# IAPP-EY Annual Privacy Governance Report 2022

# Table of Contents

# What should a privacy function look like in 2022 and beyond?

## Foreword

The word “governance” ultimately derives from the Greek verb kubernaein (κυβερνάω), meaning to steer. Many privacy professionals seek the perfect metaphorical vehicle to help steer them to success as they navigate the most complicated of paths while trying to stay ahead of the competition and avoid the many obstacles along the way.

For many, this can feel like they are steering an oil tanker, across the Atlantic Ocean, with a spade, while navigating a Category 5 hurricane.

Yet, effective governance is not just about getting to the end point. If done correctly, it seeks to drive more productivity out of the workforce by engaging employees to increase loyalty and buy-in to help achieve the organization’s strategic objectives. It also positions organizations to stay nimble as they navigate the always shifting tides of privacy.

In this year’s IAPP-EY governance survey report we go back to the foundations of governance, seeking to explore “the way that organizations are managed, and the systems for doing this,” with a view to shedding light on the question senior executives routinely ask chief privacy officers: “What should a privacy function look like in 2022 and beyond?”

This year’s survey is set against the backdrop of the widespread changes brought about by COVID-19 and how it forced organizations to change how they interacted with their customers, their employees, and their partners.

So many conversations this year have started with "have you gone back to the office?" or "now we are allowed out perhaps we can grab a coffee?" or, one of my favorites, "it would be nice to meet you in person!"

COVID-19 inflicted change is just the start, with fundamental market drivers causing significant disruption including:

- **Increased staff turnover**: Challenges associated with the "great resignation," a global trend where record numbers of employees changed jobs.
- **Spiraling staff costs**: Wage inflation set record highs across the world.
- **High inflation**: Hit double digit levels not seen for decades.
- **The Fourth Industrial Revolution**: Accelerating technological change and the blurring of boundaries between the physical, digital and biological worlds.

For privacy professionals this is all challenging enough, but we also have the multipliers of:

- **New privacy regulations**: These continue to emerge across the world, adding new and increasingly complex requirements to the already complicated mix.
- **Privacy as a household word**: Individuals better understand their rights and push organizations to provide increased transparency and control over personal information processing.

These factors combined have put stresses and strains on organizations' governance structures far beyond the norm of the last 20 years. Privacy functions have the opportunity to evolve to meet these ever-changing market challenges. Whether they can do so at pace will continue to serve as the defining challenge of the profession.

**Mark Thompson**
Chief Strategy Officer, IAPP

**Angela Saverice-Rohan**
EY Global Privacy Leader

More than 700 responded from over 40 countries to the 29-question governance survey.

# Executive summary

This year's research focused on five key foundational areas of governance:

→ **Governance and operating model**: The organizational structures, roles and responsibilities for managing the collection, use, retention, disclosure and disposal of personal data.

→ **Privacy strategy and planning**: The activities undertaken by the privacy office to determine the strategic direction of the privacy office and its associated planning activities.

→ **Compensation management**: The annual process of determining the compensation of privacy office staff.

→ **Budget management**: The processes and activities supporting the development, approval and spending of annual privacy budgets.

→ **Performance metrics and monitoring**: The processes and measurements to understand how the organization is performing against privacy strategy.

This report is meant to serve as a point-in-time "check-in" for the privacy profession. What does the average privacy office look like in 2022?

## Scope

We asked our global membership base to complete the 29-question governance survey. Over the course of 10 weeks, more than 700 responded from over 40 countries.

# Summary of results

### There is no golden model for the privacy office

More than 50% of organizations report their privacy office is spread across more than one line of defense; 37% of organizations have it spread out across all three. Additionally, the location of the privacy office and the structure of the privacy function is dependent on what is right for that particular organization and their organizational strategy and structure.

### Privacy function responsibilities continue to expand

The breadth and scope of activities undertaken by the privacy function continues to grow far beyond the traditional expectations of a "data protection officer." More than 30% of organizations are prioritizing international transfer rules and privacy impact assessments. These increasing demands are creating both demand management and prioritization challenges.

### Privacy is increasingly aligned with organizational strategy

An organization's privacy strategy is increasingly aligned with the organization's overall corporate strategy, with 66% of respondents having at least "considerable" alignment.

### Privacy is hiring, but it's not enough

The demand for privacy expertise continues to accelerate, with the average privacy team growing by 12%. The need for the skills and experience that help organizations "navigate the most complicated of paths" is compounded by the limited availability of privacy professionals across workforce function areas.

### The ratio of privacy staff to company resources is reasonably consistent

Despite the significant variance in organizational approaches to privacy, the ratio of privacy resources deployed to support the management of privacy is reasonably consistent across industries and geographies at approximately two to three staff members per billion U.S. dollars of revenue.

### Privacy investment continues

Organizations continue to invest skills and resources into privacy as a strategic imperative. On average, more than 50% of an organization's privacy budget is allocated to salary and benefits.

### Most, but not all, companies gather privacy metrics

While the vast majority of organizations collect privacy metrics, almost 20% of organizations indicated they do not. These metrics are used more for analyzing company performance than informing privacy strategy.

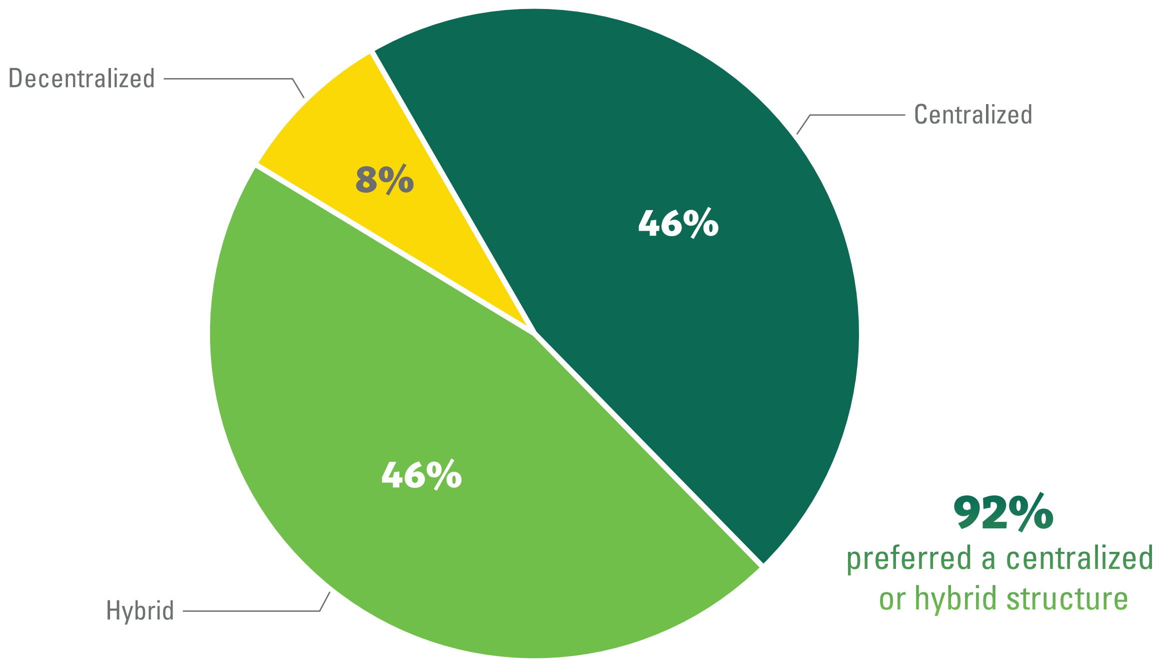
While the privacy profession is showing signs of pressure in some areas — staff turnover, organizational alignment, and resource allocation — it is also maturing and developing. Teams continue to grow in size and purpose, while developing closer relationships with company leaders and consumers alike. Corporate governance and organizational models, in the myriad forms they can take, play a key role in the performance of the privacy function overall.

More than 90% of respondents indicated a preference for centralized or hybrid structures.

## Governance is foundational to success

Market challenges, the profusion of new touch points across organizations, and the resultant proliferation of personal data have caused digital systems to continue to explode. The amount of data created or consumed in some form across the entire world — from the natural language processing-enabled chat bot to the employee on the shop floor — has grown almost 50 times since 2010, to 97 zettabytes or 97,000,000,000,000 gigabytes! As such, the last few years have seen a perfect storm which have forced organizational structures to change and adapt.

**Types of governance structures**



For every business — whether it is a small innovative startup, a business located in only one country, a big, listed entity, or a global 25 multinational — organizational governance is foundational to how privacy professionals operate every day. In some ways, governance choices and structures are so pervasive that their importance to our daily work is not fully appreciated.

Internal structures, procedures and processes don't just allow organizations to run efficiently and effectively, they provide clarity to management, investors, employees, and customers on how an organization runs. If done right, they help to direct and influence the value and culture of the organization itself.

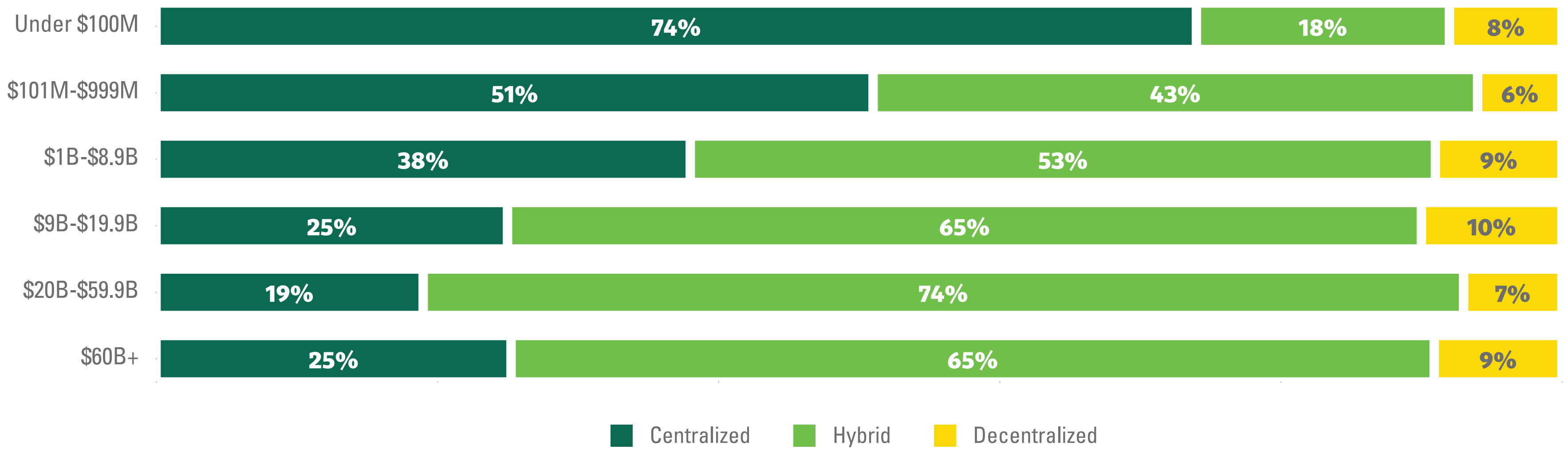
Many organizational functions have learned the hard way that effective governance is critical to ensuring success. Simply walk across the office to the finance or human resources functions and they will have a treasure trove of stories around historical issues that have arisen through weak governance.

The privacy office has become an important pillar of governance. As privacy functions have matured, they have been forced to evolve to meet organizational needs, often defining their place somewhere on the centralized vs. decentralized continuum.

Our survey results provide a compelling view that organizations are in favor of a centralized or hybrid approach to organizational structure:

- → More than 90% of respondents indicated a preference for centralized or hybrid structures.
- → There was only a 3% variance across geographic regions and a 10% variance by sector.
- → Companies with lower revenues favor centralized approaches. The preference for a hybrid structure generally increases as company revenue does. *(See graph below).*

**Types of governance structures by revenue**



75% of companies have their privacy office to some extent in the second line of defense.

## Drawing the lines of defense

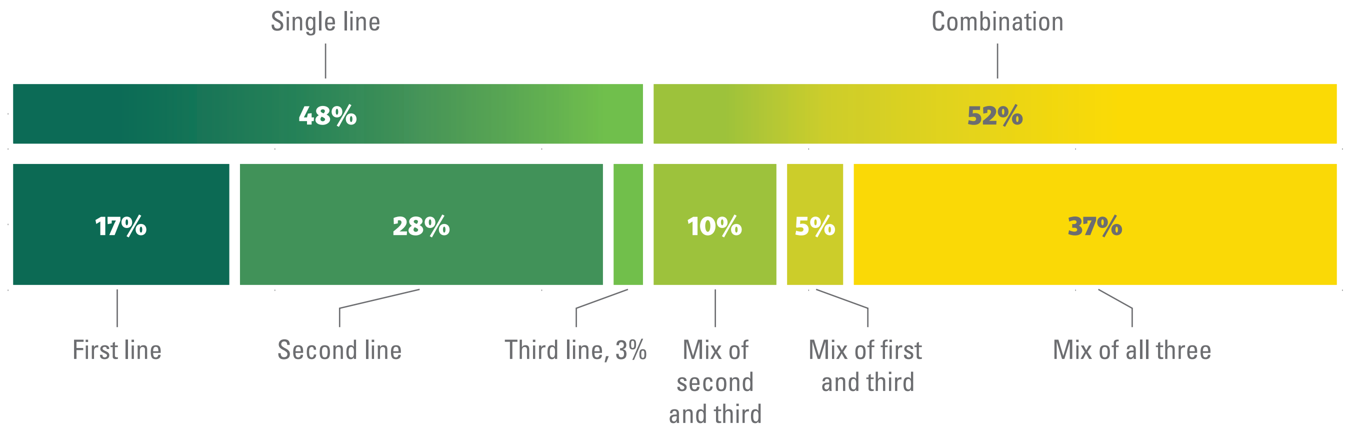
The “Three Lines of Defense” model is often used by organizations as a way of explaining the relationship between functions and how responsibilities should be divided.

01 **The first line of defense: Those who own and manage risks.**
These functions are made up of managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives.

02 **The second line of defense: Those who oversee or who specialize in compliance or the management of risk.**
These functions provide the policies, frameworks, tools, techniques, and support to enable risk and compliance to be managed in the first line, conduct monitoring to judge how effectively risk is mitigated and helps ensure consistency of definitions and measurement of risk.

03 **The third line of defense: Those who provide independent assurance.**
These functions, which often report to the board or an audit committee, ensure that the first two lines are operating effectively and advise how they could be improved. It can also give assurance to sector regulators and external auditors that appropriate controls and processes are in place and are operating effectively.

Three lines of defense model



### Where do privacy professionals' roles fit into this model?

Our respondents were almost evenly split as to whether their privacy office falls into a single line of defense or in some combination of the three lines.

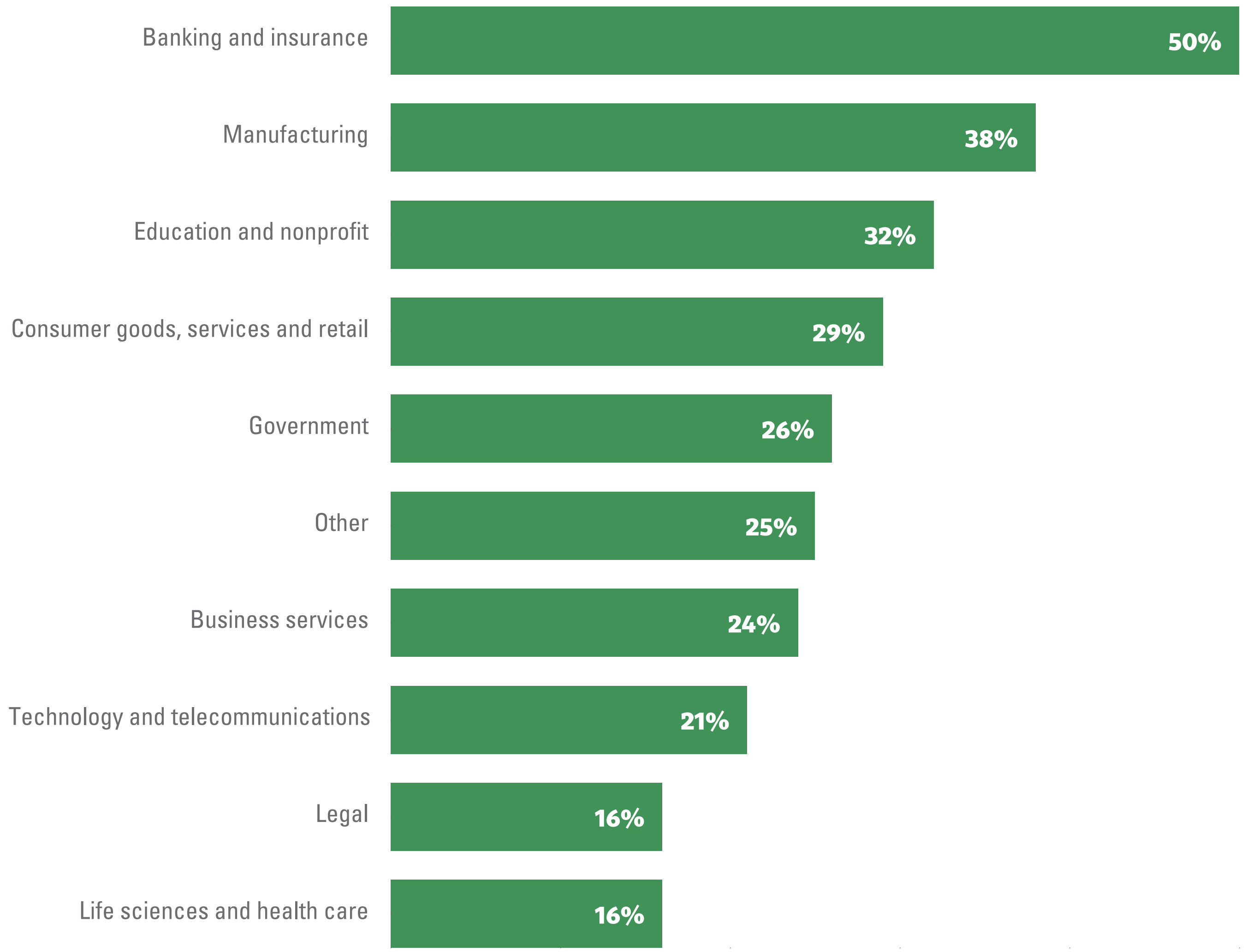
The second line of defense is the most popular position for organizations who only use a single line of defense, and is the most popular line when looking at the model as a whole:

- → 75% of companies have their privacy office to some extent in the second line.
- → 59% have it to some extent in the first line.
- → 55% have it to some extent in the third line.

To what extent this second-line activity is focused on risk management and compliance versus supporting privacy-enabled value creation, i.e., supporting privacy enabled analytics, is an open question for future exploration.

