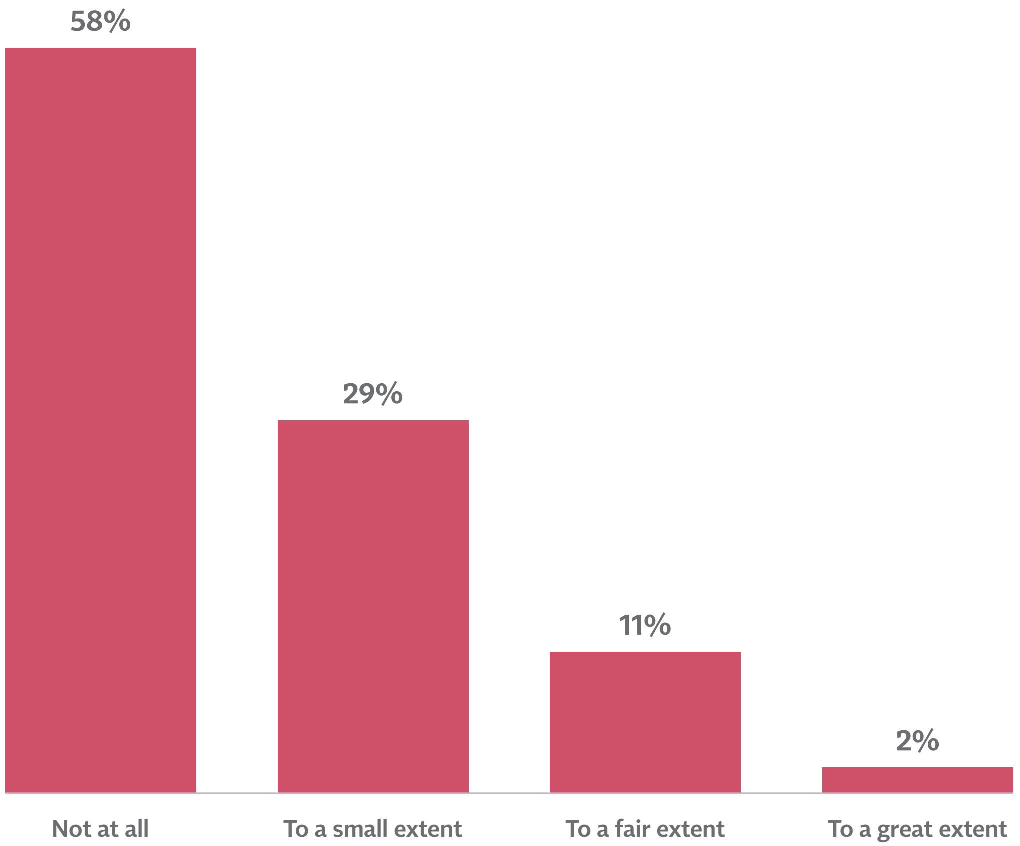
# PRIVACY PRIORITIES AND CHALLENGES

EY Building a better working world | iapp

# Most think that COVID-19 has ***not*** sidelined **privacy priorities**.

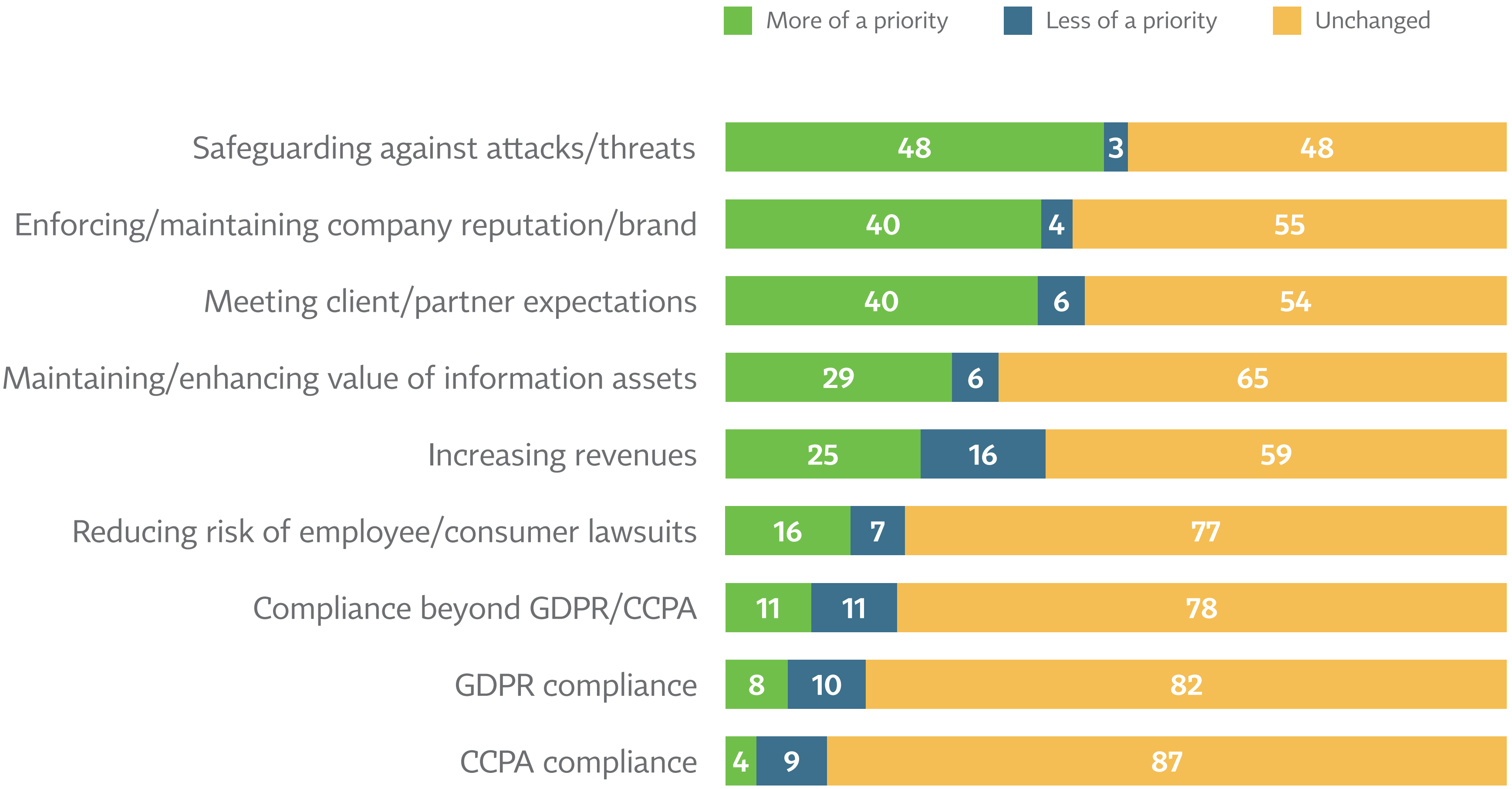
## Has COVID-19 lowered the priority of privacy?

