IAPP-EY Privacy Governance Report 2023

Table of contents

What's inside?

Foreword

Privacy governance has never been more crucial to the success of an organization than it is in 2023.

While data privacy as a practice began in the 1970s and 1980s in the legal and policy realm, the technological advancements of recent decades necessitated a truly cross-disciplinary approach, with training, tools and wider professionalization across privacy law and policy, technology, business management, and design. Today, the privacy function is one of the most in-demand, prominent and mission-critical organizational functions. Its rise to such status was not unexpected, considering the increased circumstantial necessity and competitive advantages associated with good privacy governance in the modern data-driven economy.

But these are not halcyon days for the privacy function. The privacy function is contending with formidable challenges. The scale, velocity and variety of regulatory, technological and organizational change is unprecedented. The EU General Data Protection Regulation is now but one — albeit one very important — law. The proliferating alphabet soup of global privacy and privacy-relevant laws, combined with the advancement and integration of new technologies, such as artificial intelligence, add to the privacy work pile. The trend of organizations bringing the effective utilization of data closer to the core of their operating models is resulting in inter- and multidisciplinary privacy functions, which work across and feed into many other parts of the organization. Maturing, consequential public scrutiny and regulatory enforcement have heightened risk exposure. In today's economic climate, more work does not necessarily translate into larger budgets for privacy teams.

The IAPP-EY Privacy Governance Report 2023 builds on previous comprehensive efforts to shine a light on the location, performance and significance of privacy governance within organizations. For the first time, we explored organizational confidence when it comes to privacy governance and the drivers of those confidence levels. We shine a light on the increasingly important role of the data protection officer, as well as trending themes around privacy strategy, resourcing and budget. Crucially, the report also explores how privacy functions do more work and, invariably, do more with less. In doing more with less, we highlight the emergence and prevalence of privacy-enhancing technologies in privacy governance. These technologies, we expect, will not only grow in importance and use for privacy governance but will be increasingly underpinned by a more professional and standard privacy engineering community.

This year's survey generated instructive insights on how organizations are approaching the governance of AI. Some of those insights are included in the report. More will be shared in the IAPP-EY Professionalizing Organizational AI Governance Report later in the year.

We are pleased and humbled to bring you this year's report. We would like to thank the hundreds of professionals who gave their time and responded to this year's survey. Your insights, expertise and lived experience help power and empower the privacy profession and privacy functions around the world. We hope this report makes a meaningful and positive impact on organizations' privacy governance. Our thanks also to the IAPP and EY teams that made this report not only possible but challenged themselves and others to make it expert and engaging.

As you delve into the report, we encourage you to take a moment to reflect on your own role in governing privacy within your respective organizations. Each one of us plays a vital part in shaping a future where the use of personal data thrives alongside a deep-rooted respect for privacy. Together, let us continue to advance the privacy field, navigating emerging laws, technologies and risks, so effective privacy governance is ingrained into every aspect of the way our organizations use personal data.

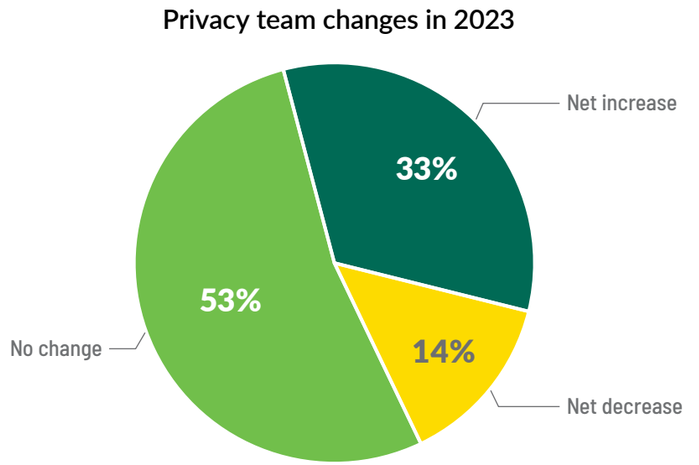
Joe Jones
Director of Research and Insights, IAPP

Angela Saverice-Rohan
EY Global Privacy Leader

Executive summary

Despite challenging economic conditions, 33% of organizations saw their privacy teams grow in the past year.

This investment reflects how the role of the privacy professional and privacy team has expanded and integrated into every facet of both day-to-day organizational operations and top-level strategic planning. Gone are the days when privacy was an insular workflow. Today, the privacy function is a beating heart for organizations, especially as they become more data-driven in the information economy. Of surveyed privacy pros, 86% reported regularly working with three or more teams within their organization. Decisions are being made at the top, with over 50% of those surveyed noting their reporting line goes directly to their company's C-suite and 78% responding that the most senior privacy leader is in the five highest levels of their organizations.



Information on privacy and privacy regulations is readily available, with just over 96% of respondents identifying that they are confident in their ability to stay informed about new privacy laws and policy initiatives. There is no question of privacy's importance nor does there seem to be a lack of information for those looking to deepen their own understanding of the field.