> Privacy professionals must work across organizational lines and levels to translate policies into practice. This demands fluency in law, technology, business, and design. Regardless of where the function is housed, privacy professionals are collaborating across all three lines. That's the multifaceted challenge of privacy.
>
> **Caitlin Fennessy**
> IAPP Chief Knowledge Officer

Second line of defense model by sector



## Other notable insights

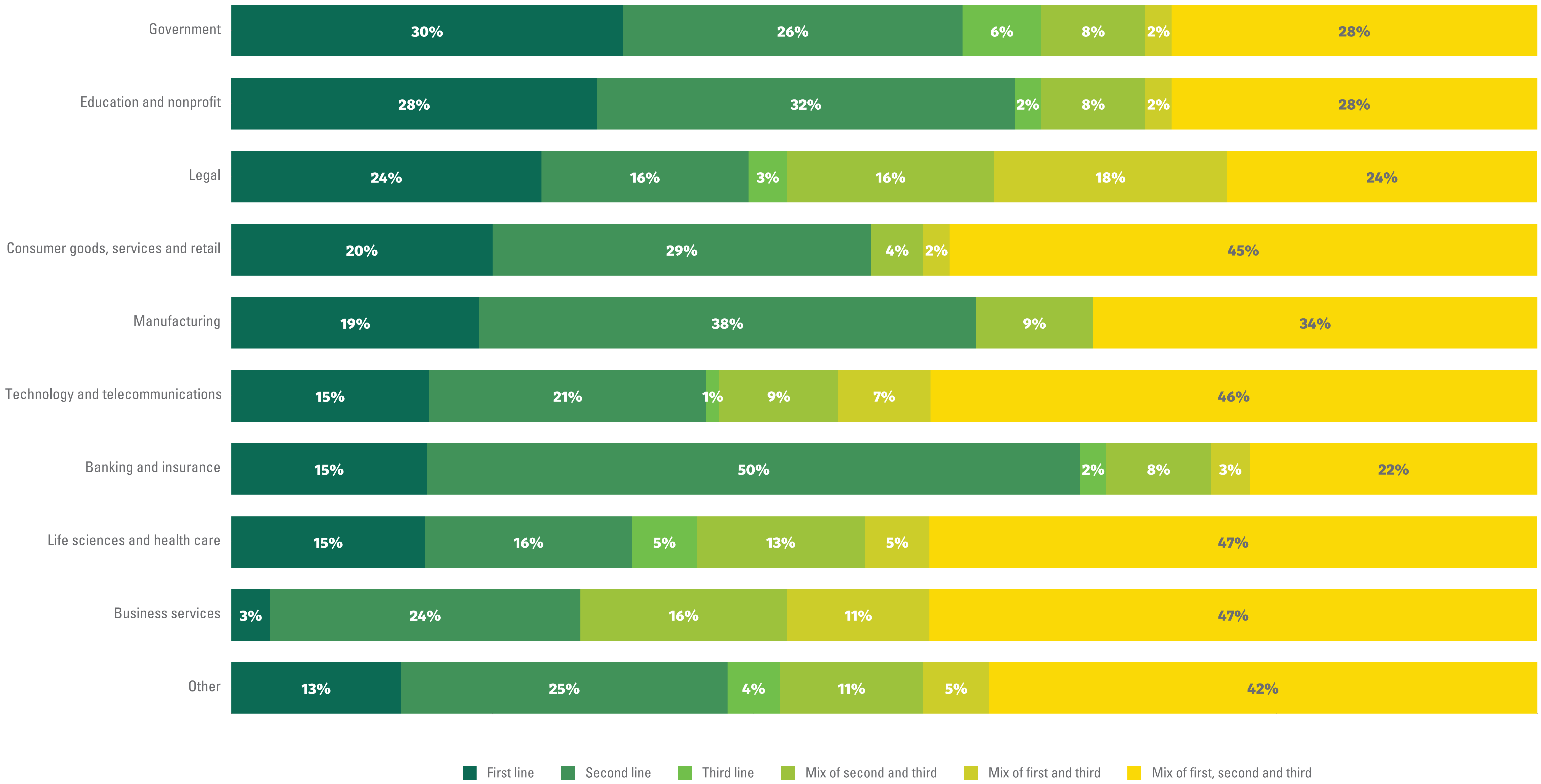
- → There is an interesting degree of variability by industry: for example, 50% of respondents in banking and insurance indicated that they use a second-line model, compared to just 16% in life sciences and health care, both of which are highly regulated global sectors. *(See graph to the left).*
- → 50% of Asia-based privacy offices operated across all three lines of defense.
- → 55% of respondents with annual revenues of more than $60 billion have privacy offices across the three lines of defense, compared to just 34% of respondents with less than $100 million in annual revenues.
- → Organizations that use a combination defense model appear to favor spreading it out across the three lines. Those that prefer to house the privacy function exclusively in a single line, typically select the first or second, but rarely the third.

**"Increasingly, organizations are applying the three lines of defense model to effectuate privacy risk management in their organizations. This requires delineation of risks across the business and decisions about who will be accountable as well as formalizing the right governance routine to bring all of it together. Once the interlock is well defined between the lines, the organization can manage for new privacy regulations or privacy risk reporting much more efficiently. The success of this model is highly dependent on the organization's controls. Organizations can't get to accountability without robust controls and they can't control risk without accountability."**

**Angela Saverice-Rohan**

EY Global Privacy Leader

Three lines of defense model by sector

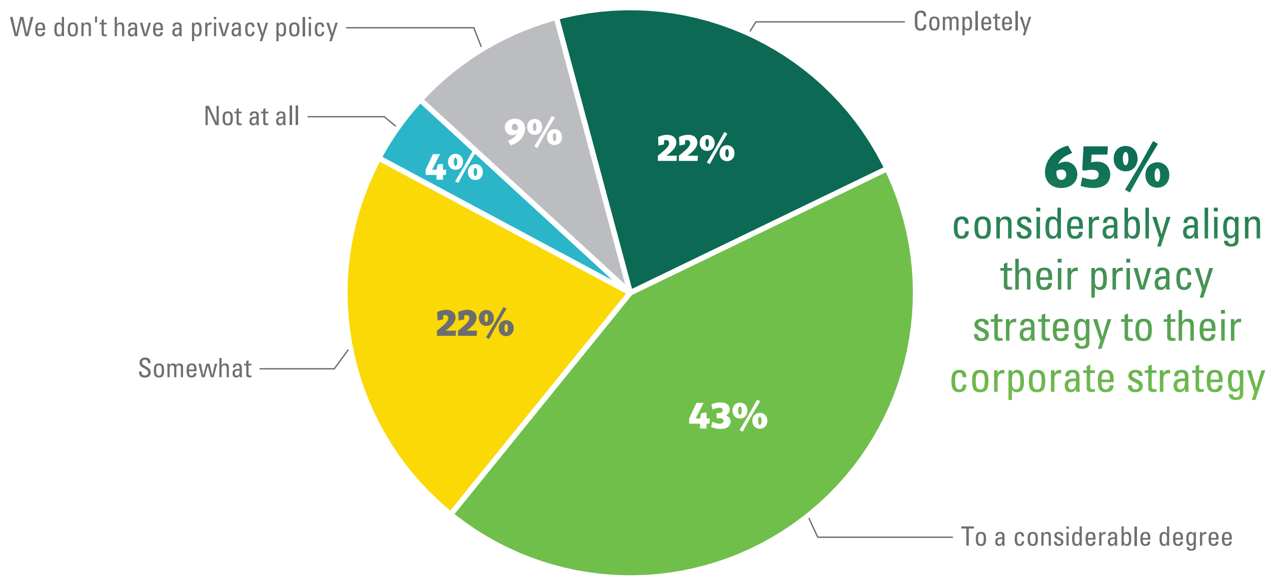


Two-thirds of respondents "considerably" align their privacy strategy to their corporate strategy.

## The essence of strategy: Choosing what not to do

Despite the need to be attentive to the constantly changing landscape of privacy regulation, an organization is often more effective when its privacy strategy is aligned with its overall corporate strategy. By contrast, unaligned strategies often result in conflicting efforts that can significantly undermine an organization's productiveness. For instance, prioritizing children's privacy is a worthy endeavor from a moral, legal and consumer trust standpoint. But when strategies are unaligned, and an organization decides to no longer sell child-directed products or services, a privacy professional's noble efforts are unlikely to provide benefit to the organization.

**Alignment of privacy strategy with overall corporate strategy**



Privacy professionals must engage with their organization's overall strategy to design and maintain a privacy strategy that is best suited to the organization's objectives. This year, we set out to understand the extent to which an organization's privacy strategy was aligned with its overall corporate strategy.

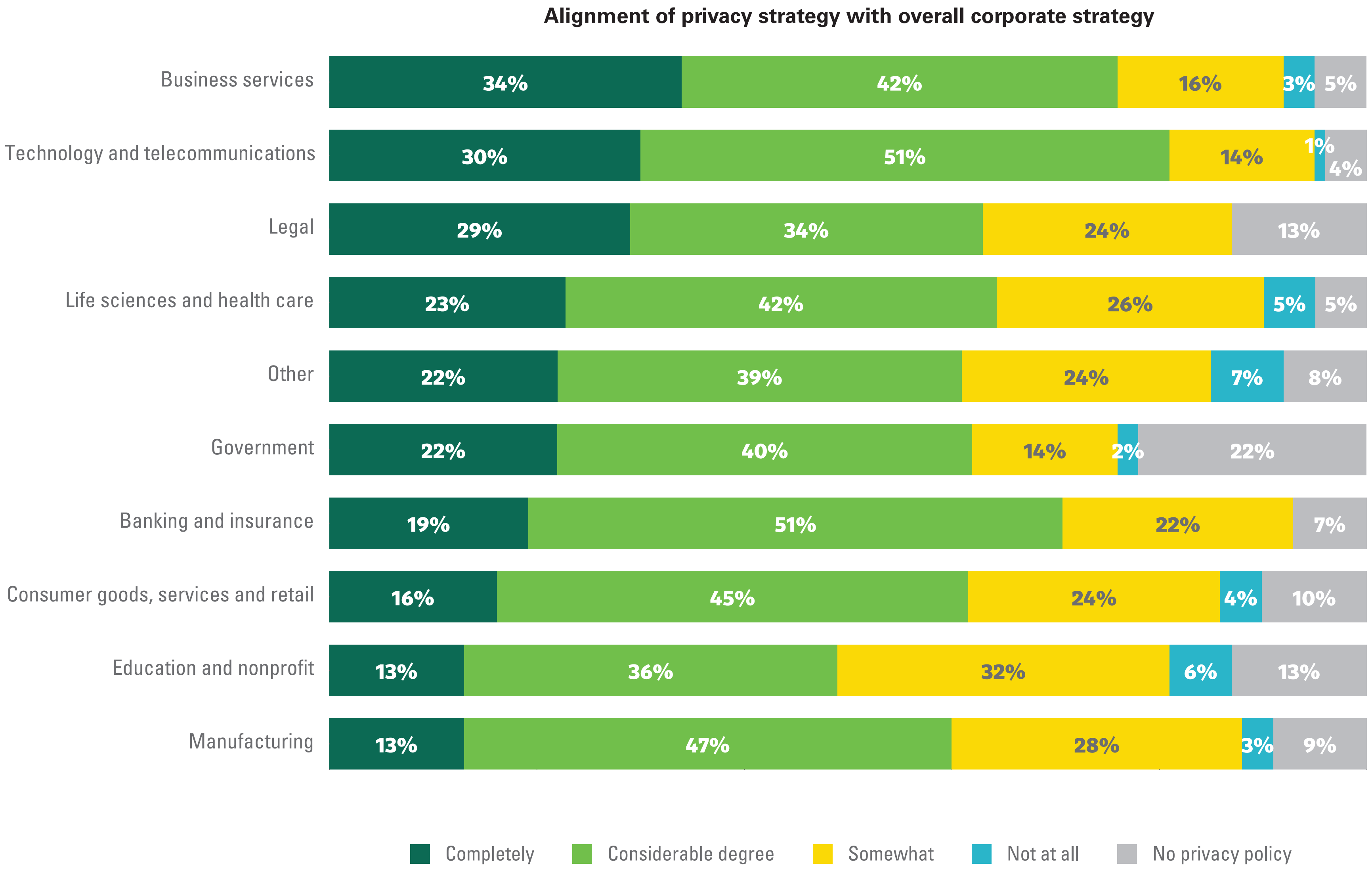
## Our results

→ Two-thirds of respondents surveyed "considerably" align their privacy strategy to their overall corporate strategy.

→ 13% either do not have a privacy strategy or have one that does not align at all with their corporate strategy.

→ Broken down by industry, we see that business services companies are most likely to completely align their privacy strategy with their overall corporate strategies (34%), while manufacturing firms and educational/nonprofit organizations are least likely to completely align their strategies (13%). *(See graph to the right).*

→ More than one-fifth of businesses in the governmental sector do not have a privacy strategy. *(See graph to the right).*



## How often are these strategies reviewed and updated?

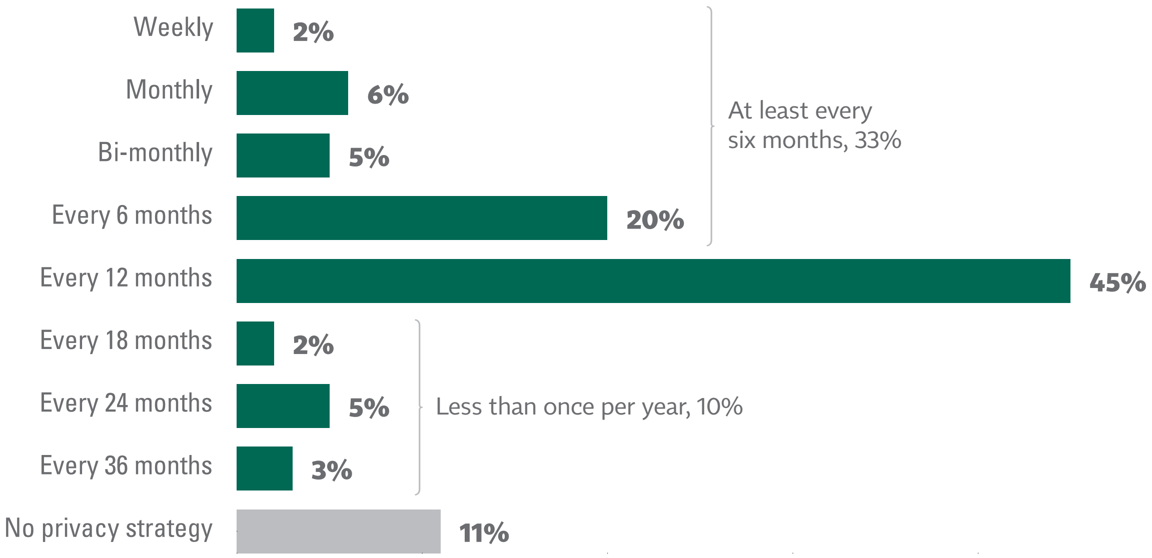
→ More than a third of respondents with a privacy strategy reported updating it at least every six months. *(See graph below).*

→ Another half reported updating their strategy every 12 months. *(See graph below).*

→ This left only 11% who update their privacy strategy less than annually. *(See graph below).*

While these results indicate that privacy offices are already strategic, they have the opportunity to further align their strategies to ensure they can demonstrate to company executives the strategic benefit and value of the privacy function and how it supports the organization's objectives.

**Frequency of reviewing/updating privacy strategy**

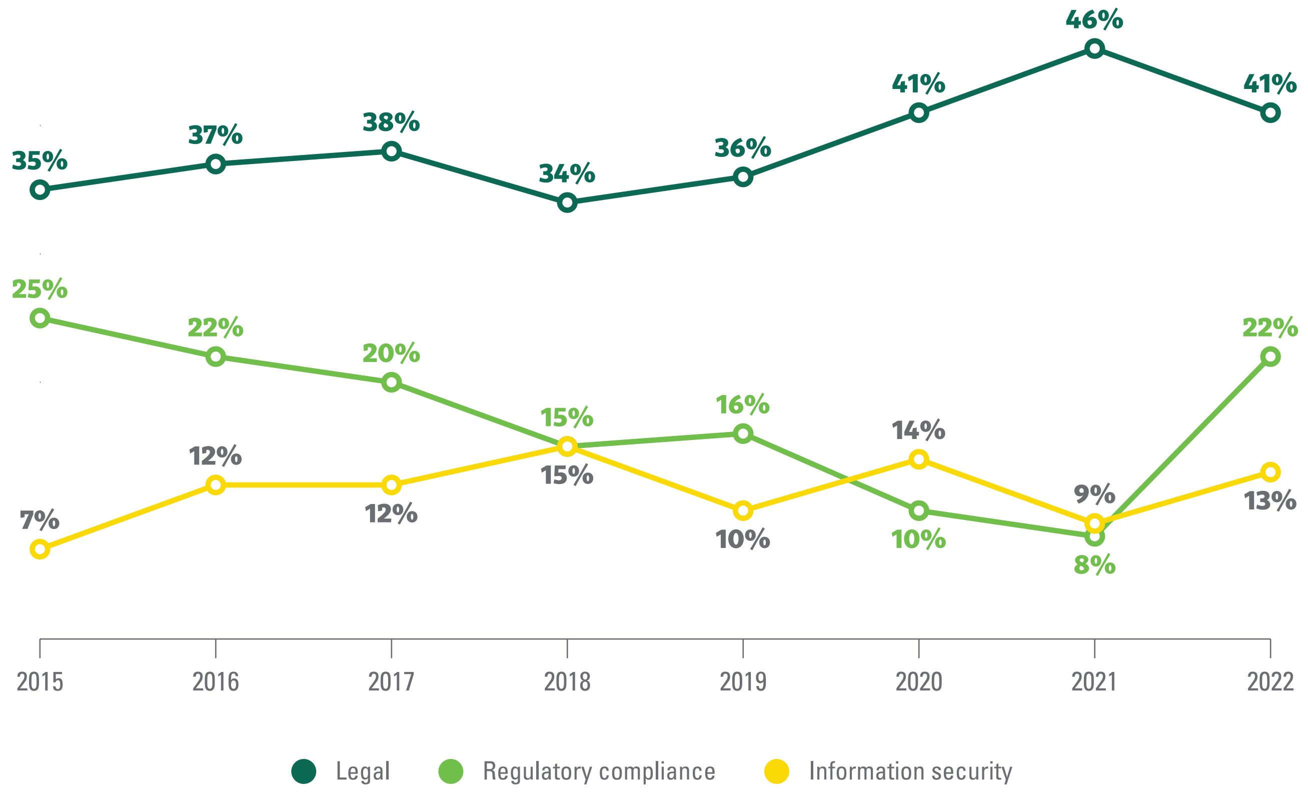


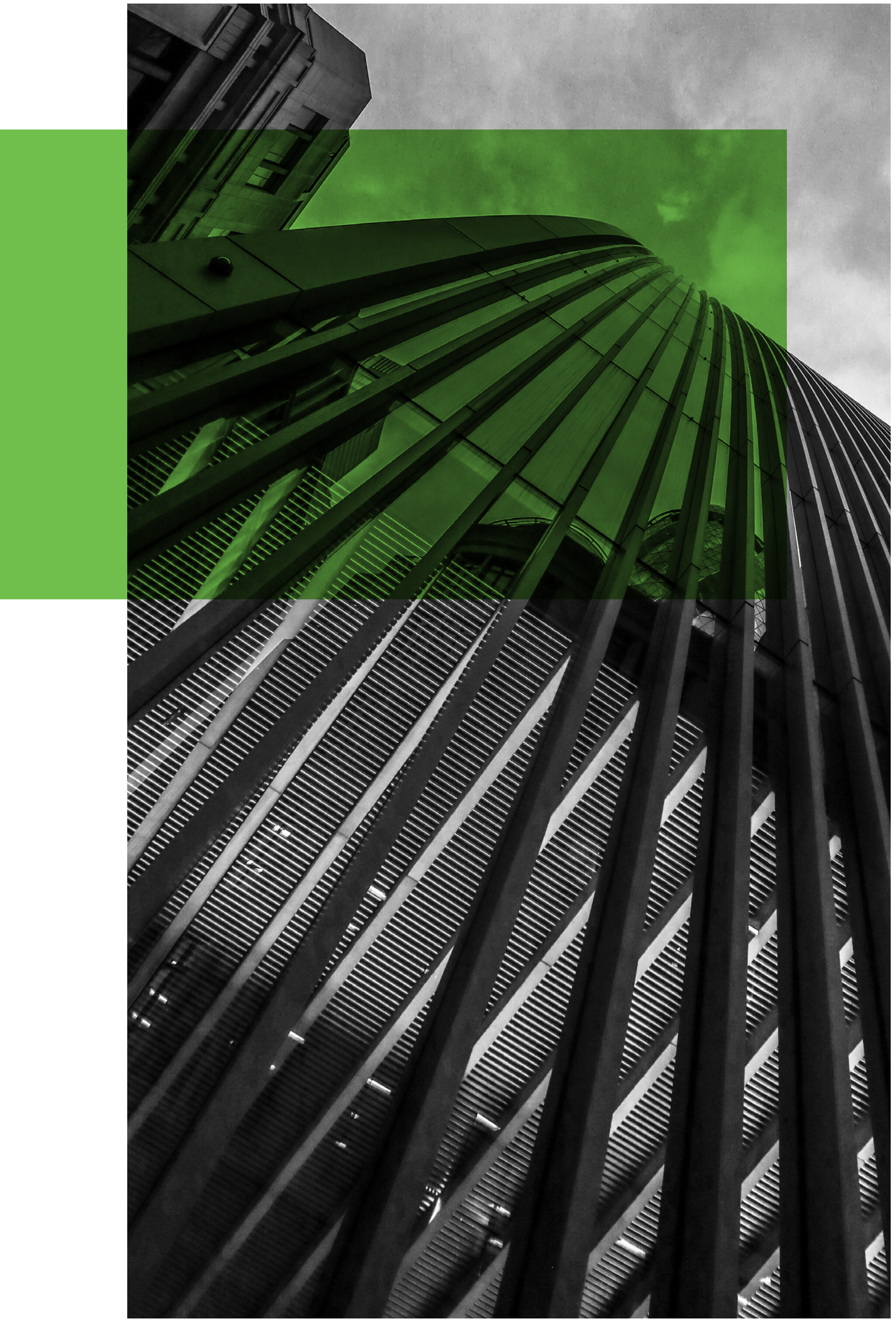
Legal remains the most prominent place for privacy offices at 41%.