*58% of all respondents say "not at all."*

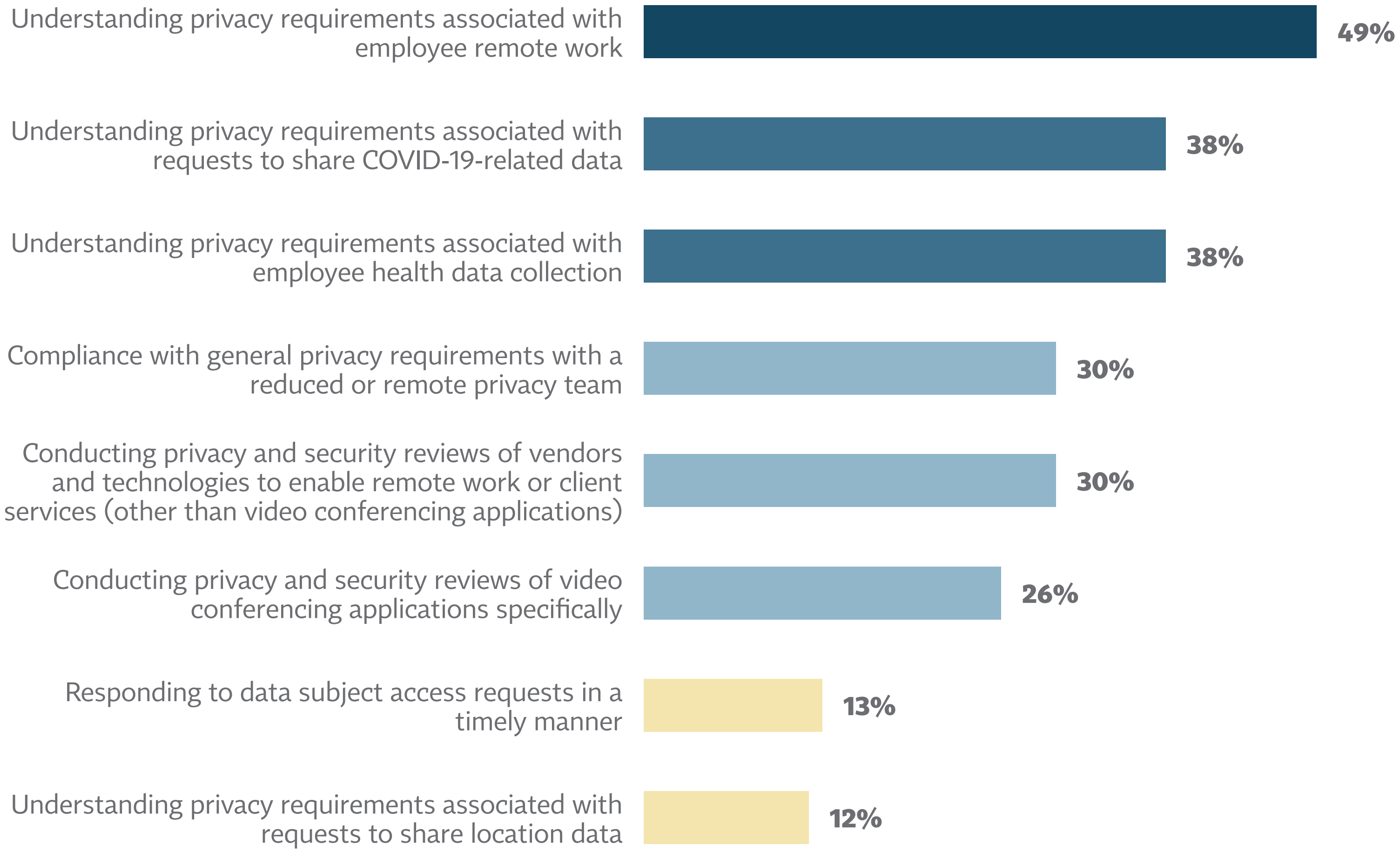


*Question: To what extent, if any, would you say that the COVID-19 pandemic has lowered the priority of privacy within your organization?*

# **Cybersecurity, brand reputation** and **business expectations** have become increasingly important for privacy pros.



# **The work-from-home environment, employee health monitoring** and **COVID-19 data sharing** are the biggest privacy challenges.

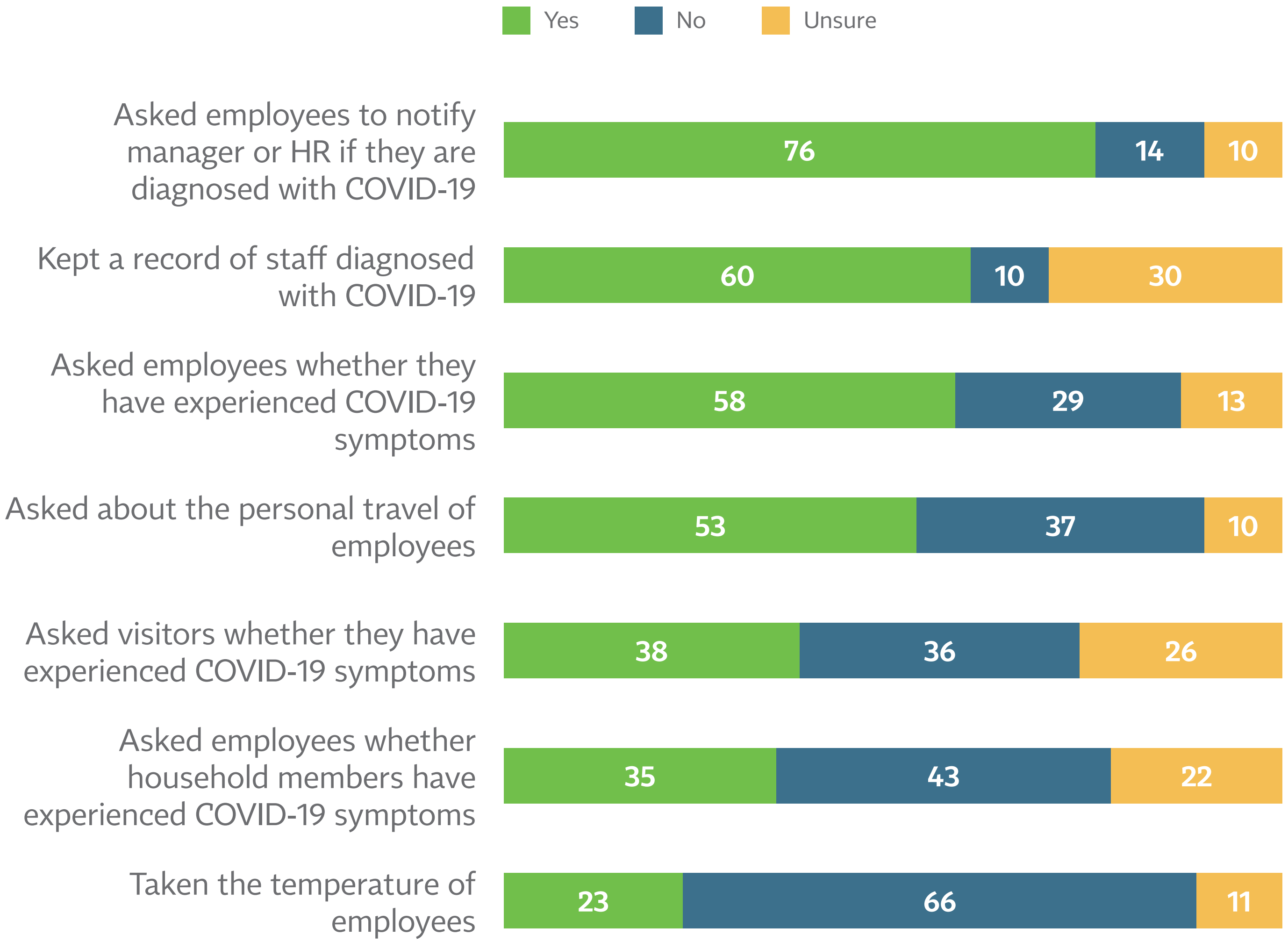


*Question: What are your organization's top privacy-related challenges as a result of COVID-19? (Select up to three)*