However, despite widespread recognition that adhering to global privacy regulations and standards is critical for success, fiscal headwinds and budgetary constraints threaten organizations' confidence in the efficacy of their privacy governance. Of respondents, 63% agreed that the limited availability of resources within their organization impacts their organization's ability to deliver on its privacy goals. The limitations were clearly outlined within survey responses, with 63% identifying that no recruitment is currently being undertaken and 67% indicating their budget is less than sufficient. To that end, only two out of 10 of those surveyed reported they were totally confident in their organization's privacy law compliance. The paradigm of doing more with less is a clarion call for more investment and smarter ways of working. Investment in training and technology — like emerging PETs, which 70% of organizations have yet to implement — will grow with importance.

All of this is against a backdrop where getting privacy right or wrong has never been so consequential. An organization's ability to adapt and thrive is increasingly linked to the extent to which privacy is connected to their larger strategic plan. Consumers, increasingly aware of their rights to privacy, may choose to seek alternative products and services in the absence of appropriate protections. For those unable to keep pace and comply with proliferating and maturing privacy laws, we've seen multi-billion-dollar fines, consumer distrust, business-model fracturing and market shutouts.

Today, the privacy function is a beating heart for organizations, especially as organizations become more data-driven in the information economy.

The path forward is clear — it is becoming more essential for privacy governance to be elevated to, integrated with, and even become the governance of everything. We demonstrate not only why this is important to organizations, but what steps organizations are taking now and looking to take in the future to make a success out of privacy governance.

Saz Kanthasamy
Principal Researcher,
Privacy Management, IAPP

Brandon Lalonde
Research and Insights Analyst, IAPP

A note on statistical significance: Throughout this piece, the term "significant" is only used to denote figures that are statistically significant at a 95% confidence interval (p=0.05). ↑ denotes a figure that is significantly higher than the rest of the sample, and ↓ denotes a figure that is significantly lower than the rest of the sample.

Part I. Compliance

Of organizations surveyed, 18% reported total confidence in their privacy law compliance and 10% reported no confidence.

The proliferation of privacy legislation, pace of reform and increased regulatory focus all helped propel privacy functions to unchartered prominence within organizations. Privacy programs are no longer one-off exercises designed to meet the requirements of new privacy legislation. Now privacy functions are at the forefront of strategic decisions on personal data use, weaving privacy requirements into all levels of the organization. It is no surprise privacy compliance has been thrust to the front of consumers' minds, requiring organizational leadership to pay more attention to — and invest more in — privacy.

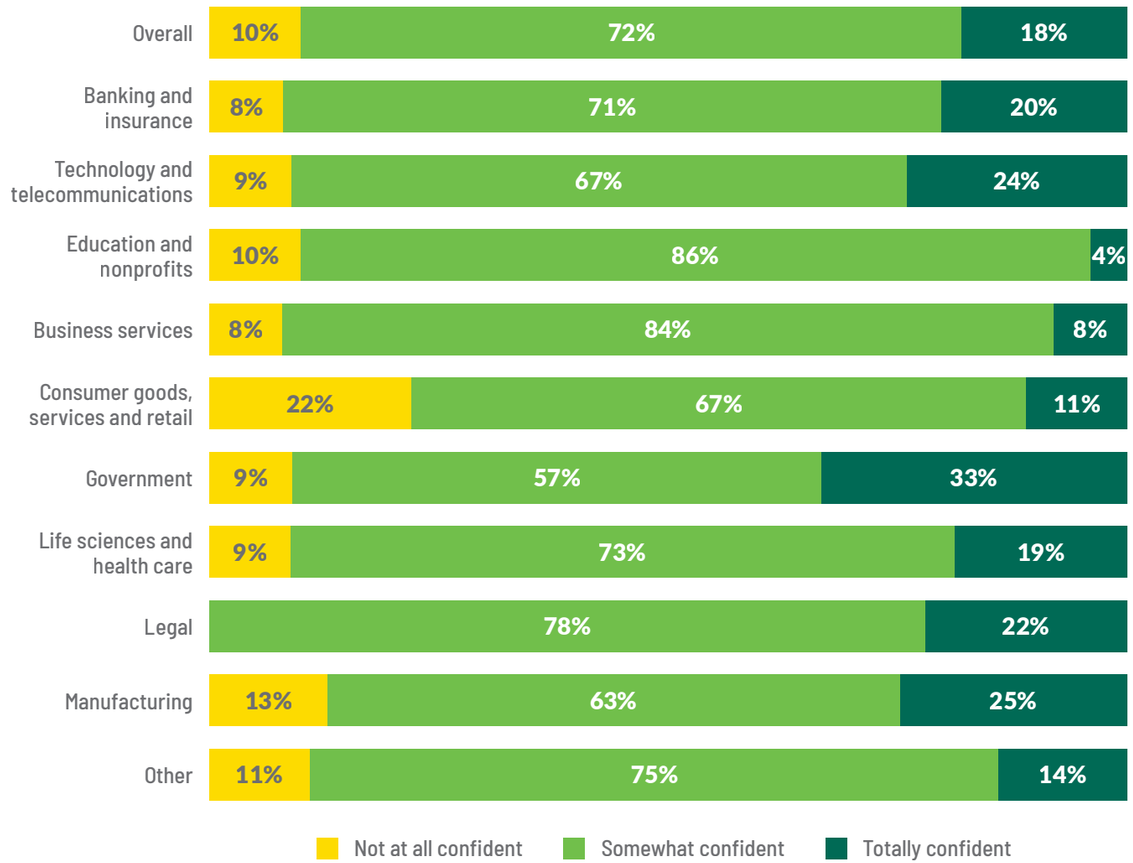
Given the journey they have taken since the advent of major privacy legislation, we sought to understand the level of confidence privacy pros have in their organization's ability to comply with the many privacy laws and policies across applicable jurisdictions. Three years after the GDPR went into force, just over 50% of respondents rated themselves as very or fully compliant with the law in our 2021 survey. While that is an improvement on the six in 10 who predicted partial compliance at best when the GDPR entered into force in May 2018, it highlights the challenge of maintaining sustainable compliance in the face of internal and external changes. The world has moved on, with proliferating and, in many cases, competing or conflicting laws, merging technologies with novel use cases of personal data and a challenging economic environment. How confident are privacy pros in their company's compliance with privacy laws and policies in 2023?