## To be or not to be in the legal department?

Organizations frequently change form to address evolving needs, perhaps by changing their operating model or altering their privacy strategy, for example. Among these needs is the ability to have a functional, nimble and efficient privacy office. This can take several forms depending on the organization and its structure and hierarchy.

Where privacy function is housed, trend





## Understanding how corporate governance affects the location of the privacy function

- → The legal department is still the most popular place to house the privacy function in an organization (41%), but there was a slight downward trend between last year and this year.
- → Approximately 20% of businesses in both the education/nonprofit and government sectors house their privacy function in the information security department, compared with just 3% in the legal profession. *(See table on next page).*
- → Almost half of organizations in North America house their privacy function in legal, compared to approximately one-third of organizations across the rest of the world.
- → In a significant change, the percentage of companies housing their privacy function in the regulatory and compliance department more than doubled to 22%.
- → 20% of respondents have privacy departments located in "other" functions, like finance/operations and facilities.
- → At 34%, Asia is the only continent where the compliance department is most popular. Every other continent prefers the legal department.
- → Generally speaking, companies with higher revenue are more likely to house their privacy functions in departments other than legal.

What has caused these shifts? Perhaps the growing multidisciplinary focus of privacy offices. An effective privacy program does not usually focus on a singular domain, but rather considers facets such as consumer trust, data regulation, and privacy education, in addition to more common issues like compliance and legal risk.

**Where privacy function is housed by sector**

| | | SECTOR | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| DEPARTMENT | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| Legal | 41% | 33% | 55% | 32% | 39% | 53% | 24% | 39% | 66% | 34% | 38% |
| Compliance | 22% | 34% | 16% | 9% | 26% | 14% | 14% | 32% | 18% | 25% | 22% |
| Information security | 13% | 7% | 8% | 21% | 5% | 16% | 20% | 11% | 3% | 9% | 18% |
| Corporate risk | 5% | 11% | 5% | 11% | 3% | 0% | 4% | 6% | 0% | 3% | 3% |
| Operations | 4% | 1% | 8% | 8% | 8% | 4% | 0% | 2% | 0% | 3% | 4% |
| Finance and accounting | 2% | 0% | 1% | 2% | 0% | 2% | 4% | 0% | 0% | 9% | 2% |
| Business development | 1% | 1% | 1% | 2% | 3% | 0% | 0% | 0% | 3% | 0% | 2% |
| Marketing | 1% | 3% | 0% | 0% | 0% | 2% | 2% | 0% | 0% | 3% | 1% |
| Customer service/relations | 1% | 0% | 1% | 0% | 3% | 0% | 2% | 2% | 0% | 3% | 1% |
| Human resources | 1% | 1% | 0% | 0% | 5% | 0% | 2% | 0% | 0% | 0% | 1% |
| Research and development | 1% | 0% | 1% | 2% | 0% | 0% | 0% | 0% | 0% | 0% | 1% |
| Internal audit | 0% | 0% | 0% | 2% | 0% | 2% | 0% | 0% | 0% | 3% | 0% |
| Facilities | 0% | 0% | 0% | 0% | 3% | 0% | 0% | 0% | 0% | 0% | 1% |
| Other | 9% | 8% | 3% | 11% | 5% | 6% | 28% | 8% | 11% | 6% | 8% |

"In addition to being housed under Legal, we generally see privacy align under Risk or Compliance. It is important to integrate privacy into these other functions, so that it can be managed through the same mechanisms as other compliance programs, subject to KPIs and KRIs, as opposed to viewing it solely through the lens of legal requirements. Even if Legal is key to capture the huge changes observed globally in legal frameworks, to translate them in complex organizations and to develop fruitful discussions with regulators, proper management of privacy risk on the ground implies onboarding in due course other key players of risk management."

**Fabrice Naftalski**

EY Global Head of Data Protection Law Services,
Attorney at Law/Partner, France

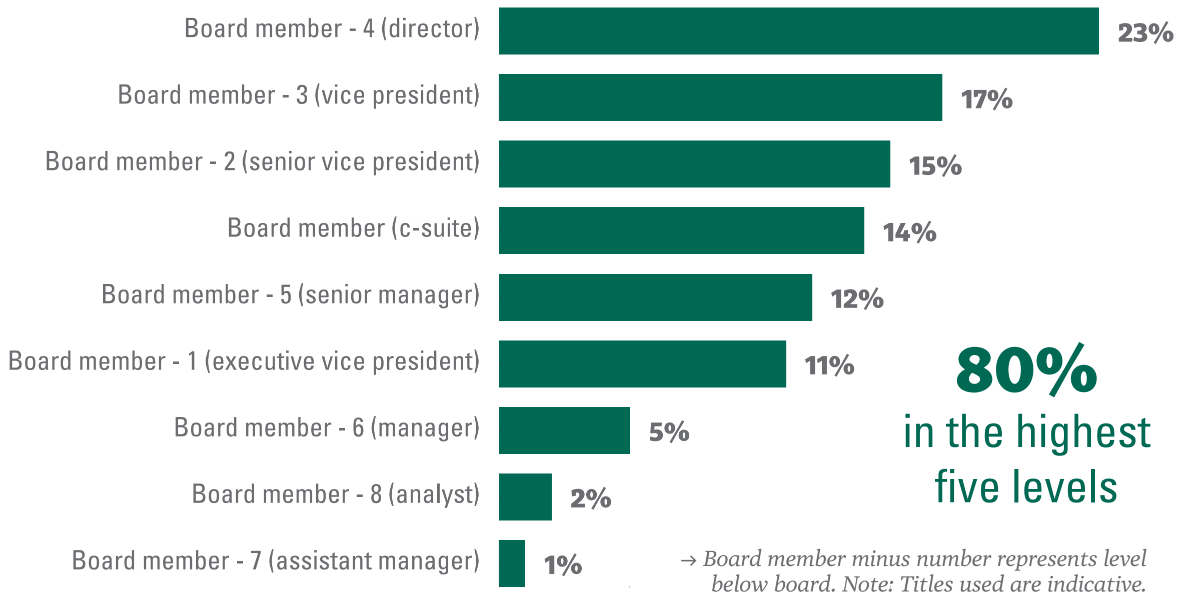
Nearly 80% of organizations indicated their most senior privacy employee was in the highest five levels of the organization.

## Up and up! — Privacy in the organization hierarchy

As organizations increasingly see privacy as a competitive advantage, while tapping into the promise of data, privacy professionals are climbing the corporate ladder.

In previous years, the governance survey analyzed the seniority of the privacy leader in comparison to other roles, e.g., 2021 — chief compliance officers, chief technology officer, chief information officer, chief information security officer. This year we examined the role relative to the board to try to situate the privacy leader's position within the organizational hierarchy and provide real clarity on the seniority level of the privacy leader.

Most senior privacy employee



→ *Board member minus number represents level below board. Note: Titles used are indicative.*

## Our results

- → Nearly 80% of organizations indicated the most senior privacy employee in an organization was in the highest five organizational levels. *(See table on next page).*
- → More than 50% of respondents indicated the most senior privacy employee in an organization was in the highest three organizational levels. *(See table on next page).*
- → Nearly 25% of respondents indicated the most senior privacy employee in an organization was in the highest two organizational levels. *(See table on next page).*
- → 39% of $60 billion revenue organizations have their most senior privacy employee either at the board level or one level down from the board, with 63% having it in the highest three levels! *(See table on page 23).*
- → The top three sectors with the highest percentage of most senior privacy employee in an organization serving at the board level were technology and telecommunications, business services, and legal. *(See table on next page).*
- → Asia is unique in reflecting that the most common (23%) senior-most privacy employee is a board member.
- → North America has, on average, less-senior privacy employees compared to other continents.

Just as we see the data privacy profession maturing along a parallel path with technology, we also see privacy officers becoming more senior as companies digitize.

**Cobun Zweifel-Keegan**
IAPP Managing Director, Washington, D.C.

**Most senior privacy employee by sector**

| | | SECTOR | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| MOST SENIOR PRIVACY EMPLOYEE | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| Board member - 4 (director) | 23% | **19%** | 15% | **26%** | **16%** | **29%** | **32%** | **23%** | 8% | **31%** | **28%** |
| Board member - 3 (vice president) | 17% | **25%** | **20%** | 8% | **16%** | **27%** | 8% | **21%** | 8% | 9% | **17%** |
| Board member - 2 (senior vice president) | 15% | **19%** | **22%** | 9% | 11% | **14%** | 4% | 15% | 11% | **19%** | **17%** |
| Board member (c-suite) | 14% | 7% | **18%** | **11%** | **24%** | 2% | **16%** | 13% | **34%** | 9% | 13% |
| Board member - 5 (senior manager) | 12% | 11% | 8% | **19%** | 11% | **14%** | **20%** | 8% | **13%** | **16%** | 10% |
| Board member - 1 (executive vice president) | 11% | 15% | 14% | 8% | 5% | 8% | 8% | **19%** | 11% | 6% | 8% |
| Board member - 6 (manager) | 5% | 3% | 0% | **11%** | 11% | 6% | 8% | 0% | **13%** | 3% | 4% |
| Board member - 8 (analyst) | 2% | 2% | 2% | 8% | 8% | 0% | 0% | 2% | 3% | 3% | 1% |
| Board member - 7 (assistant manager) | 1% | 0% | 1% | 0% | 0% | 0% | 4% | 0% | 0% | 3% | 1% |

→ *Board member minus number represents level below board. Note: Titles used are indicative.*

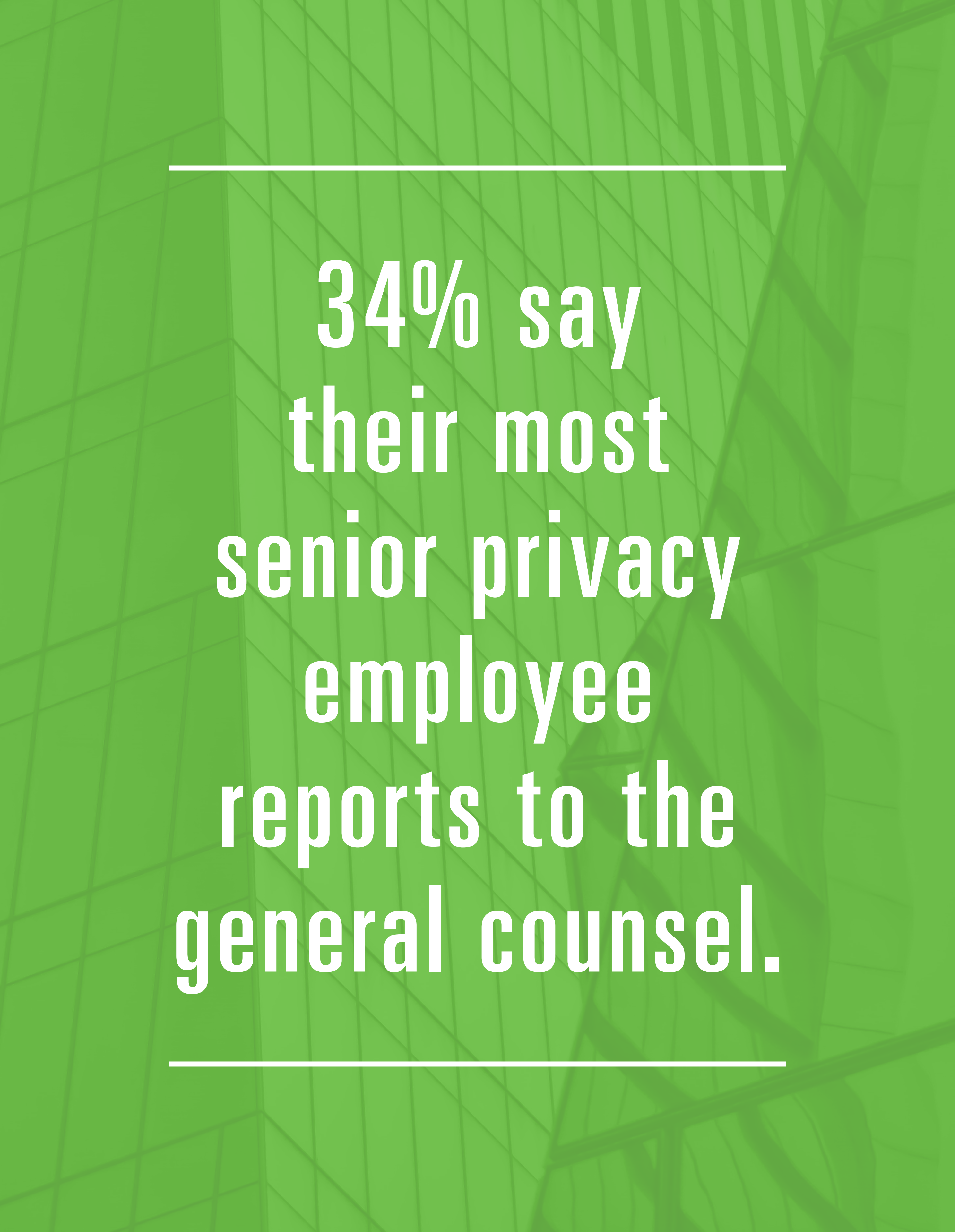
🟩 *Top 3 most senior*

## Most senior privacy employee by revenue

| | | REVENUE | | | | | |
|---|---|---|---|---|---|---|---|
| MOST SENIOR PRIVACY EMPLOYEE | Total | Under $100M | $101M-$999M | $1B-$8.9B | $9B-$19.9B | $20B-$59.9B | $60B+ |
| Board member - 4 (director) | 23% | 18% | 26% | 25% | 25% | 24% | 20% |
| Board member - 3 (vice president) | 17% | 11% | 15% | 21% | 32% | 19% | 13% |
| Board member - 2 (senior vice president) | 15% | 7% | 16% | 18% | 14% | 24% | 22% |
| Board member (c-suite) | 14% | 24% | 11% | 8% | 11% | 9% | 15% |
| Board member - 5 (senior manager) | 12% | 20% | 10% | 13% | 5% | 5% | 5% |
| Board member - 1 (executive vice president) | 11% | 8% | 12% | 10% | 6% | 12% | 24% |
| Board member - 6 (manager) | 5% | 6% | 6% | 3% | 5% | 7% | 0% |
| Board member - 8 (analyst) | 2% | 5% | 3% | 1% | 2% | 0% | 2% |
| Board member - 7 (assistant manager) | 1% | 1% | 1% | 2% | 0% | 0% | 0% |

→ *Board member minus number represents level below board. Note: Titles used are indicative.*

🟩 *Top 3 most senior*

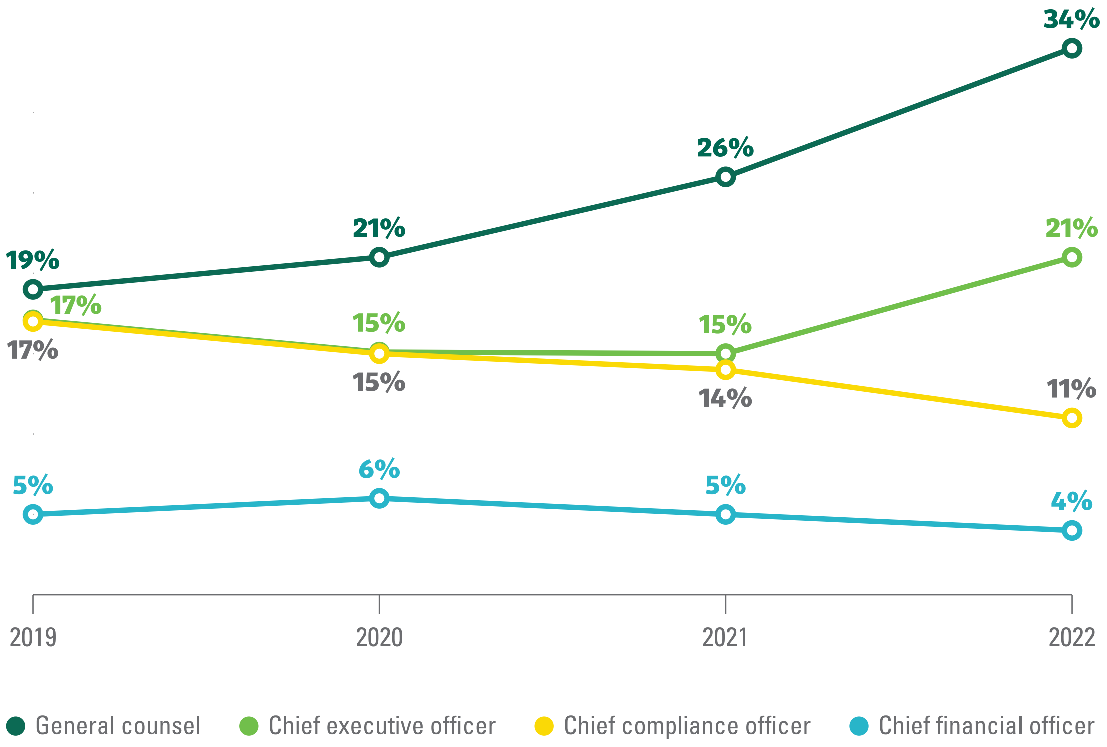


34% say their most senior privacy employee reports to the general counsel.

## Reporting structures: All the way to the top!

Regulations continue to amplify the need for privacy resources. Most explicitly, we see this in the EU General Data Protection Regulation Articles 37–39 requirement to “Designate a DPO,” China’s Personal Information Protection Law Article 52 requirements to “Appoint a personal information protection officer” and similar legal requirements across more than 50 countries.