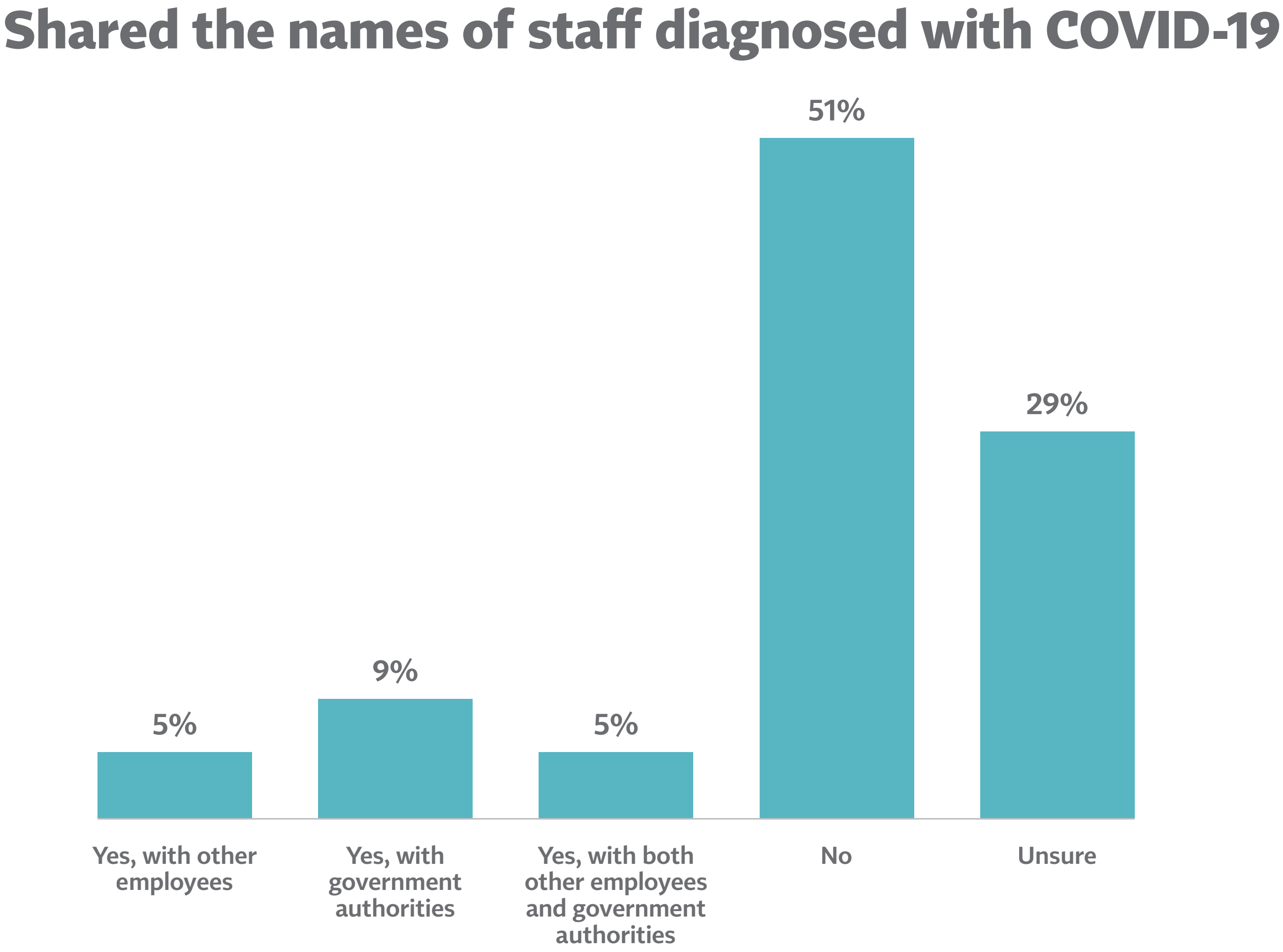
# EMPLOYEE HEALTH MONITORING

EY Building a better working world | iapp

# Most organizations have collected data from employees about **COVID-19 symptoms** and **kept diagnostic records**.



# About **1 in 5 organizations** have shared the names of staff diagnosed with COVID-19.



*Question: Has your organization shared the names of any staff who are diagnosed with COVID-19 with other employees or government authorities?*

# Compared to other sectors, more in **aerospace/defense** and **health** have shared the names of staff with COVID-19.

## Shared the names of staff diagnosed with COVID-19

| | Yes | No | Unsure |
|---|---|---|---|
| Aerospace and defense | **40%** | 53% | **7%** |
| Health care | **26%** | **44%** | 29% |
| Government | 25% | 40% | 35% |
| Education/academia | 19% | 47% | 34% |
| Banking | 16% | 60% | 25% |
| Insurance | 16% | 56% | 28% |
| Software and services | 16% | 56% | 28% |
| Consulting | **7%** | 49% | **44%** |
| **OVERALL** | **19%** | **51%** | **29%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization shared the names of any staff who are diagnosed with COVID-19 with other employees or government authorities?*

# **More firms in Asia** have shared the names of staff diagnosed with COVID-19, while **fewer U.S. firms** have.

## Shared the names of staff diagnosed with COVID-19

| | Yes | No | Unsure |
|---|---|---|---|
| Asia | **38%** | **43%** | **20%** |
| Australia/New Zealand | 31% | 35% | 35% |
| Canada | 23% | 42% | 35% |
| European Union | 23% | 60% | 17% |
| United States | **16%** | 49% | **35%** |
| United Kingdom | 14% | 63% | 22% |
| **OVERALL** | **19%** | **51%** | **29%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization shared the names of any staff who are diagnosed with COVID-19 with other employees or government authorities?*