**Reporting line trend**



Increasingly, we see the seniority of these roles integrated into new regulations. Examples include GDPR Article 38(3) stating, “the data protection officer shall directly report to the highest management level of the controller or the processor,” and Thailand’s Personal Data Protection Act Sections 41 and 42 indicating the need to “Report to chief executive…”

## But to whom does the most senior privacy employee report?

- → General counsel tops our survey for the ultimate reporting line of the most senior privacy individual, at 34%. This trend has grown since 2019. *(See graph on previous page).*
- → More than one-fifth of respondents have their most senior privacy individual report directly to the chief executive officer. *(See table to the right).*
- → Almost half of businesses in the technology and telecommunications sector have their most senior privacy individual report to general counsel. *(See table to the right).*
- → Chief financial officer is one of the top reporting lines for both the consumer goods, services, and retail sector and the manufacturing sector. *(See table to the right).*
- → CEO is the most common top reporting line in every continent besides North America, where it’s general counsel. This aligns with legal being the most popular department for the privacy function in North America. This could potentially be a reflection of the lack of U.S. legal requirements requiring that the privacy officer to report to the highest level of an organization.
- → Reporting to the chief compliance officer becomes more common as revenue gets higher.
- → The chief risk officer and chief operating officer are two of the top reporting lines for companies with less than $1B in revenue.

**Reporting line by sector**

| | | SECTOR | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| REPORTING LINE | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| General counsel/ head of legal | 34% | **33%** | **49%** | **25%** | **21%** | **39%** | **22%** | **35%** | **26%** | **41%** | **32%** |
| Chief executive officer | 21% | **16%** | **20%** | **30%** | **47%** | 6% | **18%** | **19%** | **37%** | **19%** | **21%** |
| Chief compliance officer | 11% | **19%** | **6%** | 0% | **11%** | **16%** | 4% | **23%** | 3% | 6% | **10%** |
| Chief information security officer | 6% | 4% | 4% | 4% | 3% | 8% | **6%** | 2% | **5%** | 3% | **10%** |
| Chief risk officer | 4% | 11% | 0% | 4% | 3% | 4% | 4% | 5% | 3% | 3% | 4% |
| Chief information officer | 4% | 4% | 4% | **9%** | 0% | 2% | **6%** | 3% | 3% | **9%** | 3% |
| Chief financial officer | 4% | 1% | 2% | 8% | 3% | **10%** | 4% | 0% | 0% | **9%** | 5% |
| Chief operating officer | 3% | 3% | 3% | 8% | 3% | 2% | 4% | 2% | 3% | 0% | 4% |
| Chief technology officer | 2% | 2% | 2% | 4% | 3% | 4% | 4% | 2% | 0% | 0% | 3% |
| Chief product officer | 1% | 2% | 0% | 2% | 0% | 0% | 0% | 0% | 0% | 0% | 1% |
| Chief people officer/ head of HR | 0% | 0% | 0% | 0% | 0% | 0% | 2% | 0% | 0% | 0% | 1% |
| Chief consumer officer | 0% | 0% | 0% | 0% | 0% | 0% | 2% | 0% | 0% | 0% | 1% |
| Other | 9% | 6% | 9% | 8% | 8% | 8% | 24% | 10% | 21% | 9% | 6% |

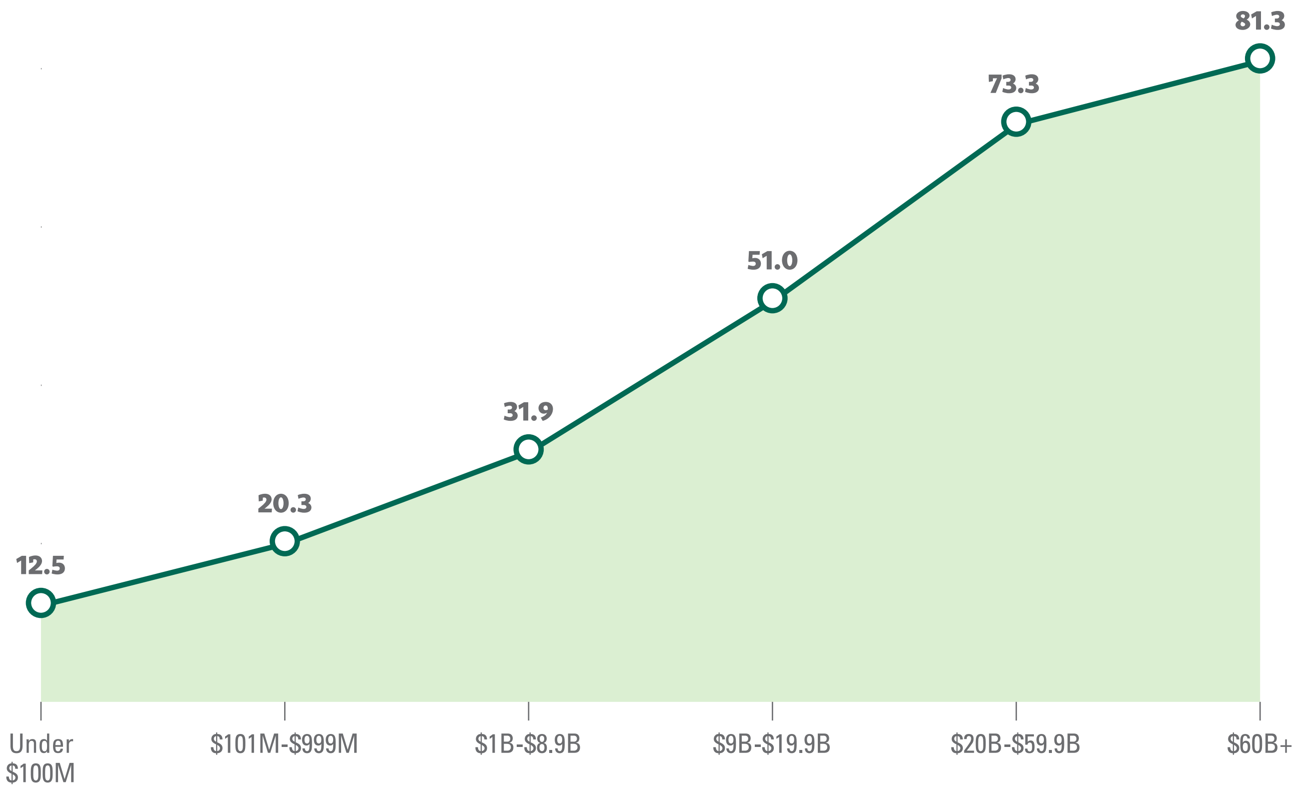
🟩 *Top 3 most senior*

As revenue increases, staff size increases steadily at approximately two to three staff members per billion U.S. dollars of revenue.

## Never enough: How big is a typical privacy function?

Organizations continue to strive for the right balance of privacy skills at the right scale to respond to ever-changing organizational needs, wants and demands. This is a real challenge as privacy is relatively young as an organizational function, growing and maturing with the rapid pace of technical and social change.

Total number of privacy staff by revenue



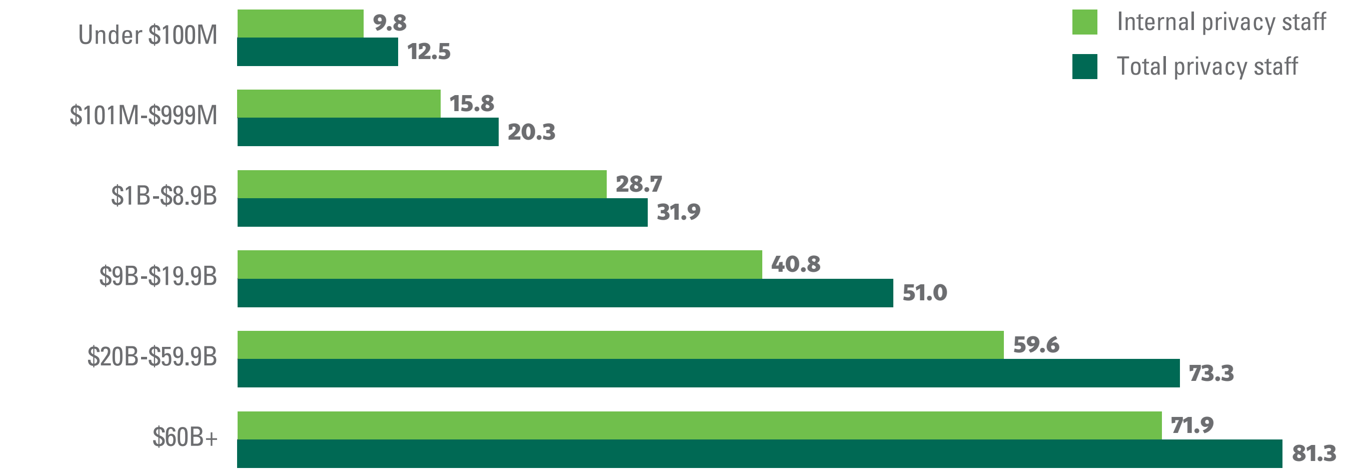
Privacy officers often ask themselves two questions: “How does the size and scale of my privacy function compare to others?” and, “Is it of reasonable size and scale compared to my organizational structure, industry, and footprint?”

In this year’s survey we tried to answer those questions and seek to dispel the myths surrounding the size and shapes of privacy functions.

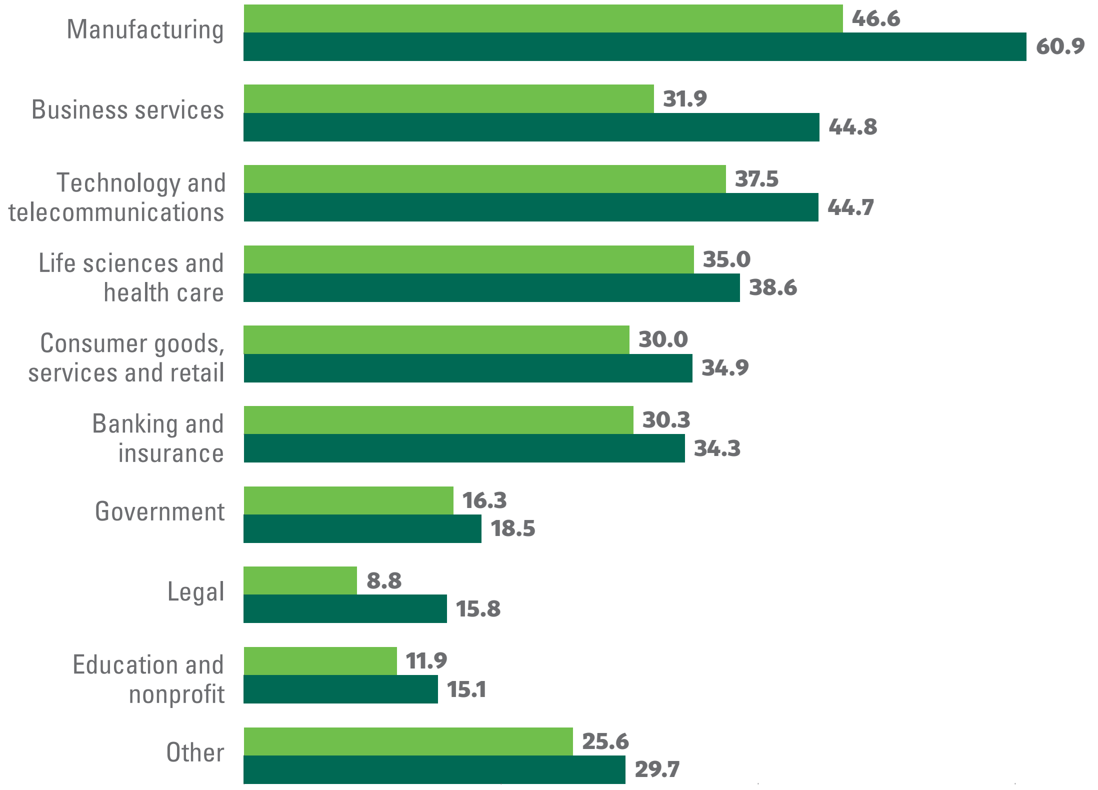
## Key findings

- Unsurprisingly, the total number of privacy staff in an organization is driven heavily by its revenue, with staff size increasing steadily as revenue increases. *(See graph to the right).*
- The ratio of privacy staff to revenue remains relatively consistent as revenue increases. In other words, privacy teams scale rather equally across organizations of all sizes, at approximately two to three staff members per billion U.S. dollars of revenue.

**Number of privacy staff by revenue**



**Number of privacy staff by sector**

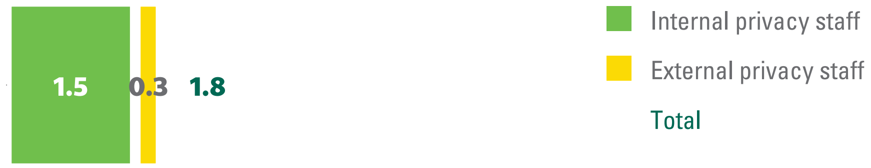


> **Due to the modest size of most privacy teams, rapidly increasing requirements and the need for multi-skilled practitioners, organizations are leveraging external professionals to assist with critical matters like data discovery, impact assessments and privacy incident remediation. Outside professionals often will have technologies and cross-disciplinary skills at their disposal that the organization doesn't have, experience with similar events or projects and importantly, they can offer insights into how your peer companies are managing similar issues.**
>
> **Charlie Offer**
> EY Oceana Cybersecurity Leader, Australia

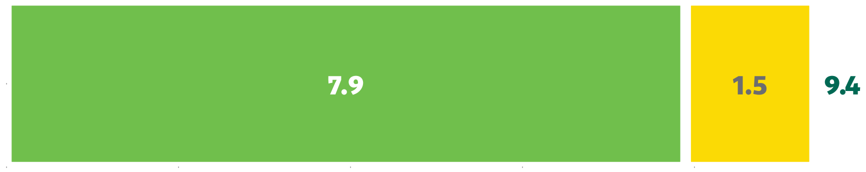
## Additional key findings

- → External privacy support is a key part of the resourcing model for organizations, meeting 10-20% of the privacy staffing requirements.
- → Companies have approximately two privacy employees for each country in which they operate, and approximately 10 for each continent. *(See graph below).*
- → Asia-based respondents have significantly more privacy staff than other continents, on average. More than half of these Asian firms also had over $1 billion in annual revenue, indicating they have the resources to support a larger privacy team.

**Ratio of privacy staff to number of countries in which organizations operate**



**Ratio of privacy staff to number of continents in which organizations operate**

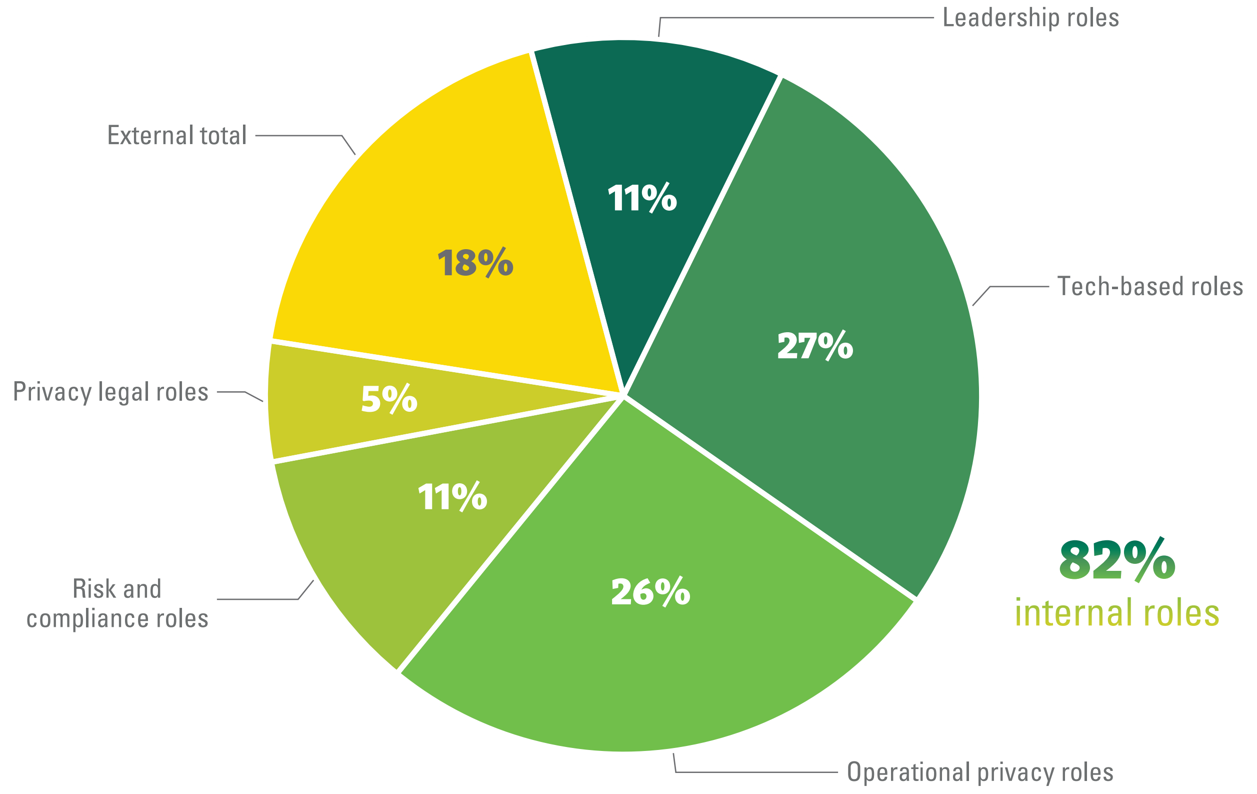


The government, legal, and education and nonprofit sectors rely on less privacy staff compared to other sectors.

## What's the perfect mix of privacy roles?

The privacy profession grew up in the legal realm. As a result, the occupation has long been associated with a high percentage of lawyers. As the privacy function has evolved and demanded new skillsets, we have seen an explosion of new roles, including in privacy engineering. What does the mix of privacy resources look like in a modern day privacy function?

**Average privacy staffing model**



In this year's survey we attempt to answer this question and provide insight into organizations' privacy staffing models. To do this we have defined the following roles:

→ **Privacy leadership roles**: Executives in charge of managing the privacy directive as a whole. Roles in this category may include accountable board members, chief privacy officers and regional privacy officers.

→ **Technology-based roles**: Includes engineers who build, review, and recommend changes to digital tools that implement privacy protections, as well as cyber professionals that design, develop, and deliver on security for personal data.

→ **Operational roles**: Individuals who are full time or are assigned a percentage of their time to support an aspect of privacy or perform duties related to privacy, such as the execution of subject rights requests.

→ **Privacy risk and compliance roles**: Encompasses the roles and responsibilities surrounding risk management, regulatory compliance, and the development of internal policies and audits that guide the organization towards its privacy goals.

→ **Privacy legal roles**: Legal professionals who provide support to organizations on the legal aspect of privacy standards and regulations.

→ **External roles**: Resources that support the privacy team but are not employees of the organization.

**Average privacy staffing model by revenue**

| | ROLES | Total | REVENUE | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Under $100M | $101M-$999M | $1B-$8.9B | $9B-$19.9B | $20B-$59.9B | $60B+ |
| Internal roles | Leadership roles | 3.8 | 1.7 | 2.5 | 3.1 | 5.8 | 7.4 | 11.6 |
| | Tech-based roles | 9.1 | 2.3 | 4.4 | 9.3 | 13.4 | 23.7 | 24.1 |
| | Operational privacy roles | 8.7 | 2.5 | 5.3 | 10.9 | 13.4 | 16.5 | 17.7 |
| | Risk and compliance roles | 3.7 | 1.7 | 2.2 | 3.0 | 5.0 | 8.1 | 10.8 |
| | Privacy legal roles | 1.8 | 0.8 | 1.1 | 1.8 | 2.0 | 3.4 | 5.2 |
| | **Internal total** | 27.1 | 9.0 | 15.5 | 28.1 | 39.6 | 59.1 | 69.4 |
| | **External total** | 6.1 | 3.5 | 4.8 | 3.8 | 11.4 | 14.2 | 11.9 |
| | **Total** | 33.2 | 12.5 | 20.3 | 31.9 | 51.0 | 73.3 | 81.3 |

## Key findings

→ Privacy organizations are leveraging an increasingly wide range of skillsets to help them deliver on their organizational objectives.

→ The largest reported internal privacy team was comprised of more than 400 people.

→ External privacy resources are generally leveraged by organizations across every sector and revenue bracket. The largest reported external privacy team had more than 150 people.

→ The number of privacy leadership roles are relatively consistent across revenue brackets until $9B, where the number almost doubles and continues an upward trend as revenue increases. *(See table to the left).*

→ Operational and compliance roles are more staffed than technology-based roles for companies with less than $20B in revenue. *(See table to the left).*

→ The manufacturing sector relies on about twice as many privacy legal staff compared to all other sectors. *(See table on next page).*

→ Technology-based roles are most common in the technology and telecommunications and the manufacturing sectors. *(See table on next page).*

→ The government, legal and education and nonprofit sectors rely on notably less privacy staff compared to other sectors. *(See table on previous page).*

**Average privacy staffing model by sector**

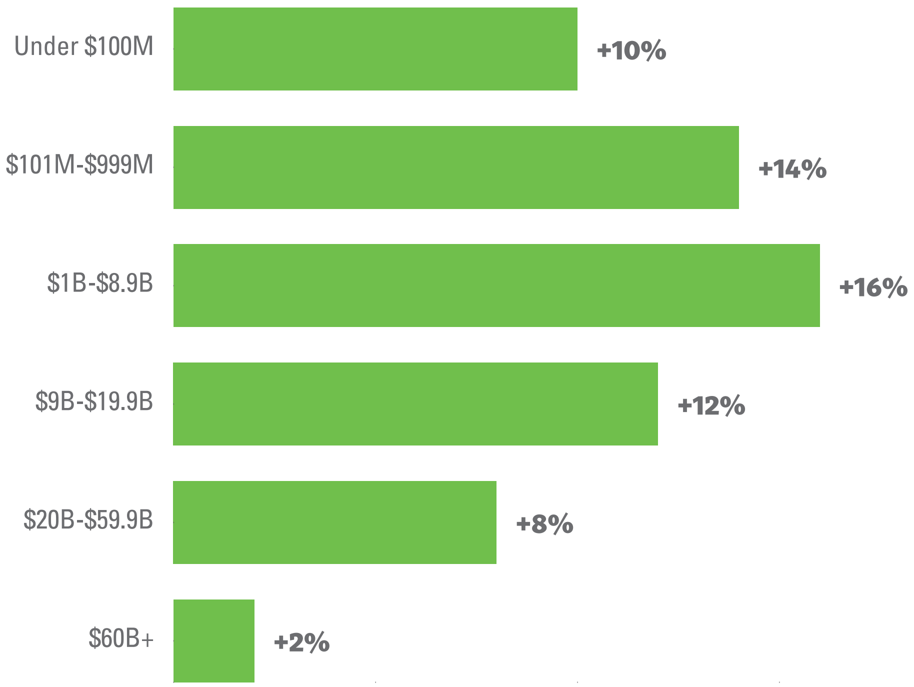
| | | | SECTOR | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ROLES | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| Internal roles | Leadership roles | 3.8 | 4.4 | 5.9 | 1.2 | 3.6 | 3.1 | 2.3 | 4.5 | 2.1 | 5.3 | 3.8 |
| | Tech-based roles | 9.1 | 9.7 | 14.3 | 4.8 | 12.3 | 9.1 | 3.6 | 9.9 | 1.0 | 15.6 | 8.2 |
| | Operational privacy roles | 8.7 | 9.0 | 10.6 | 3.4 | 8.9 | 11.8 | 5.5 | 13.3 | 2.6 | 13.8 | 7.6 |
| | Risk and compliance roles | 3.7 | 4.5 | 4.2 | 1.5 | 4.1 | 3.5 | 3.3 | 4.3 | 0.6 | 7.7 | 3.4 |
| | Privacy legal roles | 1.8 | 2.1 | 1.9 | 0.7 | 1.8 | 2.2 | 1.6 | 1.6 | 1.6 | 3.9 | 1.6 |
| | **Internal total** | 27.1 | 29.7 | 36.9 | 11.6 | 30.7 | 29.7 | 16.3 | 33.6 | 7.9 | 46.3 | 24.6 |
| | **External total** | 6.1 | 4.6 | 7.8 | 3.5 | 14.1 | 5.2 | 2.2 | 5.0 | 7.9 | 14.6 | 5.1 |
| | **Total** | 33.2 | 34.3 | 44.7 | 15.1 | 44.8 | 34.9 | 18.5 | 38.6 | 15.8 | 60.9 | 29.7 |

Firms with $60 billion or more in revenue had the greatest staff turnover.

## We need more expertise!

The composition of the privacy team has undoubtedly changed, but our survey also looked at the extent to which organizations' privacy teams had grown or shrunk over the last 12 months.

Average privacy team growth in the last 12 months by revenue



## Key results

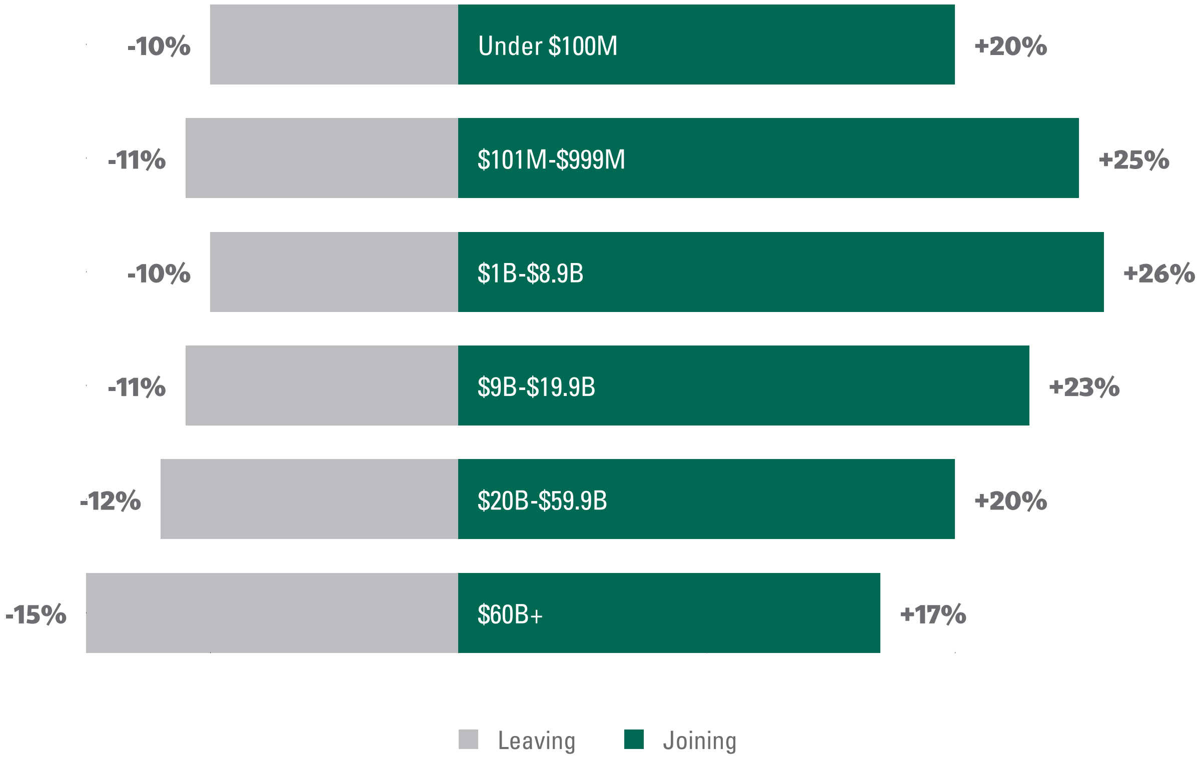
- → There was an average 12% increase in the size of privacy teams in the last 12 months. This represents thousands of individuals entering the privacy profession!
- → Firms with $60 billion or more in revenue had the greatest turnover. They saw the highest number of staff departures from privacy teams, resulting in the lowest overall growth, with only a 2% net positive turnover. *(See graph to the right).*

> Organizations, large and small, across all industries are struggling to identify, onboard, and retain employees with requisite skills to meet today's increasing data protection and privacy demands. The ideal candidates now need to understand privacy law, compliance, risk management, data governance and how to manage privacy operations at scale.

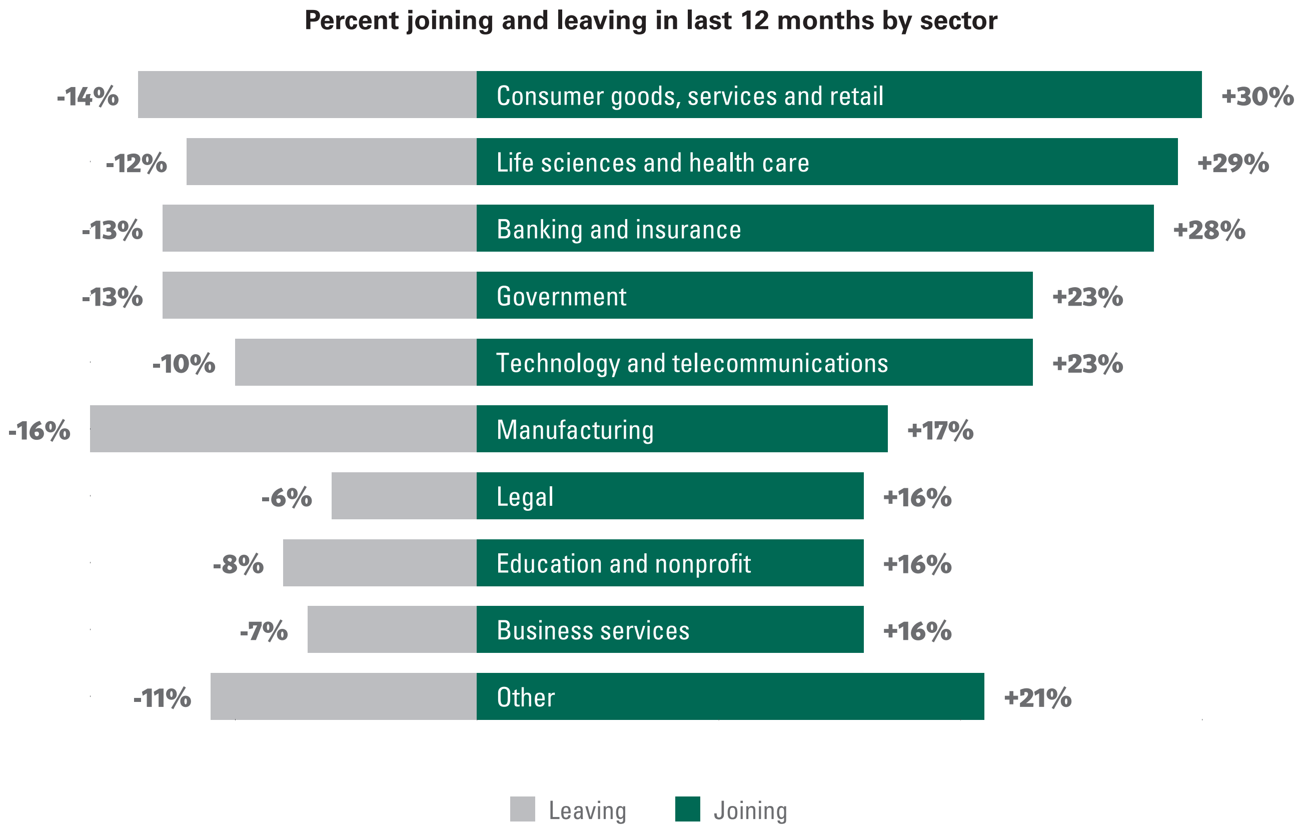
**Andy Ng**

EY EMEIA Data Protection & Privacy Consulting Leader, United Kingdom

**Percent joining and leaving in last 12 months by revenue**



> A 12% average increase in privacy headcount in organizations is a highly significant shift. We expect that this will continue to grow as new privacy regulations continue to emerge and privacy becomes a business imperative.
>
> **J. Trevor Hughes, CIPP**
> IAPP President and CEO



## Additional results

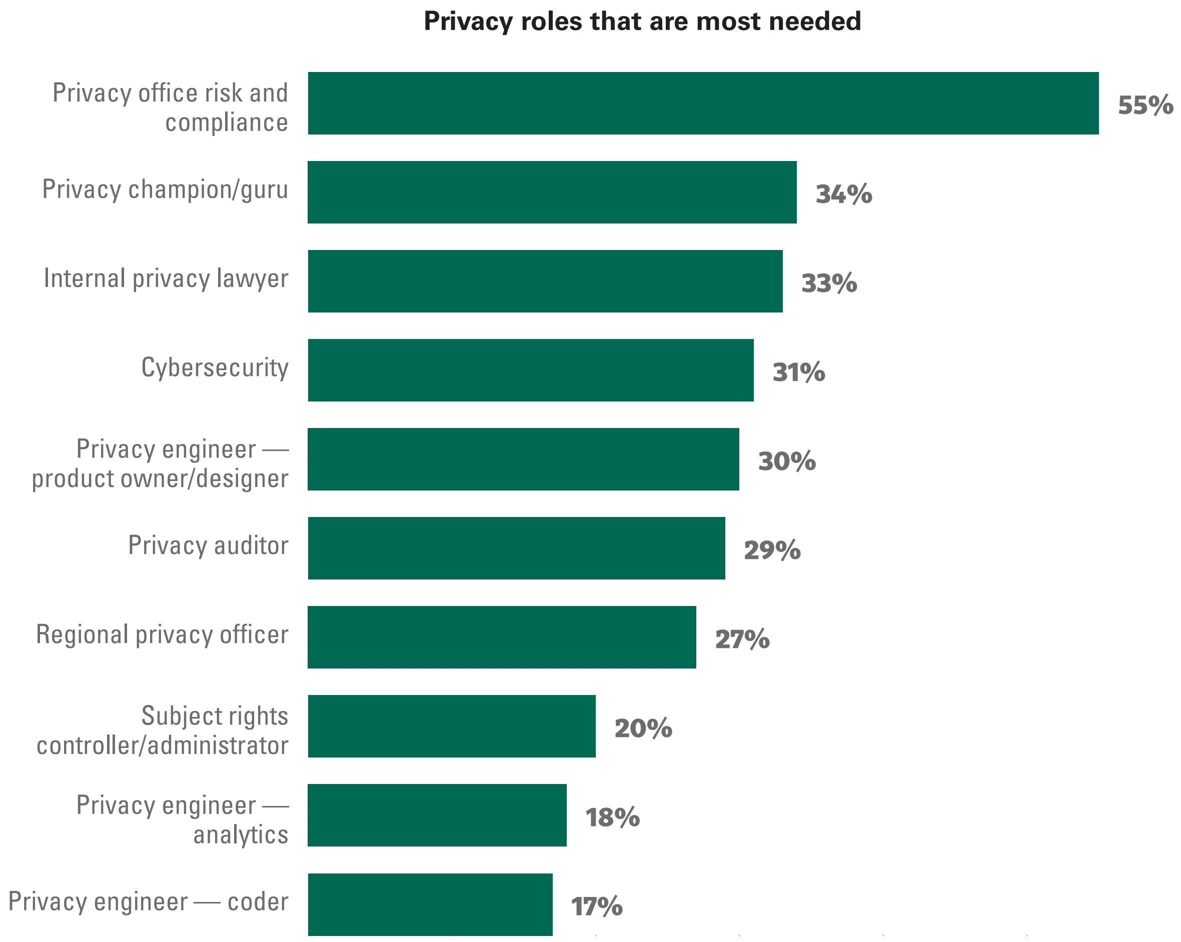
→ Industries across the board were adding privacy team members, with the top three sectors — consumer goods, services, and retail; life sciences and health care; and banking and insurance — increasing the size of their privacy teams by around 15% over the past 12 months. *(See graph above).*

→ From a geographic perspective, there were staff increases across the board. The lowest increase (7%) was in Europe, and the highest increase (18%) was outside North America, Europe and Asia.

55% of respondents indicated they need privacy risk and compliance expertise.

## Skills and expertise: Mind the gap!

The data overwhelmingly demonstrates the expansion of the privacy profession in recent years, both in volume and in talent, but what are the most in-demand skills and expertise? How are organizations shifting their privacy resources to meet their changing needs? What skills are helping them deliver on their short-, medium- and long-term privacy objectives?



## Our results

- → Privacy risk and compliance expertise is the most in-demand skill, with 55% of respondents indicating this need. *(See table to the right).*
- → Privacy risk and compliance demand is especially evident in banking and insurance, government, and health care, where more than three-fifths of organizations reported needing this skillset. *(See table on next page).*
- → Regionally, 66% of Asia-based respondents indicated that compliance expertise is needed most. *(See table to the right).*
- → Roles which make up the greatest portion of privacy teams — privacy champions/gurus, privacy lawyers, and privacy office and compliance specialists — are also in highest demand. *(See table to the right).*

**Privacy roles that are most needed by continent**

| | | CONTINENT | | | |
|---|---|---|---|---|---|
| PRIVACY ROLES | Total | North America | Europe | Asia | Other |
| Privacy office risk and compliance | 55% | 55% | 51% | 66% | 59% |
| Privacy champion/guru | 34% | 35% | 32% | 39% | 31% |
| Internal privacy lawyer | 33% | 30% | 35% | 32% | 56% |
| Cybersecurity | 31% | 29% | 33% | 32% | 28% |
| Privacy engineer — product owner/designer | 30% | 33% | 25% | 41% | 19% |
| Privacy auditor | 29% | 29% | 32% | 30% | 19% |
| Regional privacy officer | 27% | 22% | 33% | 34% | 25% |
| Subject rights controller/administrator | 20% | 19% | 20% | 27% | 16% |
| Privacy engineer — analytics | 18% | 20% | 12% | 32% | 9% |
| Privacy engineer — coder | 17% | 19% | 11% | 25% | 6% |

*Top 3 most lacking*

**Privacy roles that are most needed by sector**

| | | SECTOR | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PRIVACY ROLES | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| Privacy office risk and compliance | 55% | 62% | 45% | 58% | 42% | 59% | 66% | 63% | 42% | 34% | 56% |
| Privacy champion/guru | 34% | 30% | 30% | 43% | 29% | 49% | 34% | 37% | 11% | 41% | 37% |
| Internal privacy lawyer | 33% | 34% | 26% | 25% | 29% | 31% | 34% | 37% | 50% | 41% | 33% |
| Cybersecurity | 31% | 26% | 29% | 36% | 32% | 16% | 36% | 37% | 24% | 38% | 33% |
| Privacy engineer — product owner/designer | 30% | 34% | 33% | 25% | 16% | 37% | 26% | 31% | 3% | 34% | 36% |
| Privacy auditor | 29% | 21% | 33% | 40% | 32% | 24% | 30% | 29% | 16% | 25% | 33% |
| Regional privacy officer | 27% | 24% | 28% | 11% | 34% | 31% | 10% | 24% | 11% | 56% | 33% |
| Subject rights controller/administrator | 20% | 19% | 14% | 19% | 18% | 24% | 20% | 19% | 11% | 25% | 23% |
| Privacy engineer — analytics | 18% | 17% | 18% | 15% | 5% | 31% | 8% | 19% | 3% | 13% | 26% |
| Privacy engineer — coder | 17% | 12% | 20% | 9% | 8% | 20% | 8% | 19% | 5% | 13% | 25% |

*Top 3 most lacking*

> “Our CIPM training is aimed at supporting Privacy Professionals so that they understand how to implement privacy in day-to-day operations, and Privacy Risk and Compliance concepts are a core part of this. This year’s survey results support the trend of a growing demand for CIPM certification.”