# **Large organizations** have shared the names of staff diagnosed with COVID-19 **more than small ones** have.

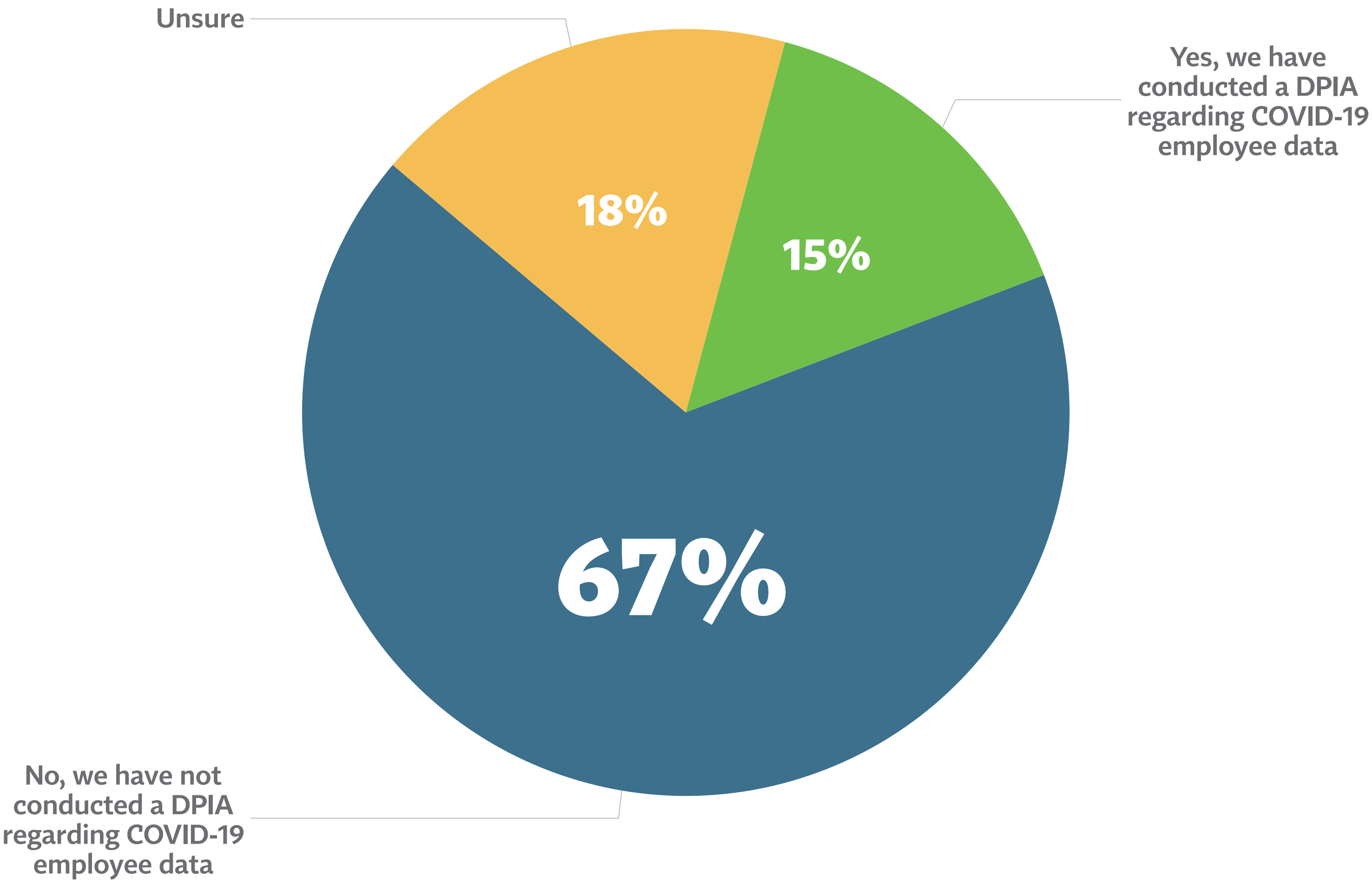
## Shared the names of staff diagnosed with COVID-19

| Size | Yes | No | Unsure |
|---:|:---:|:---:|:---:|
| 1–250 | **6%** | **74%** | **21%** |
| 251–1,000 | 19% | 54% | 27% |
| 1,001–5,000 | 20% | 52% | 28% |
| 5,001–25,000 | **26%** | **45%** | 30% |
| 25,001 or more | 20% | 43% | 36% |
| **OVERALL** | **19%** | **51%** | **29%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization shared the names of any staff who are diagnosed with COVID-19 with other employees or government authorities?*

# **15% of organizations** have conducted a **data protection impact assessment** focused on COVID-19 data collected from employees.



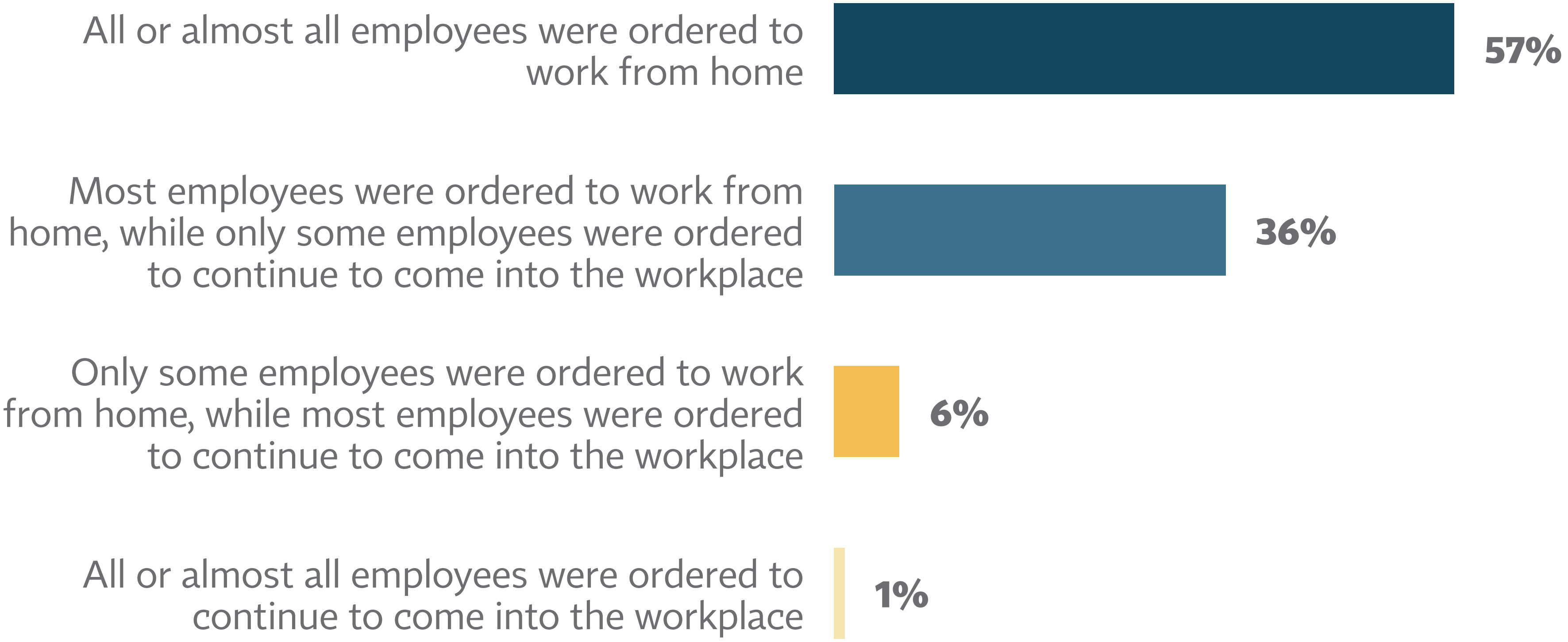
*Question: Has your organization conducted a data protection impact assessment specifically with regards to the data collected from employees in the context of COVID-19?*