**Marla Berry**
IAPP Training Director

## Additional results

→ Companies with higher revenues are more likely to need privacy risk and compliance expertise compared to those with lower revenues. Higher-revenue companies are also more in need of regional privacy officers.
*(See table on next page).*

→ Roughly 20-30% of respondents indicated that privacy engineering skills (i.e., coder/analytics/designer roles) are needed most. *(See table on previous page).*

→ After privacy risk and compliance expertise, the most needed skills varied by sector:

- For example, more than half of manufacturing organizations and 34% of business services companies noted they need a regional privacy officer. However, this role is in lower demand elsewhere. *(See table on previous page).*

- While privacy auditors ranked sixth most needed overall, they are a top three need for the technology and telecommunications, education and nonprofit, and business services sectors. *(See table on previous page).*

**"Organizations across every industry are adopting new technologies to gain competitive advantage and grow market share. The pace and scope of adoption of these new technologies is reshaping every facet of business. Embedded in — or a focal point of — these changes is the use of personal information, which must be contextualized to the technology and how it operates. Each organization, will need practitioners that can not only effectively integrate general requirements and the unique obligations of a given industry, but can define a course forward that is flexible and scalable to meet the future of Web 3.0 and the metaverse."**

**Reese Solberg**

EY US Privacy Leader, United States of America

**Privacy roles that are most needed by revenue**

| PRIVACY ROLES | Total | REVENUE | | | | | |
|---|---|---|---|---|---|---|---|
| | | Under $100M | $101M-$999M | $1B-$8.9B | $9B-$19.9B | $20B-$59.9B | $60B+ |
| Privacy office risk and compliance | 55% | 🟩 49% | 🟩 52% | 🟩 56% | 🟩 52% | 🟩 67% | 🟩 65% |
| Privacy champion/guru | 34% | 26% | 🟩 35% | 🟩 40% | 🟩 44% | 31% | 29% |
| Internal privacy lawyer | 33% | 🟩 29% | 29% | 33% | 35% | 🟩 41% | 🟩 45% |
| Cybersecurity | 31% | 🟩 34% | 31% | 25% | 35% | 36% | 27% |
| Privacy engineer — product owner/designer | 30% | 24% | 🟩 32% | 33% | 30% | 36% | 27% |
| Privacy auditor | 29% | 23% | 28% | 33% | 🟩 37% | 31% | 31% |
| Regional privacy officer | 27% | 15% | 21% | 🟩 34% | 33% | 🟩 40% | 🟩 36% |
| Subject rights controller/administrator | 20% | 14% | 16% | 26% | 17% | 17% | 33% |
| Privacy engineer — analytics | 18% | 11% | 16% | 21% | 22% | 28% | 20% |
| Privacy engineer — coder | 17% | 13% | 15% | 19% | 21% | 17% | 22% |

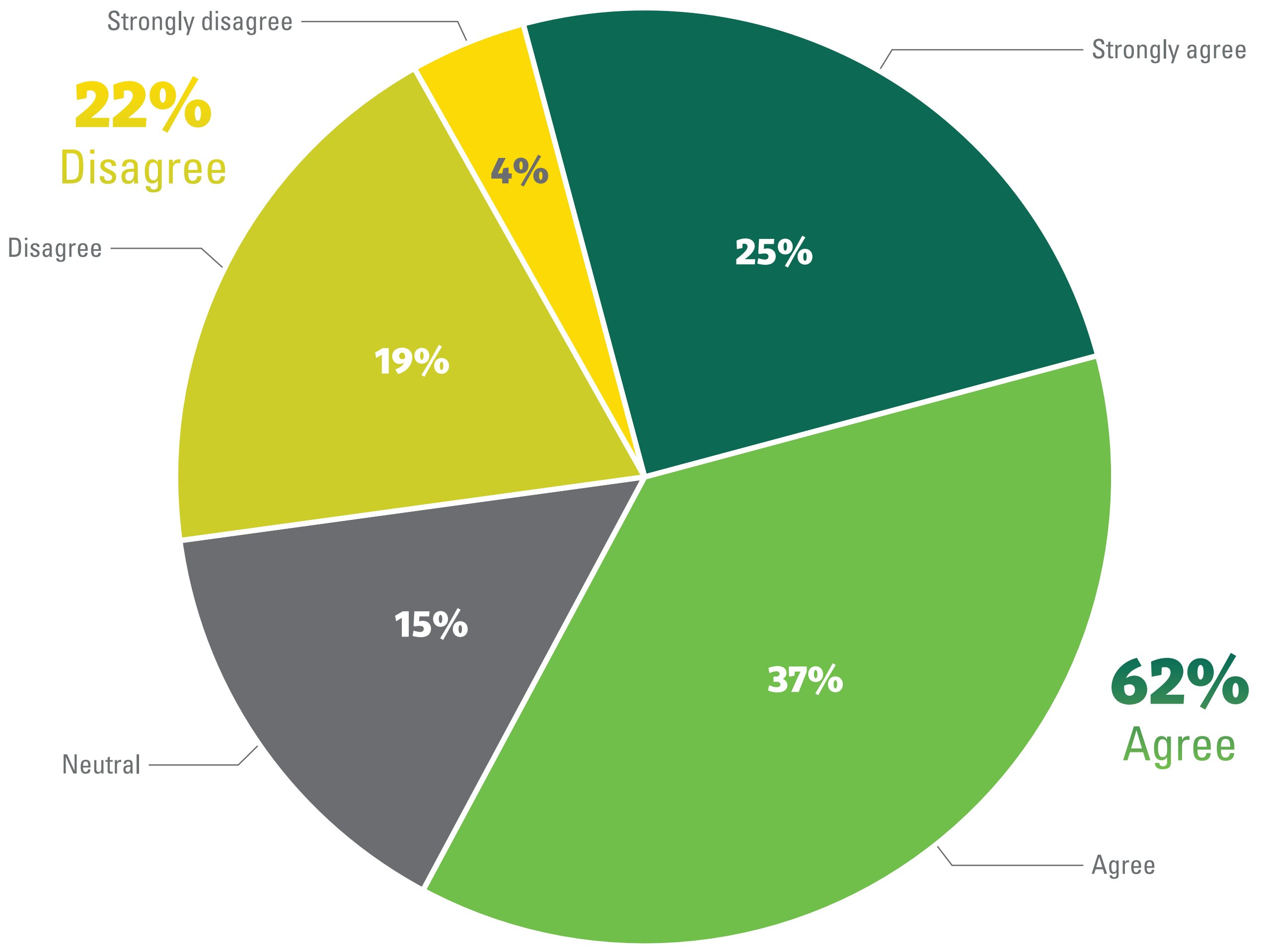
🟩 *Top 3 most lacking*

62% of organizations agree that the limited availability of privacy resources impacts their ability to deliver on their objectives.

## Meeting the need for expertise

There are a wide range of privacy skills that are in demand in the marketplace today. Not only is this privacy skills gap a long-standing challenge, but it also seems to be growing at a quickening pace.

Lack of resources limits ability to deliver on objectives



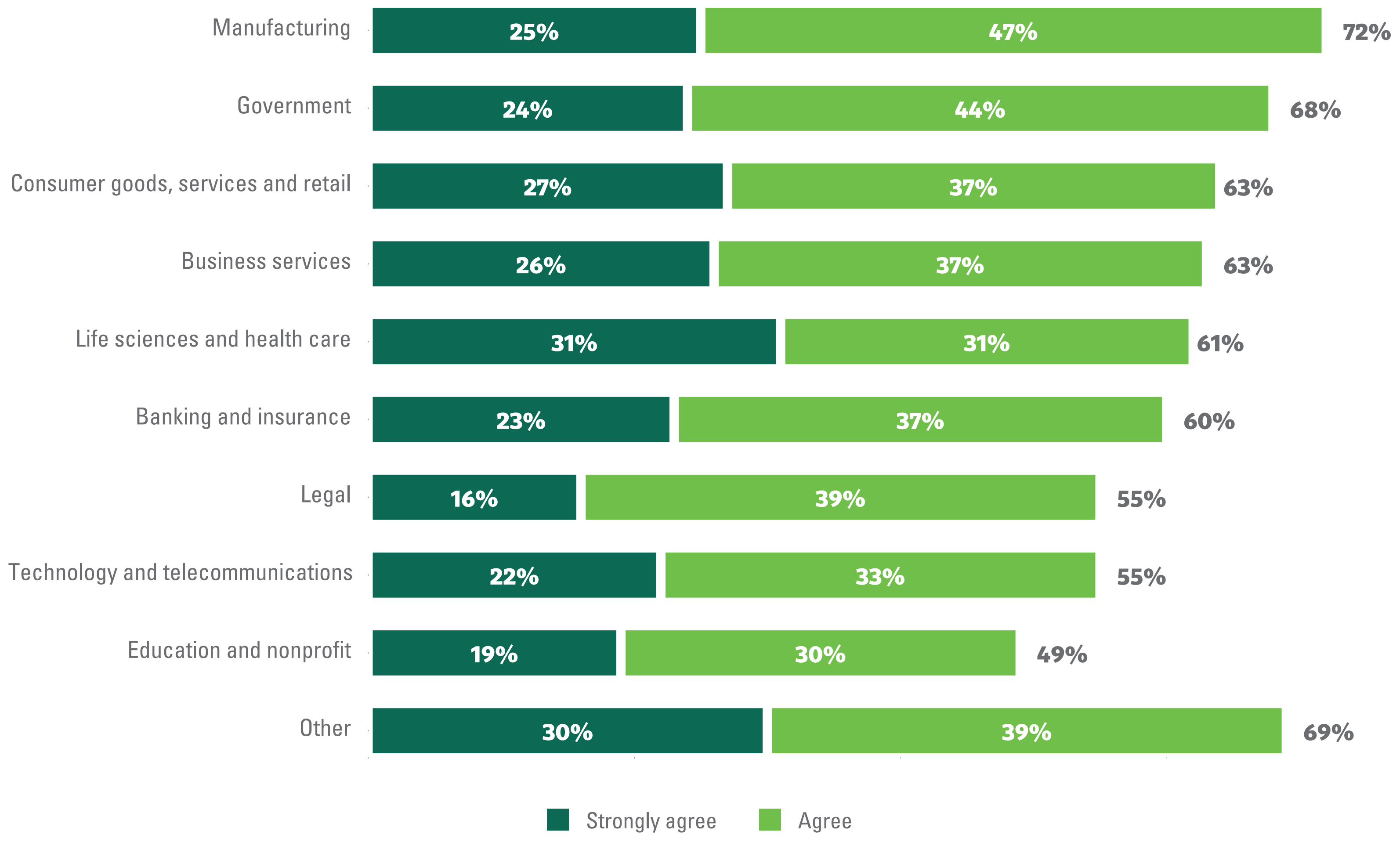
For privacy professionals, it truly has been a land of opportunity with the abundance of available roles. Job reports have indicated continuous growth in the number of available privacy roles, with 2020 and 2021 showing as much as a 30% increase.

The trend doesn't stop there. We have seen an increase in demand for privacy professionals across the world. This trend is also present in IAPP membership numbers, which have increased by almost 20% per year since 2017.

With 2022 as the year where over 50% of the world's population and over 80% of the world's GDP are now covered by privacy laws, there is likely to be further strain on the already limited privacy resources. Should a U.S. privacy law be adopted, this challenge could be exacerbated further due to demand for privacy resources from both U.S. businesses and large multinationals with global operations.

Though privacy has similar challenges to cybersecurity in this regard, cybersecurity is ahead of the privacy profession in seeking to build a talent pipeline from the classroom to the office. The IAPP has recognized this and seeks to further support the recruitment of more privacy professionals into the marketplace. For starters, the IAPP has created a fund to support students who are identified by their professors as future leaders in the field of privacy or data protection in a program we call the Westin Scholar Award.

Lack of resources limits ability to deliver on objectives by sector



## The results of our survey underline the extent of these challenges

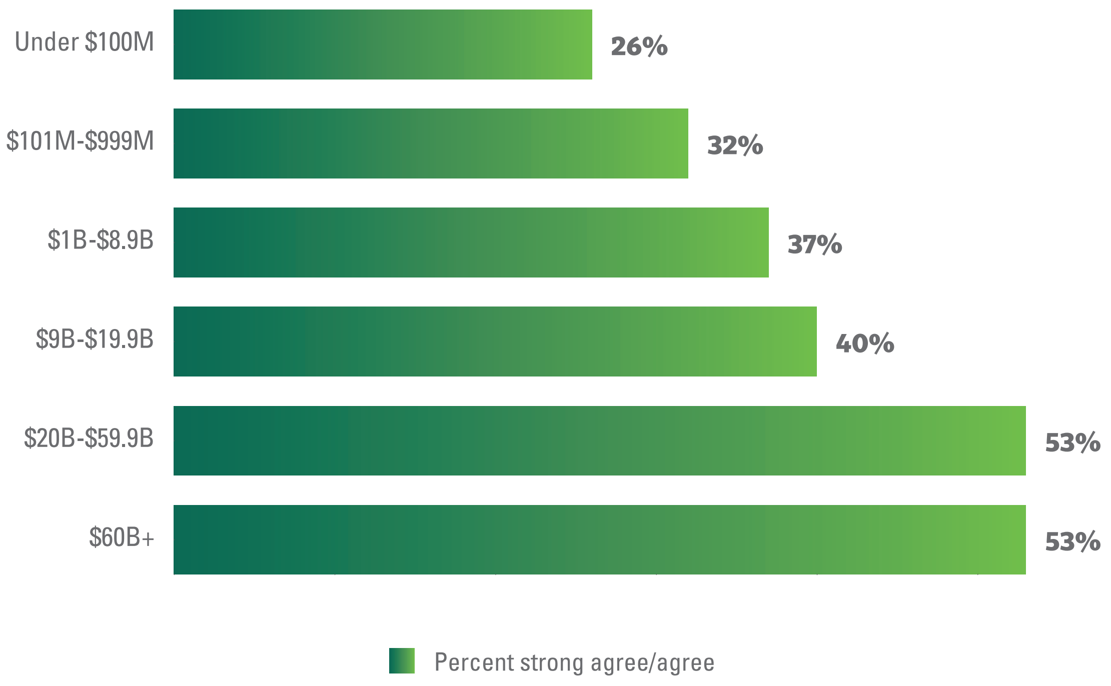
- → 62% of organizations across the world agree that the limited availability of privacy resources impacts their ability to deliver on their objectives.
- → Nearly 80% of Asia-based respondents agree that the limited availability of privacy resources impacts their ability to deliver on their objectives.
- → Even in Europe, where the GDPR has been in place for five years, 50% of respondents agree that the limited availably of privacy resources impacts their ability to deliver on their objectives.
- → While there was around a 20% difference in agreement from the highest (72%) to lowest (49%) that the limited availability of privacy resources impacts ability to deliver on objectives, by industry, every sector is facing similar challenges. *(See graph to the left).*

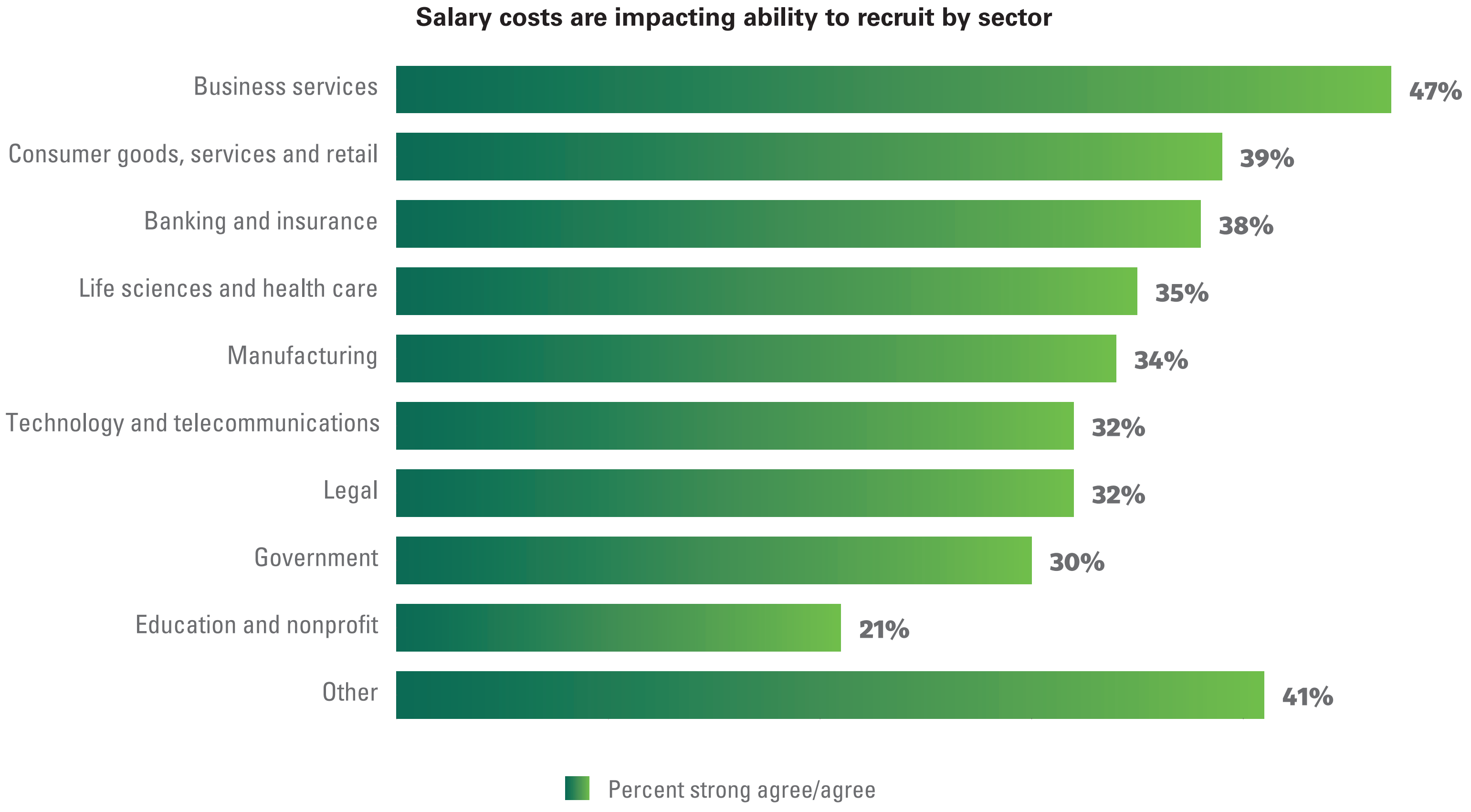
Firms with higher revenues indicated they have more difficulty recruiting employees due to salary costs.

## Growing salaries: Checks and challenges on the profession

Market economics are at play in the privacy marketplace, and we saw this play out in our 2021 Salary Survey where results indicated that 6 in 10 privacy professionals received an average of $21,000 in additional compensation since 2019.

Salary costs are impacting ability to recruit by revenue





## As a follow-up, we wanted to understand the extent to which this dynamic was impacting privacy organizations' ability to recruit

→ Roughly one-third (36%) indicated salary costs are impacting their ability to recruit.

→ Looking at both ends of the industry spectrum, nearly half (45%) of business service organizations are finding salary costs a significant challenge, compared to around one-fifth (21%) of education and nonprofit organizations. *(See graph above).*

→ In Asia, nearly half of respondents (45%) indicated salary costs are impacting their ability to recruit, compared to 34% in North America.

→ Firms with higher revenues generally indicated they have more difficultly recruiting employees due to salary costs. *(See graph on previous page).*

Mean annual privacy budgets are highest in Asia and North America, which both eclipse $2 million.

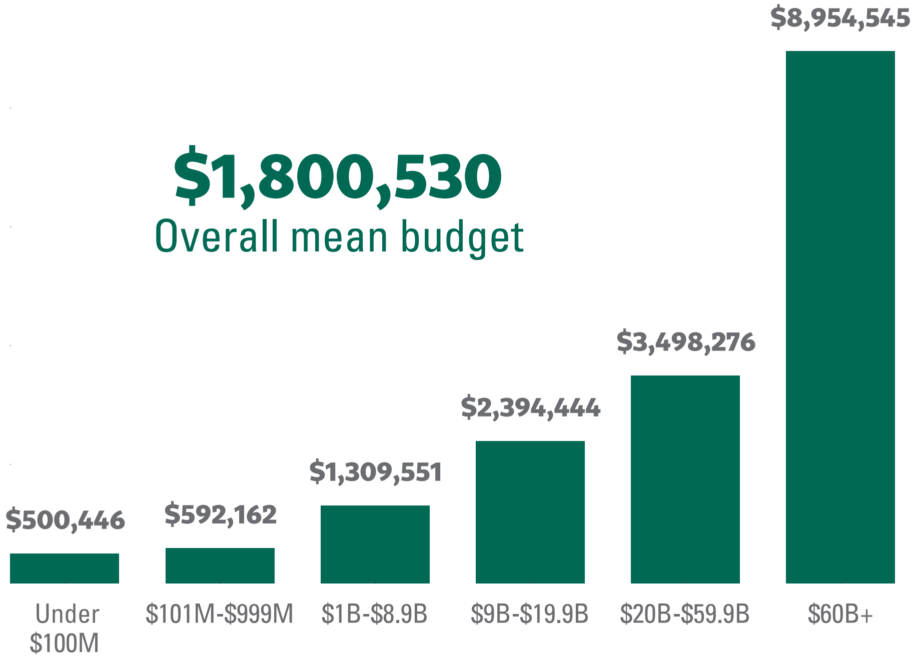
## Organizational investment in privacy continues

Privacy budgets are always a hot topic, as privacy professionals battle to understand if their resources are in line with their peers.

### How much is enough?

- → The mean annual privacy budget for 2022 is $1,800,530.
- → Approximately 6% of respondents indicated they have privacy budgets over $5 million. Approximately 1% indicated they have privacy budgets of over $50 million.

Mean annual privacy budget by revenue



### Annual privacy budget by sector

|  |  | SECTOR |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|
| BUDGET | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| **Average** | $1,800,530 | $1,935,648 | $2,392,268 | $1,214,623 | $1,468,421 | $1,930,102 | $1,443,500 | $1,781,855 | $390,132 | $2,869,531 | $1,821,250 |
| $0K-$99.9K | 25% | 21% | 22% | 36% | 37% | 18% | 30% | 15% | 58% | 22% | 21% |
| $100K-$249.9K | 21% | 17% | 12% | 30% | 21% | 24% | 24% | 15% | 26% | 28% | 24% |
| $250K-$499K | 15% | 17% | 8% | 17% | 16% | 14% | 14% | 19% | 8% | 19% | 16% |
| $500K-$999K | 11% | 17% | 14% | 11% | 5% | 8% | 16% | 3% | 5% | 3% | 10% |
| $1M-$1.99M | 13% | 10% | 23% | 4% | 5% | 6% | 12% | 26% | 0% | 9% | 16% |
| $2M+ | 15% | 19% | 21% | 2% | 16% | 29% | 4% | 23% | 3% | 19% | 14% |

## Additional findings

- → 61% of companies have an annual privacy budget less than $500,000. 66% of the education and nonprofit sector budgets less than $250,000. 58% of the legal sector budgets less than $100,000. *(See table on previous page).*
- → Average budgets are highest in Asia and North America, which both eclipse $2 million.
- → Both the technology and telecommunications and manufacturing sectors have mean annual privacy budgets of over $2 million whereas the legal sector's annual privacy budget is less than a quarter of that, at $390,132. *(See table on previous page).*
- → The life sciences and health care sector has the highest number of organizations with privacy budgets of at least $1 million, at 49%. *(See table on previous page).*
- → Almost half of companies with at least $20 billion in revenue have privacy budgets north of $2 million. *(See table on next page).*

> The continued investment in privacy shows that organizations across sectors increasingly see privacy as a key area that needs the right levels of support and attention.

**Isabelle Roccia**
Managing Director, IAPP Europe

### Annual privacy budget by revenue

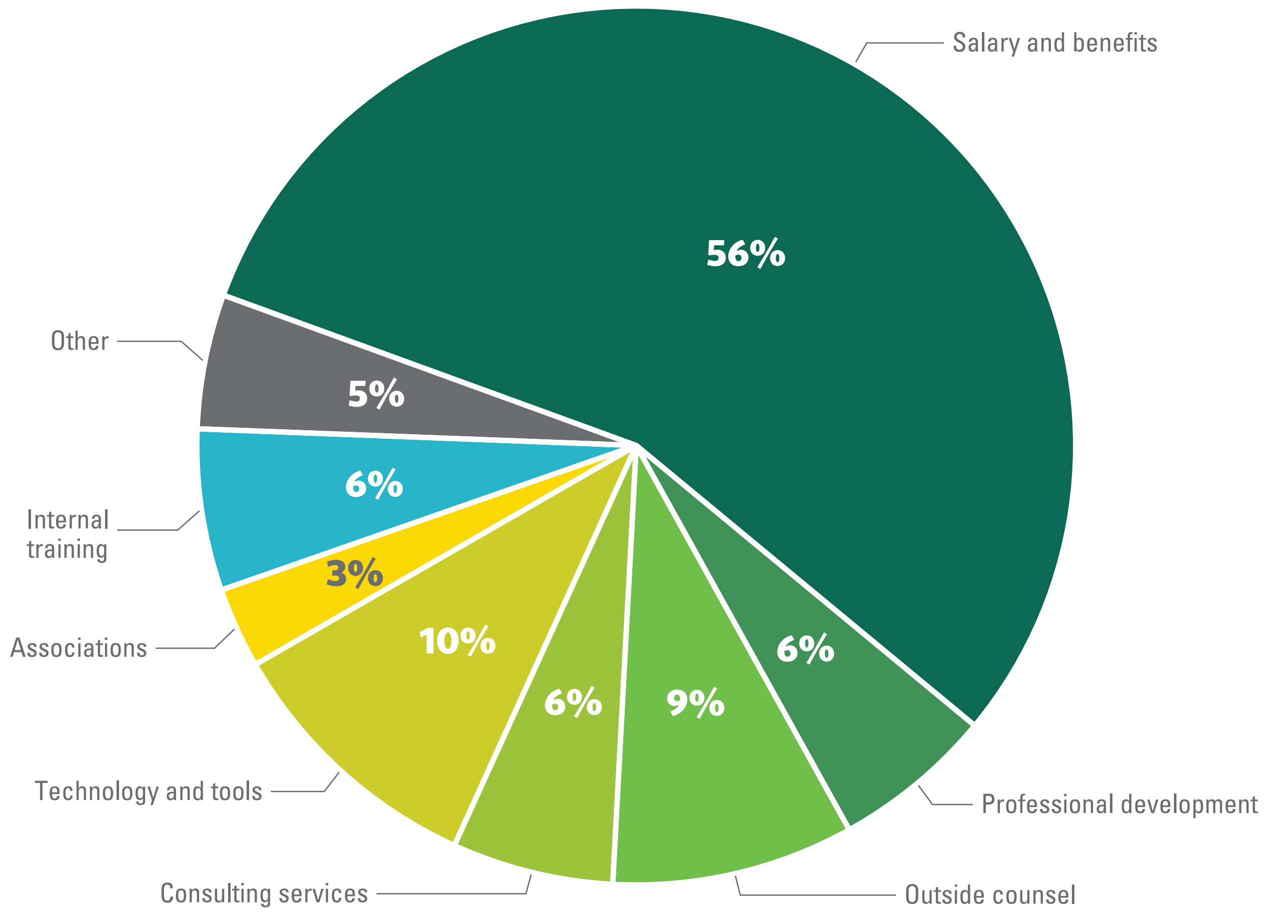
| | | REVENUE | | | | | |
|---|---|---|---|---|---|---|---|
| BUDGET | Total | Under $100M | $101M-$999M | $1B-$8.9B | $9B-$19.9B | $20B-$59.9B | $60B+ |
| **Average** | $1,800,530 | $500,446 | $592,162 | $1,309,551 | $2,394,444 | $3,498,276 | $8,954,545 |
| $0K-$99.9K | 25% | 54% | 22% | 15% | 14% | 7% | 11% |
| $100K-$249.9K | 21% | 27% | 28% | 16% | 11% | 16% | 13% |
| $250K-$499K | 15% | 10% | 22% | 19% | 8% | 9% | 5% |
| $500K-$999K | 11% | 5% | 10% | 16% | 17% | 9% | 4% |
| $1M-$1.99M | 13% | 2% | 12% | 20% | 24% | 12% | 18% |
| $2M+ | 15% | 1% | 6% | 14% | 25% | 48% | 49% |

Over half of the average firm's spending allocation goes directly to salary and benefits.

## How is it all spent?

From large scale software to awareness activities, a privacy office is never short of ways to spend its budgets. Competing priorities over what are often quite limited budgets can provide a challenge, so we looked at how organizations are making use of these resources.

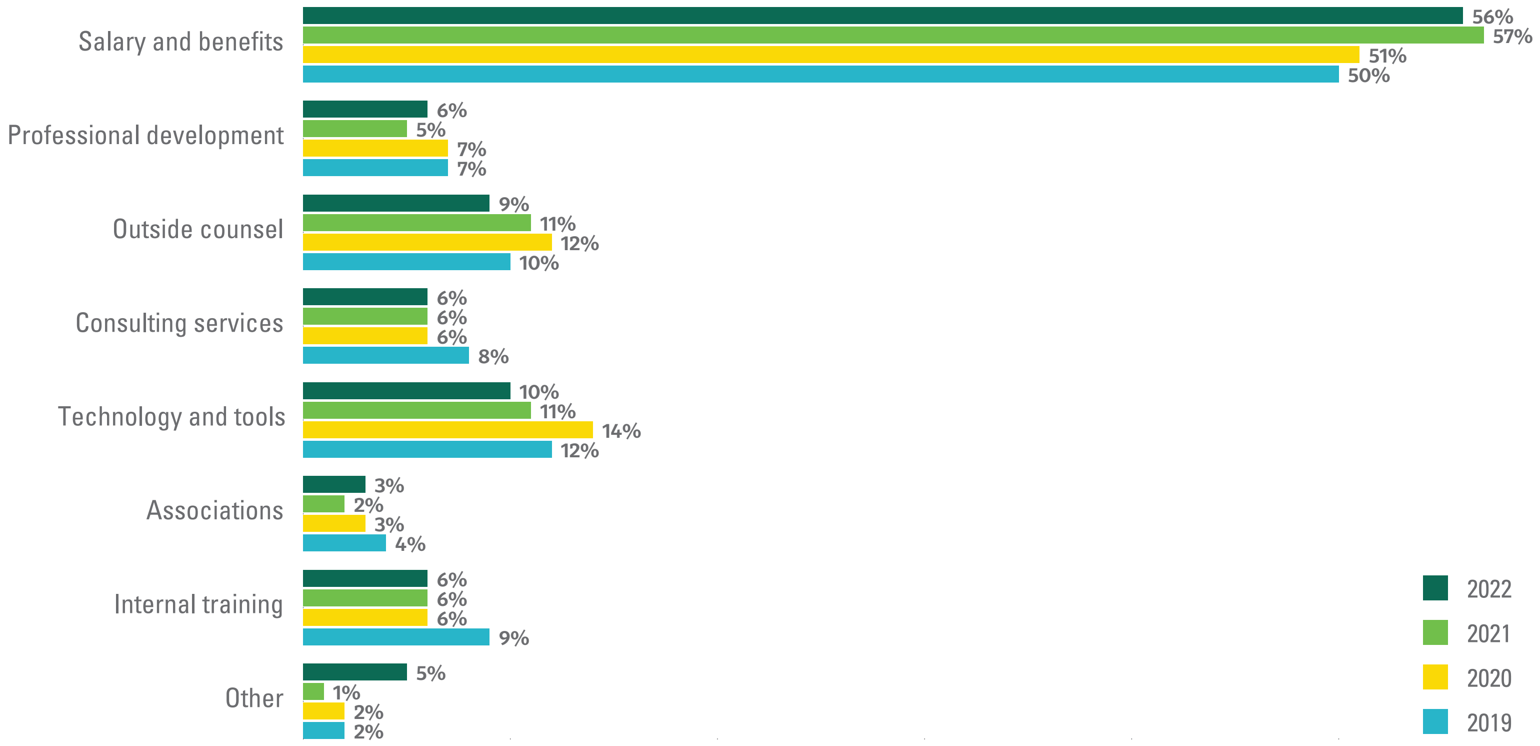
2022 privacy spending allocation



## Our findings

- → Our analysis has shown a reasonably consistent mix of privacy office spending since 2019. *(See graph below).*
- → Over half of the average firm's spending allocation goes directly to salary and benefits. This trend has been consistent since 2019. *(See graph below).*
- → Perhaps due to lower in-house privacy staff spending, Asia-based organizations dedicate approximately double what other continents do to consulting services (13% vs. approximately 6%).
- → The education and nonprofit sector allocates the most to salary and benefits (65%), whereas legal and manufacturing dedicate the least (50%). Otherwise, allocation across industry sectors is reasonably consistent. *(See table on next page).*
- → Privacy spending allocation is similar across companies in the same revenue brackets.
- → Asia is the only continent where companies on average allocate less than 50% of their privacy budget to salary and benefits.

**Privacy spending allocation trend**



> As data driven organizations recognize the competitive advantages and growth opportunities that come with strengthening digital trust, there is a shift in the privacy team's strategic value. The return on privacy team investment expands past cost avoidance (fines, litigation expense) and is now measured in impact on brand equity. Much like security team budgets have increased significantly, organizations are recognizing the need to invest in people, processes, technology, and data to manage their privacy programs optimally.

**John Drake**

Chief Product Strategist IAPP

**Privacy spending allocation by sector**

| | | SECTOR | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PRIVACY SPENDING ALLOCATION | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| Salary and benefits | 56% | 59% | 54% | 65% | 53% | 54% | 63% | 58% | 50% | 50% | 53% |
| Technology and tools | 10% | 11% | 11% | 10% | 9% | 12% | 8% | 10% | 7% | 10% | 11% |
| Outside counsel | 9% | 8% | 10% | 7% | 9% | 14% | 4% | 10% | 3% | 15% | 10% |
| Consulting services | 6% | 6% | 6% | 4% | 4% | 6% | 6% | 5% | 6% | 6% | 7% |
| Internal training | 6% | 5% | 7% | 4% | 8% | 4% | 5% | 3% | 9% | 4% | 6% |
| Professional development | 6% | 5% | 5% | 5% | 6% | 4% | 8% | 6% | 10% | 4% | 5% |
| Associations | 3% | 2% | 3% | 2% | 3% | 2% | 2% | 2% | 4% | 2% | 3% |
| Other | 5% | 3% | 3% | 3% | 8% | 4% | 5% | 5% | 12% | 8% | 4% |

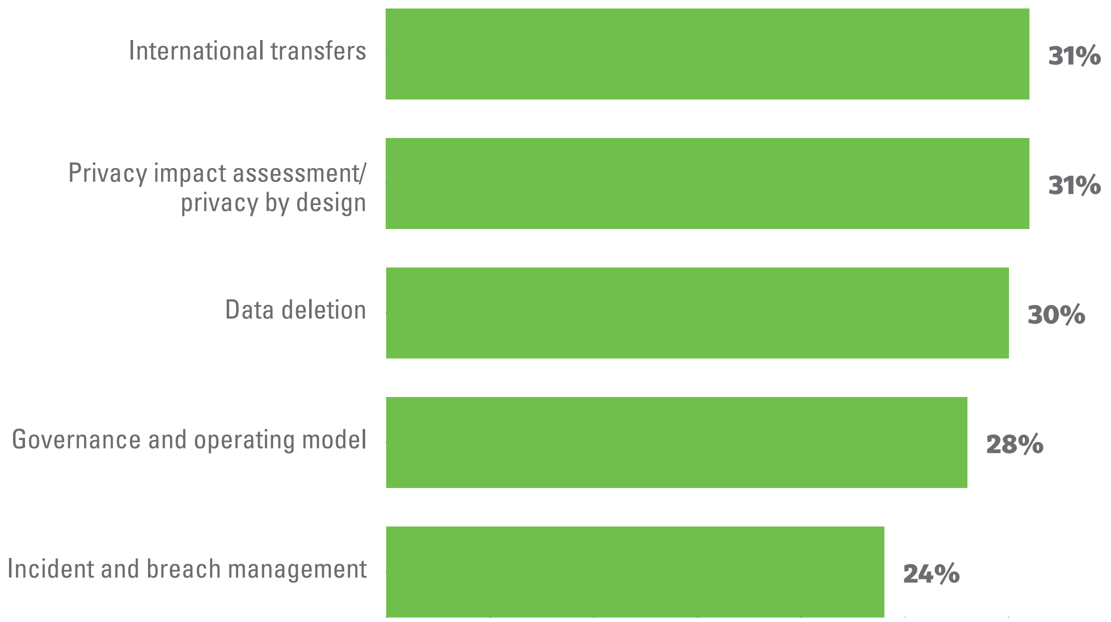
31% of respondents overall are prioritizing international transfers.

## Competing priorities: Getting the balance right

There has been no shortage of privacy priorities for privacy offices to consider. The foundational privacy items such as inventory, governance and incident response have been long-standing areas of focus for many organizations. With turbulent market conditions there are new and emerging challenges that are also vying for attention.