# WORKING FROM HOME:
## NEW TECH IN THE “NEW NORMAL”

EY Building a better working world | iapp

# More than **90% of organizations** have put in place a policy requiring most or all employees to work from home.

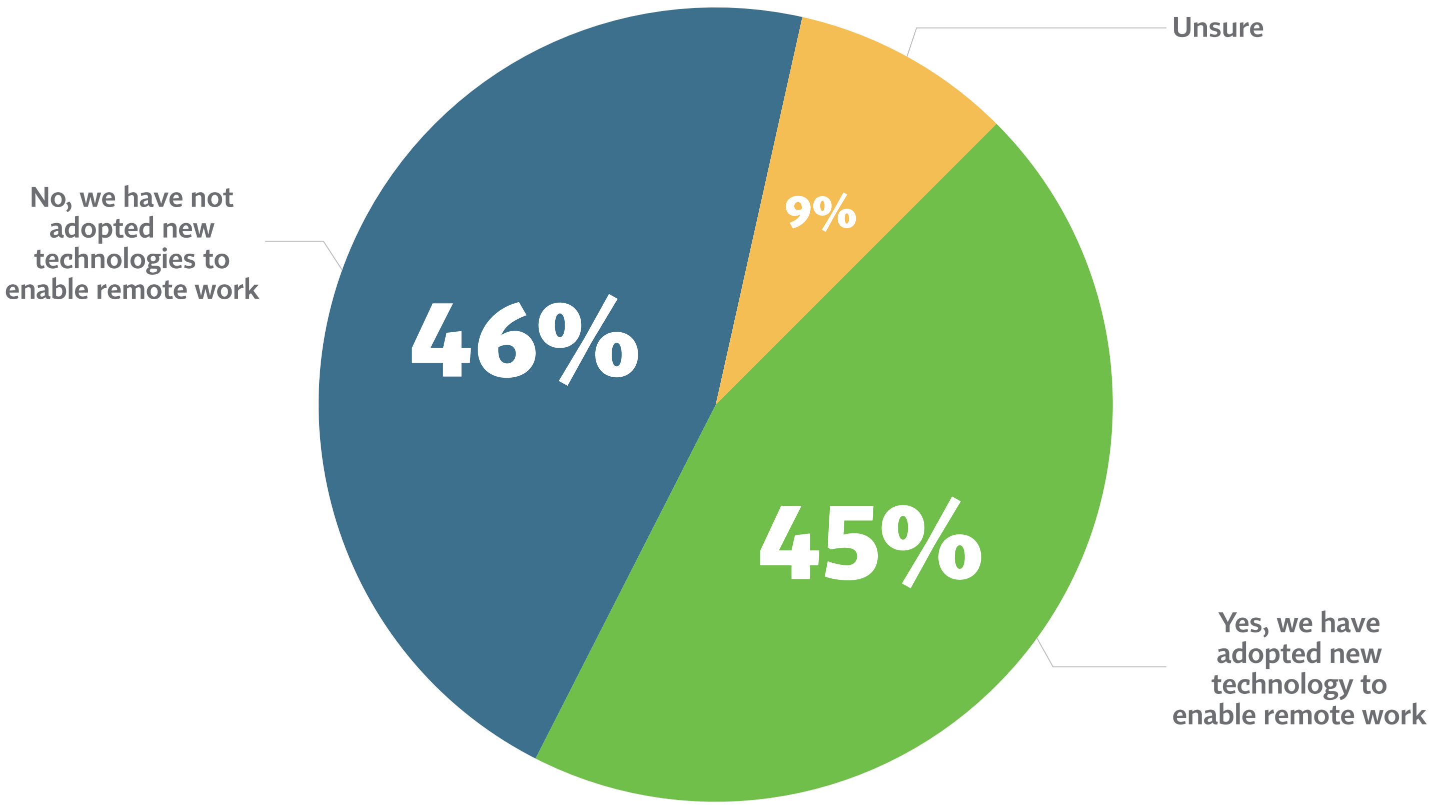
## Remote working policies in response to COVID-19



*Question: Which of the following best describes your organization's policy since the COVID-19 pandemic began?*

# **About half of organizations** have adopted a new technology to enable WFH as a result of COVID-19.

## New tech adoption to enable remote work as a result of COVID-19



*Question: Has your organization adopted new technologies or contracted with new vendors to enable remote work as a result of COVID-19?*

# **Legal services** and **education/academia** have been the biggest new adopters of WFH technologies.

## New tech adoption to enable remote work as a result of COVID-19

| | Yes | No | Unsure |
|---|---|---|---|
| Legal Services | **68%** | **24%** | 8% |
| Education/Academia | **67%** | **22%** | 11% |
| Health care | **60%** | **32%** | 8% |
| Government | **60%** | **28%** | 13% |
| Banking | 54% | 34% | 12% |
| Insurance | 40% | 46% | 13% |
| Software and services | **32%** | **59%** | 9% |
| Tech hardware/equipment | **22%** | **66%** | 13% |
| Marketing | **22%** | **72%** | 6% |
| Materials | **0%** | **60%** | **40%** |
| **OVERALL** | **45%** | **46%** | **9%** |

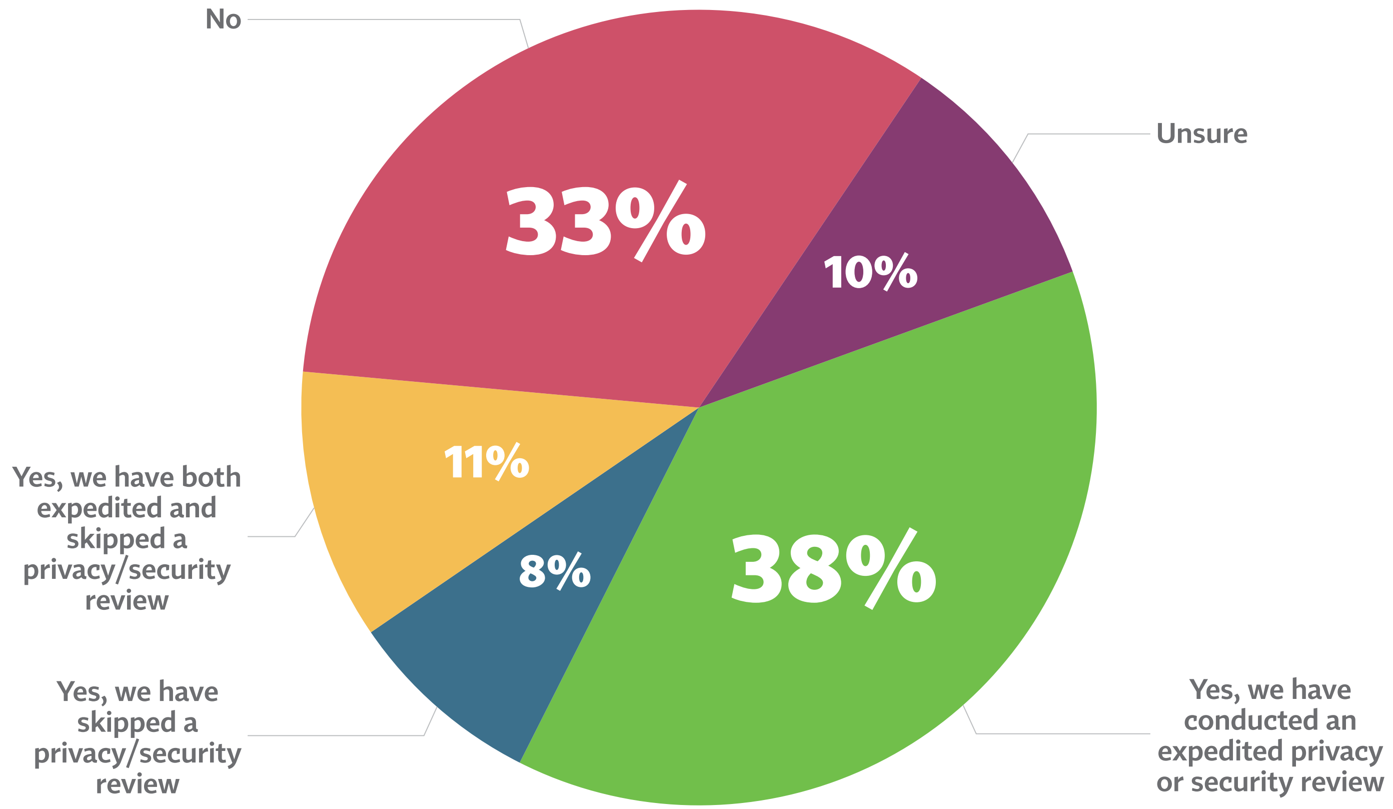
*Statistically significant difference from the overall total.*

*Question: Has your organization adopted new technologies or contracted with new vendors to enable remote work as a result of COVID-19?*

# Of the organizations that have adopted new WFH tech, nearly **60%** has accelerated or bypassed privacy/security review.

## Expedited or skipped privacy/security review as a result of COVID-19

*Base: Have adopted new WFH tech*



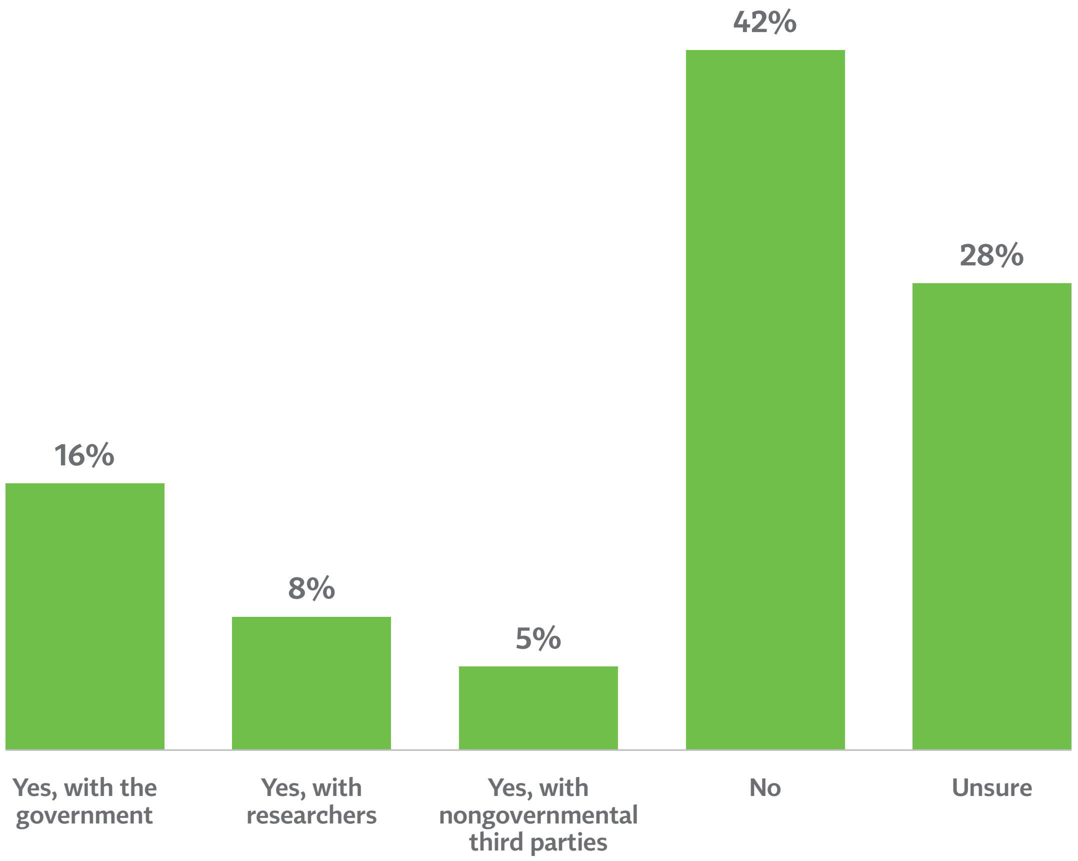
*Question: Has your organization had to expedite or skip privacy or security reviews of new technologies or vendors as a result of COVID-19?*

# COVID-19 DATA COLLECTION AND SHARING

EY Building a better working world
iapp

# **3 in 10 organizations** have been asked to share aggregated/ anonymized COVID-19 data with a third party.

## Has been asked to share aggregated/anonymized COVID-19 data



*Question: Has your organization been asked to share aggregated or anonymized data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

# **More than half** of **telecom, health and government entities** have been asked to share anonymous data to combat COVID-19.

## Has been asked to share aggregated/anonymized COVID-19 data

| | Yes | No | Unsure |
|---|---|---|---|
| Telecommunications | **56%** | **22%** | **22%** |
| Health care | **51%** | **19%** | **15%** |
| Government | **50%** | **25%** | 25% |
| Education/academia | 36% | 37% | 27% |
| Banking | 27% | 40% | 33% |
| Insurance | 8% | 44% | 48% |
| Consulting | 4% | 49% | 46% |
| Legal services | 4% | 80% | 16% |
| Marketing | 0% | 72% | 28% |
| **OVERALL** | **30%** | **42%** | **28%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization been asked to share aggregated or anonymized data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

# Entities in **Australia, New Zealand** and **Canada** have been asked to share more deidentified COVID-19 data than others.

## Has been asked to share aggregated/anonymized COVID-19 data

| | Yes | No | Unsure |
|---|---|---|---|
| Australia/New Zealand | **51%** | **19%** | 30% |
| Canada | **37%** | 38% | 26% |
| United States | 29% | 39% | 32% |
| United Kingdom | 25% | 57% | 18% |
| European Union | 24% | 51% | 26% |
| Asia | 23% | 40% | 37% |
| **OVERALL** | **30%** | **42%** | **28%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization been asked to share aggregated or anonymized data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

# **Larger companies** have been asked to share **more** deidentified COVID-19 data than smaller ones.

## Has been asked to share aggregated/anonymized COVID-19 data

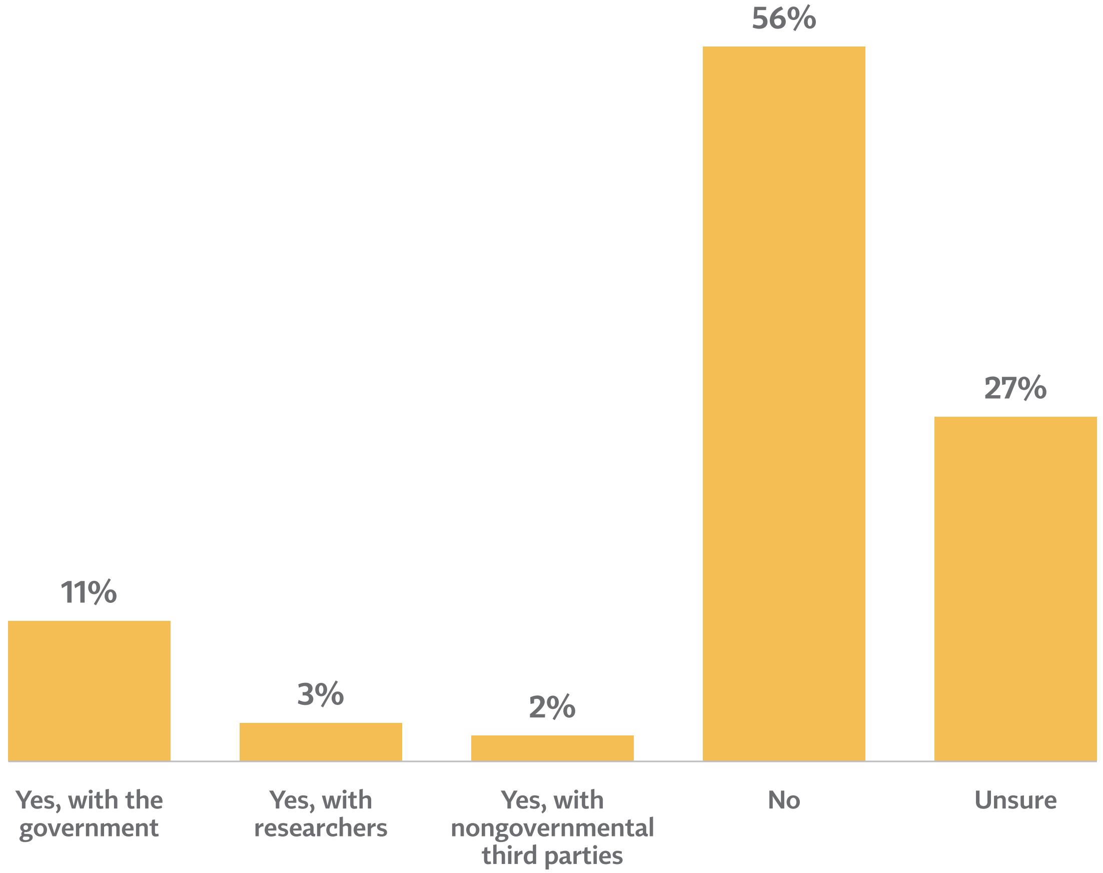
| Size | Yes | No | Unsure |
|---:|:---:|:---:|:---:|
| 1–250 | **25%** | **65%** | **11%** |
| 251–1,000 | **21%** | **58%** | **20%** |
| 1,001–5,000 | 29% | 43% | 28% |
| 5,001–25,000 | **35%** | **33%** | 32% |
| 25,001 or more | **35%** | **28%** | **38%** |
| **OVERALL** | **30%** | **42%** | **28%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization been asked to share aggregated or anonymized data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