**Top 5 strategic privacy priorities for 2022**

*Top 5 of 30 items shown*



## This year's strategic priorities showed a mix of items driven from both external and internal issues

- → International transfers are nearly matched by privacy impact assessments/privacy by design (31%), which tops the priority list for life sciences and health care organizations. *(See graph on previous page).*
- → Data deletion (30%) follows close behind, a top focus for the education and nonprofit sectors, banking and insurance and business services. It's no small task looking at how to responsibly delete potentially zettabytes of data! *(See table on next page).*
- → 31% of respondents overall — 44% in Europe, 39% in Asia and 25% in North America — are prioritizing international transfers, which is not surprising given the recent adaptations to EU-U.S. data transfers and China's model clause drafts. *(See table to the right).*
- → Governance and operating model also continue to feature highly, with over 25% of organizations identifying this as key strategic priority. *(See graph on previous page).*
- → The number one priority for companies with more than $60 billion in revenue is incident and breach management and is the only revenue bracket where this is number one. *(See table on page 56)*

**Top 5 strategic privacy priorities for 2022 by continent**

*Top 5 of 30 items shown for each continent*

| North America | | |
|---|---|---|
| 01 | Privacy impact assessment/ privacy by design | 33% |
| 02 | Governance and operating model | 27% |
| 03 | Incident and breach management | 26% |
| 03 | Data deletion | 26% |
| 05 | International transfers | 25% |

| Europe | | |
|---|---|---|
| 01 | International transfers | 44% |
| 02 | Data deletion | 38% |
| 03 | Governance and operating model | 27% |
| 04 | Privacy impact assessment/ privacy by design | 26% |
| 05 | Artificial intelligence/ machine learning | 24% |

| Asia | | |
|---|---|---|
| 01 | International transfers | 39% |
| 02 | Governance and operating model | 34% |
| 03 | Data deletion | 27% |
| 03 | Data minimization | 27% |
| 03 | Artificial intelligence/ machine learning | 27% |

| Other | | |
|---|---|---|
| 01 | Privacy impact assessment/ privacy by design | 44% |
| 02 | Data deletion | 31% |
| 02 | Governance and operating model | 31% |
| 04 | Incident and breach management | 28% |
| 04 | Data minimization | 28% |

**Top 5 strategic privacy priorities for 2022 by sector**

*Top 5 of 30 items shown for each sector*

| Banking and insurance | | |
|---|---|---|
| 01 | Data deletion | 41% |
| 02 | Privacy impact assessment/ privacy by design | 36% |
| 03 | Governance and operating model | 34% |
| 04 | Incident and breach management | 31% |
| 04 | Third-party management | 31% |

| Technology and telecommunications | | |
|---|---|---|
| 01 | International transfers | 41% |
| 02 | Data deletion | 30% |
| 03 | Privacy impact assessment/ privacy by design | 26% |
| 03 | Artificial intelligence/ machine learning | 26% |
| 05 | Data minimization | 23% |

| Education and nonprofit | | |
|---|---|---|
| 01 | Data deletion | 40% |
| 02 | Privacy impact assessment/ privacy by design | 38% |
| 03 | Governance and operating model | 28% |
| 03 | Notice and consent | 28% |
| 03 | Privacy policy management | 28% |

| Business services | | |
|---|---|---|
| 01 | Data deletion | 45% |
| 02 | International transfers | 39% |
| 03 | Incident and breach management | 26% |
| 03 | Data minimization | 26% |
| 05 | Data subject rights | 24% |

| Consumer goods, services and retail | | |
|---|---|---|
| 01 | Data subject rights | 39% |
| 01 | Consumer privacy | 39% |
| 03 | International transfers | 31% |
| 03 | Data deletion | 31% |
| 05 | Privacy impact assessment/ privacy by design | 29% |

| Government | | |
|---|---|---|
| 01 | Incident and breach management | 42% |
| 01 | Data sharing | 42% |
| 03 | Privacy impact assessment/ privacy by design | 40% |
| 04 | Governance and operating model | 34% |
| 05 | Data minimization | 28% |

| Life sciences and health care | | |
|---|---|---|
| 01 | Privacy impact assessment/ privacy by design | 39% |
| 02 | International transfers | 35% |
| 03 | Governance and operating model | 34% |
| 04 | Inventory (Article 30) | 26% |
| 05 | Incident and breach management | 24% |

| Legal | | |
|---|---|---|
| 01 | Artificial intelligence/ machine learning | 32% |
| 02 | International transfers | 29% |
| 02 | Governance and operating model | 29% |
| 04 | Employment privacy | 26% |
| 05 | Data deletion | 24% |

| Manufacturing | | |
|---|---|---|
| 01 | International transfers | 41% |
| 01 | Localized privacy program | 41% |
| 03 | Privacy and customer | 28% |
| 03 | Privacy policy management | 28% |
| 05 | Data deletion | 22% |

| Other | | |
|---|---|---|
| 01 | International transfers | 37% |
| 02 | Privacy impact assessment/ privacy by design | 32% |
| 03 | Governance and operating model | 29% |
| 03 | Data deletion | 29% |
| 05 | Inventory (Article 30) | 23% |

**Top 5 strategic privacy priorities for 2022 by revenue**

*Top 5 of 30 items shown for each revenue band*

| Under $100M | | |
|---|---|---|
| 01 | Data deletion | 34% |
| 02 | Privacy impact assessment/ privacy by design | 29% |
| 02 | Governance and operating model | 29% |
| 02 | Incident and breach management | 29% |
| 05 | International transfers | 24% |

| $101M-$999M | | |
|---|---|---|
| 01 | Governance and operating model | 32% |
| 02 | Data deletion | 31% |
| 03 | Privacy impact assessment/ privacy by design | 30% |
| 04 | International transfers | 28% |
| 05 | Inventory (Article 30) | 25% |

| $1B-$8.9B | | |
|---|---|---|
| 01 | International transfers | 36% |
| 02 | Privacy impact assessment/ privacy by design | 35% |
| 03 | Data deletion | 33% |
| 04 | Governance and operating model | 29% |
| 05 | Localized privacy program | 23% |

| $9B-$19.9B | | |
|---|---|---|
| 01 | International transfers | 37% |
| 02 | Privacy risk controls and management | 29% |
| 02 | Localized privacy program | 29% |
| 04 | Privacy impact assessment/ privacy by design | 27% |
| 05 | Data deletion | 25% |

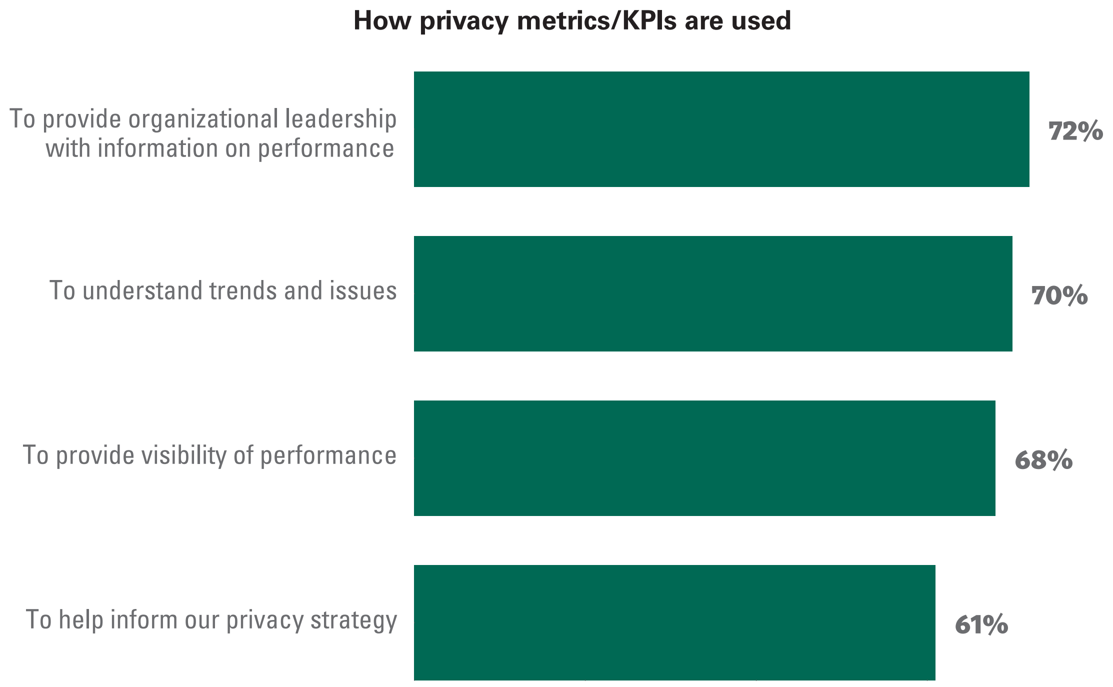
| $20B-$59.9B | | |
|---|---|---|
| 01 | International transfers | 40% |
| 02 | Artificial intelligence/ machine learning | 33% |
| 03 | Localized privacy program | 31% |
| 04 | Privacy impact assessment/ privacy by design | 26% |
| 04 | Privacy risk controls and management | 26% |

| $60B+ | | |
|---|---|---|
| 01 | Incident and breach management | 35% |
| 02 | International transfers | 33% |
| 02 | Privacy risk controls and management | 33% |
| 04 | Privacy impact assessment/ privacy by design | 31% |
| 05 | Artificial intelligence/ machine learning | 29% |

72% of organizations use KPIs to provide organizational leadership with information on performance.

## The measurement of success

Considering the multitude of priorities a privacy office needs to balance, it is essential for privacy offices to measure and evaluate how they are performing. Proper metrics help to identify the key issues and areas which need greater focus. Despite this, the subjective and contextual nature of privacy can make it a challenge to measure; often a single metric could act as both a positive and negative indicator, depending on how it is presented.


How privacy metrics/KPIs are used

## So, what privacy metrics do privacy offices capture?

→ Notably one-fifth of all respondents have not implemented privacy metrics. This increases to one-third of respondents when looking just at the lowest-revenue bracket, less than $100 million. *(See table to the right).*

→ Higher-revenue firms tend to gather metrics across more topics compared to lower-revenue firms. *(See table to the right).*

→ More than half of the companies use incident and breach management as well as data subject rights metrics. More than one-third use PIA/privacy by design and privacy programs metrics. *(See table to the right).*

→ The privacy metrics gathered reflect the industry privacy challenges in which the business operates. For example: 73% of consumer goods, services and retail businesses use data subject rights as a metric. *(See table on next page)*

→ Generally, there was not a significant difference across continents, with one notable exception: 61% of Europe-based respondents use incident and breach management as a topic for their privacy metrics, compared to just 36% of Asia-based respondents.

**Topics gathered for privacy metrics by revenue**

*Top 15 at total plus % none shown*

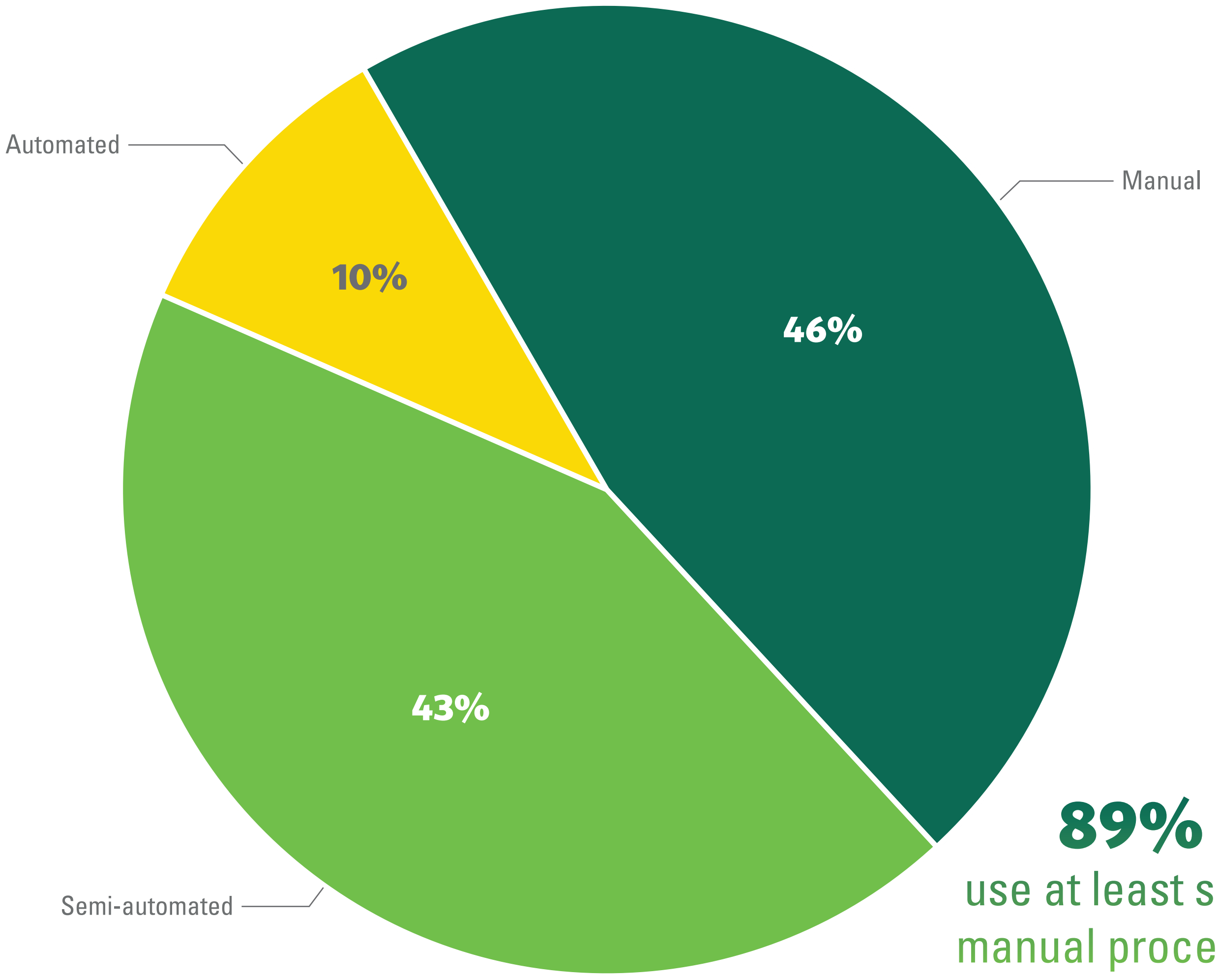
| | | REVENUE | | | | | |
|---|---|---|---|---|---|---|---|
| TOPICS | Total | Under $100M | $101M-$999M | $1B-$8.9B | $9B-$19.9B | $20B-$59.9B | $60B+ |
| Incident and breach management | 54% | 36% | 57% | 56% | 62% | 74% | 69% |
| Data subject rights | 51% | 32% | 57% | 60% | 49% | 50% | 69% |
| Privacy impact assessment/ privacy by design | 32% | 15% | 35% | 34% | 33% | 41% | 51% |
| Privacy program | 31% | 17% | 30% | 35% | 37% | 45% | 44% |
| Third-party management | 27% | 17% | 28% | 28% | 32% | 40% | 35% |
| Inventory (Article 30) | 26% | 13% | 28% | 31% | 25% | 33% | 33% |
| Data deletion | 26% | 18% | 30% | 30% | 25% | 24% | 20% |
| Privacy risk and controls management | 25% | 19% | 25% | 21% | 30% | 34% | 35% |
| Risk identification and quantification | 21% | 18% | 23% | 17% | 21% | 26% | 29% |
| Governance and operating model | 20% | 15% | 20% | 20% | 25% | 22% | 27% |
| Privacy policy management | 20% | 18% | 23% | 18% | 21% | 17% | 27% |
| Notice and consent | 20% | 15% | 16% | 25% | 16% | 24% | 31% |
| International transfers | 18% | 7% | 15% | 18% | 24% | 38% | 31% |
| Security for privacy | 18% | 17% | 20% | 12% | 21% | 26% | 16% |
| Data sharing | 15% | 13% | 15% | 13% | 21% | 14% | 16% |
| None of the above | 19% | 33% | 15% | 16% | 17% | 9% | 11% |

**Topics gathered for privacy metrics by sector**

*Top 15 at total plus % none shown*

| | | SECTOR | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| TOPICS | Total | Banking and insurance | Technology and telecommunications | Education and nonprofit | Business services | Consumer goods, services and retail | Government | Life sciences and health care | Legal | Manufacturing | Other |
| Incident and breach management | 54% | 68% | 49% | 51% | 58% | 53% | 60% | 58% | 24% | 66% | 51% |
| Data subject rights | 51% | 66% | 48% | 45% | 47% | 73% | 34% | 50% | 24% | 66% | 49% |
| Privacy impact assessment/privacy by design | 32% | 36% | 31% | 25% | 16% | 41% | 30% | 47% | 5% | 41% | 31% |
| Privacy program | 31% | 34% | 33% | 13% | 24% | 37% | 32% | 40% | 11% | 31% | 33% |
| Third-party management | 27% | 38% | 25% | 17% | 24% | 33% | 20% | 21% | 13% | 31% | 30% |
| Inventory (Article 30) | 26% | 30% | 29% | 21% | 21% | 35% | 18% | 24% | 13% | 28% | 27% |
| Data deletion | 26% | 32% | 21% | 17% | 18% | 49% | 16% | 19% | 16% | 22% | 29% |
| Privacy risk and controls management | 25% | 31% | 24% | 26% | 29% | 33% | 14% | 26% | 16% | 22% | 23% |
| Risk identification and quantification | 21% | 22% | 23% | 11% | 29% | 22% | 24% | 24% | 11% | 13% | 22% |
| Governance and operating model | 20% | 29% | 24% | 13% | 18% | 20% | 26% | 19% | 13% | 28% | 14% |
| Privacy policy management | 20% | 19% | 26% | 13% | 21% | 16% | 24% | 23% | 8% | 28% | 20% |
| Notice and consent | 20% | 21% | 15% | 19% | 24% | 24% | 10% | 19% | 11% | 22% | 25% |
| International transfers | 18% | 19% | 24% | 2% | 16% | 24% | 6% | 15% | 5% | 34% | 21% |
| Security for privacy | 18% | 15% | 19% | 19% | 29% | 16% | 18% | 15% | 16% | 22% | 17% |
| Data sharing | 15% | 17% | 10% | 11% | 16% | 16% | 22% | 11% | 5% | 16% | 17% |
| None of the above | 19% | 16% | 16% | 17% | 24% | 10% | 28% | 18% | 39% | 9% | 19% |

Process for recording/reporting on privacy metrics



89%
use at least some manual processes

## We also wanted to know how these metrics are collected and used

- → Overwhelmingly (89%), respondents use at least some manual processes to collect privacy metrics. *(See graph to the left).*
- → Firms gather privacy metrics on a wide variety of topics. The most common include incident and breach management (54%), data subject rights (51%), and PIA/privacy by design (32%). *(See table on previous page)*

More firms use these metrics to evaluate company performance than they do to help inform privacy strategy. In other words, privacy is understood by more companies to be performance-based rather than values-based.

We aim to provide research and insights that help build trust and confidence in the field of privacy.

## Our research approach

Our Research and Insight function focuses on bringing our membership accurate, meaningful, and actionable privacy insights in a digestible way. We aim to provide research and insights that help build trust and confidence in the field of privacy while addressing the most pressing current and future challenges faced by privacy professionals.

We focus our efforts on areas which matter most to our membership based on the changing world and organizational agenda.

We do this through leveraging our team of internal experts and a global network of subject matter experts, professionals, and volunteer contributors to deliver impactful insights for the benefit of our community.

The support and investment of our membership helps us to help you.

### Scope

The survey targeted IAPP members globally. It features more than 700 respondents, across over 44 countries, over a course of 10 weeks.

## The Focus

Our survey focused on gathering insight into five key areas of privacy organizational governance, specifically:

- → **Governance and Operating Model**: The organizational structures, roles and responsibilities for managing the collection, use, retention, disclosure and disposal of personal data.
- → **Privacy Strategy and Planning**: The activities undertaken by the privacy office to determine its strategic direction and the associated planning activities.
- → **Compensation Management**: The annual process of determining the compensation of privacy office staff.
- → **Budget Management**: The processes and supporting activities for the development, approval and spending of annual privacy budgets.
- → **Performance Metrics and Monitoring**: The organizational processes and measures to understand how the organization is performing against privacy strategy.

## The Approach

We have analyzed the results to provide meaningful insights. Some of the insights are based on a limited set of data points with fewer than 30 respondents. Where this is the case, we flagged these as "small sample size." Results from these segments should be considered directional and suggestive, rather than statistically definitive.

# Contacts

**Mark Thompson**
Chief Strategy Officer, IAPP
mthompson@iapp.org

**Saz Kanthasamy**
Principal Researcher –
Privacy Management, IAPP
skanthasamy@iapp.org

**Angela Saverice-Rohan**
Partner, EY Americas Privacy Leader
Angela.SavericeRohan@ey.com

**Brandon Lalonde**
Research and Insights Analyst, IAPP
blalonde@iapp.org

## Follow the IAPP on social media

Published November 2022.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.