# **1 in 7 organizations** have been asked to share personally identifiable COVID-19 data with a third party.

## Has been asked to share personally identifiable COVID-19 data



*Question: Has your organization been asked to share personally identifiable data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

# **Health care** and **government entities** have been asked **most frequently** to share identifiable COVID-19 data.

## Has been asked to share personally identifiable COVID-19 data

| | Yes | No | Unsure |
|---|---|---|---|
| Health care | **45%** | **34%** | **21%** |
| Government | **35%** | **42%** | 22% |
| Telecommunication services | 27% | 57% | 16% |
| Education/academia | 20% | 52% | 29% |
| Insurance | 10% | 56% | 34% |
| Banking | 9% | 56% | 35% |
| Software and services | 8% | 67% | 25% |
| Consulting services | 7% | 54% | 39% |
| **OVERALL** | **16%** | **56%** | **27%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization been asked to share personally identifiable data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

# Entities in **Australia/New Zealand** have been asked the **most** to share identifiable COVID-19 data.

## Has been asked to share personally identifiable COVID-19 data

| | Yes | No | Unsure |
|---|---|---|---|
| Australia/New Zealand | **42%** | **29%** | 29% |
| Canada | 24% | 49% | 28% |
| Asia | 22% | 46% | 32% |
| United States | 16% | 54% | 31% |
| European Union | 11% | 66% | 23% |
| United Kingdom | 8% | 74% | 18% |
| **OVERALL** | **16%** | **56%** | **27%** |

***Statistically significant difference from the overall total.***

*Question: Has your organization been asked to share personally identifiable data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

# **Small organizations** have been asked **less often** than larger ones to share identifiable COVID-19 datasets.

## Has been asked to share personally identifiable COVID-19 data

| Size | Yes | No | Unsure |
|---:|:---:|:---:|:---:|
| 1–250 | **7%** | **81%** | **12%** |
| 251–1,000 | **9%** | **70%** | 22% |
| 1,001–5,000 | 17% | 56% | 27% |
| 5,001–25,000 | **24%** | **51%** | 26% |
| 25,001 or more | 18% | 42% | 40% |
| **OVERALL** | **16%** | **56%** | **27%** |

*Statistically significant difference from the overall total.*

*Question: Has your organization been asked to share personally identifiable data with government entities, researchers or other third parties related to combatting the COVID-19 pandemic?*

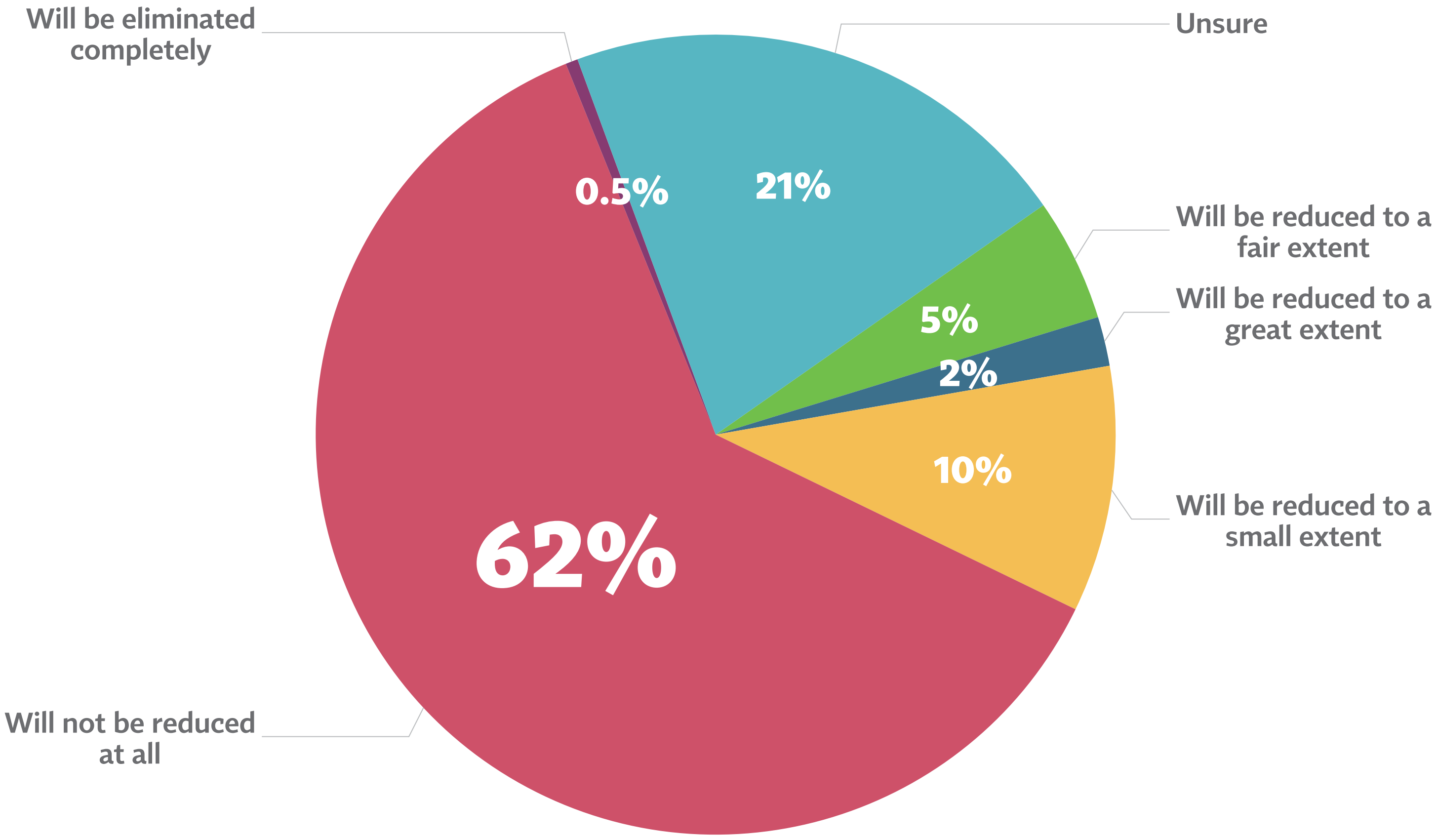
# PRIVACY STAFFING AND BUDGET

EY Building a better working world

iapp

# **Most organizations do *not*** expect significant privacy layoffs as a result of COVID-19.

## Effect of COVID-19 on privacy staffing



*Question: To what extent, if any, do you believe that your organization's privacy staffing will be reduced due to the COVID-19 pandemic and ensuing economic downturn?*

# **Hospitality, business services** and **marketing** expect the greatest cuts to privacy staff.

## Expected reduction in privacy staffing due to COVID-19

| | Not at all/small extent | A fair/great extent | Eliminated | Unsure |
|---|---|---|---|---|
| Hotels, restaurants and leisure | **50%** | **21%** | **7%** | 21% |
| Business services | 68% | 10% | **5%** | 18% |
| Marketing | **44%** | **23%** | 0% | **33%** |
| Software and services | 79% | 6% | 1% | 14% |
| Government | 78% | 4% | 0% | 18% |
| Health care | 80% | 4% | 0% | 17% |
| **OVERALL** | **72%** | **7%** | **<1%** | **21%** |

***Statistically significant difference from the overall total.***

*Question: To what extent, if any, do you believe that your organization's privacy staffing will be reduced due to the COVID-19 pandemic and ensuing economic downturn?*

# Expectations for **privacy staffing cuts** are **similar** around the world, with the U.K. bracing for a bit more.

## Expected reduction in privacy staffing due to COVID-19

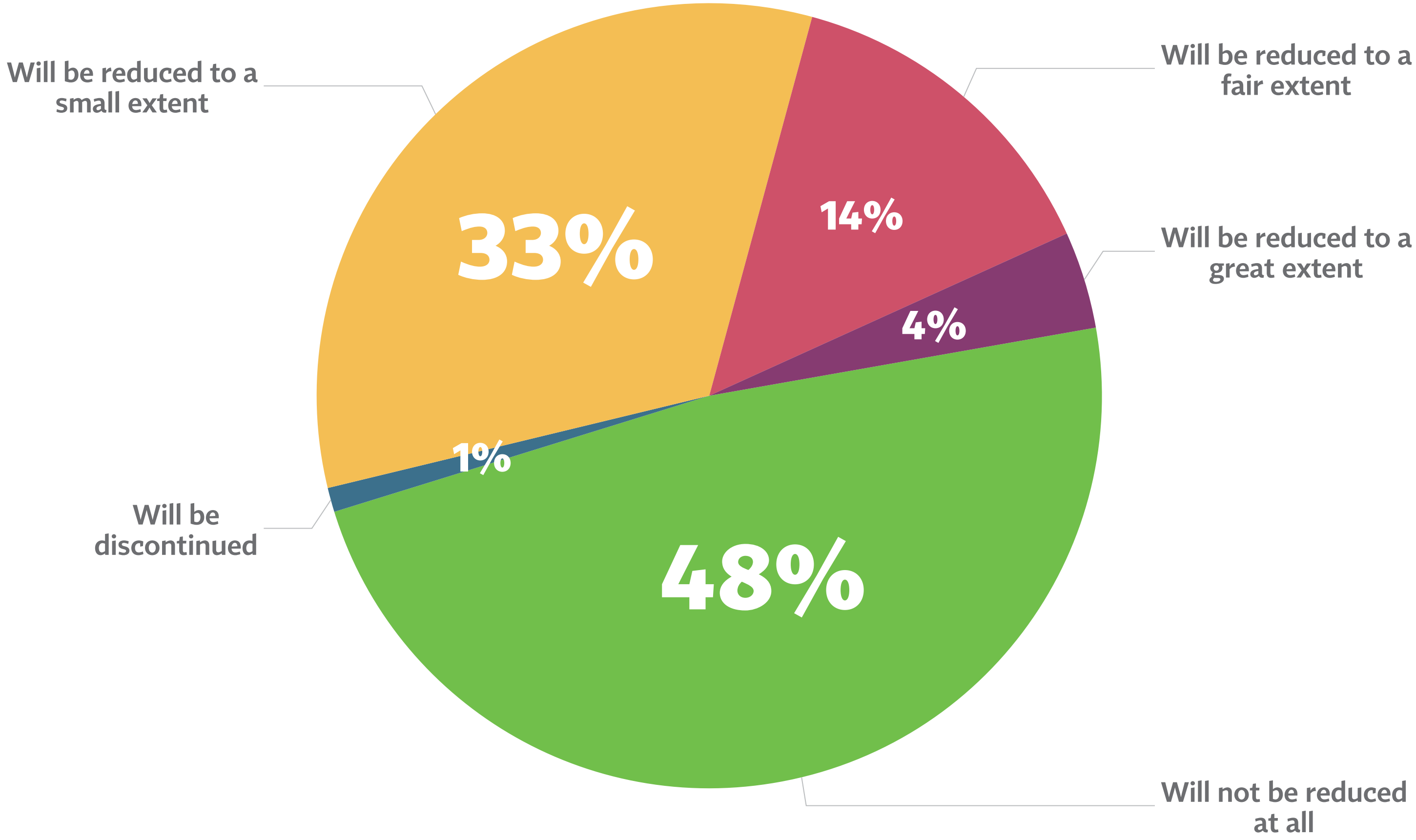
| | Not at all/small extent | A fair/great extent | Eliminated | Unsure |
|---|---|---|---|---|
| United Kingdom | **64%** | **16%** | 1% | 18% |
| Australia/New Zealand | 66% | 13% | <1% | 23% |
| United States | 71% | 6% | <1% | 22% |
| Canada | 79% | 7% | <1% | 14% |
| Asia | 68% | 3% | 3% | 28% |
| European Union | 77% | 5% | 0% | 18% |
| **OVERALL** | **72%** | **7%** | **<1%** | **21%** |

***Statistically significant difference from the overall total.***

*Question: To what extent, if any, do you believe that your organization's privacy staffing will be reduced due to the COVID-19 pandemic and ensuing economic downturn?*

# **More than 80%** of privacy pros expect **minimal to no cuts** to privacy budgets.

## Effect of COVID-19 on privacy budget



*Question: To what extent, if any, do you believe that your organization's privacy staffing will be reduced due to the COVID-19 pandemic and ensuing economic downturn?*

# **Transport** and **business services** expect the most privacy budget cuts, while **government** and **health** expect the least.

## Expected reduction in privacy staffing due to COVID-19

| | Not at all/small extent | A fair/great extent | Discontinued |
|---|---|---|---|
| Transportation | **66%** | **34%** | 0% |
| Business services | **68%** | **32%** | 0% |
| Hotels, restaurants and leisure | 65% | 28% | 7% |
| Retail | 71% | 29% | 0% |
| Software and services | 80% | 18% | 2% |
| Health care | **88%** | **13%** | 0% |
| Government | **91%** | **9%** | 0% |
| **OVERALL** | **81%** | **18%** | **1%** |

***Statistically significant difference from the overall total.***

*Question: To what extent, if any, do you believe that your organization's privacy staffing will be reduced due to the COVID-19 pandemic and ensuing economic downturn?*

# Companies in **Canada** and the **EU** expect **fewer privacy budget reductions** than those in other countries.

## Expected reduction in privacy staffing due to COVID-19

| | Not at all/small extent | A fair/great extent | Discontinued |
|---|---|---|---|
| United Kingdom | 77% | 22% | 1% |
| United States | 79% | 19% | 1% |
| Australia/New Zealand | 74% | 27% | 0% |
| Asia | 81% | 18% | 3% |
| Canada | **88%** | **11%** | 0% |
| European Union | **87%** | **13%** | 1% |
| **OVERALL** | **81%** | **18%** | **1%** |

*Statistically significant difference from the overall total.*

*Question: To what extent, if any, do you believe that your organization's privacy staffing will be reduced due to the COVID-19 pandemic and ensuing economic downturn?*

# CONTACTS

**Angela Saverice-Rohan**

EY Americas and FSO Privacy Leader

Angela.SavericeRohan@ey.com

**Tony de Bos**

EY Global and EMEIA Data Protection Leader

Tony.de.Bos@nl.ey.com

**Kris Lovejoy**

EY Global Cybersecurity Leader

Kristin.Lovejoy@eyg.ey.com

EY Building a better working world | iapp