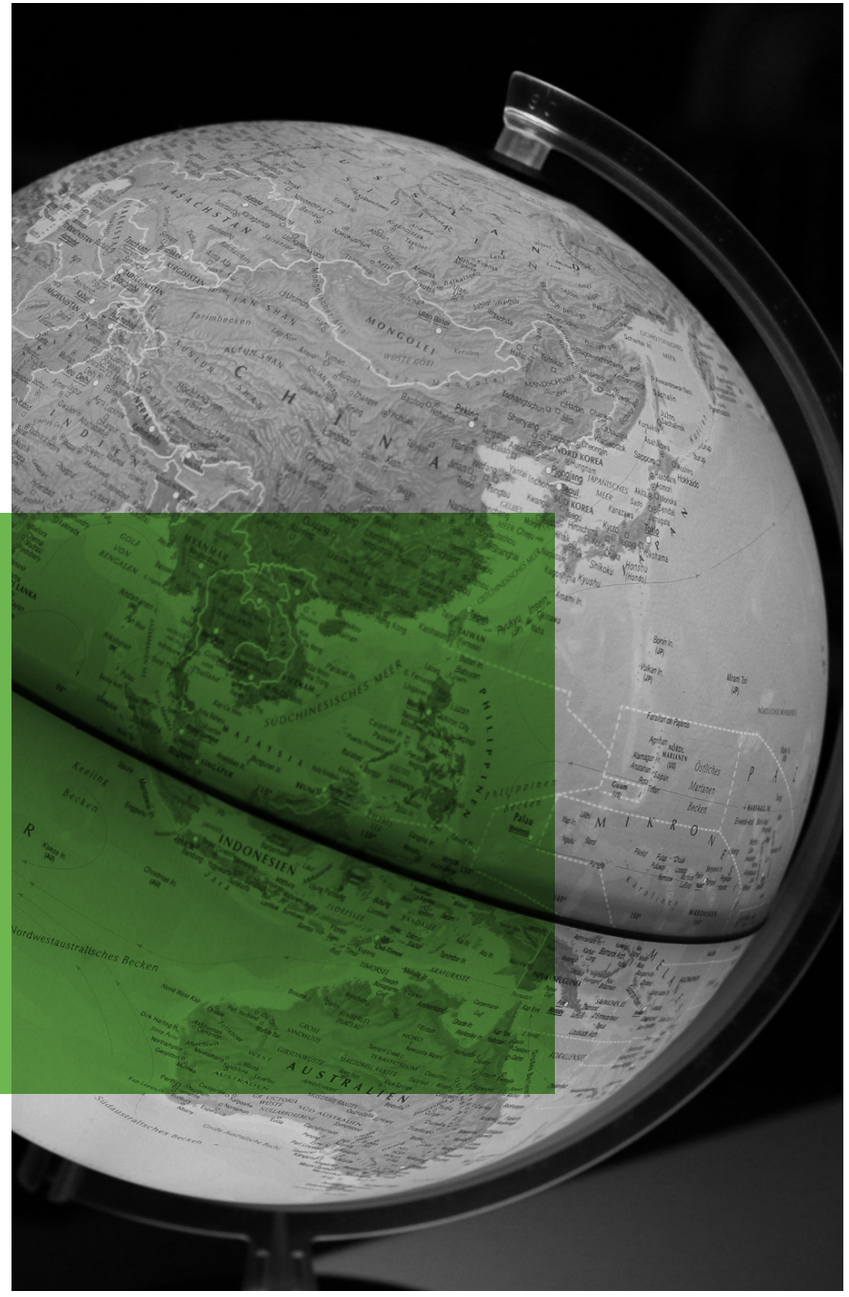
Confidently compliant?

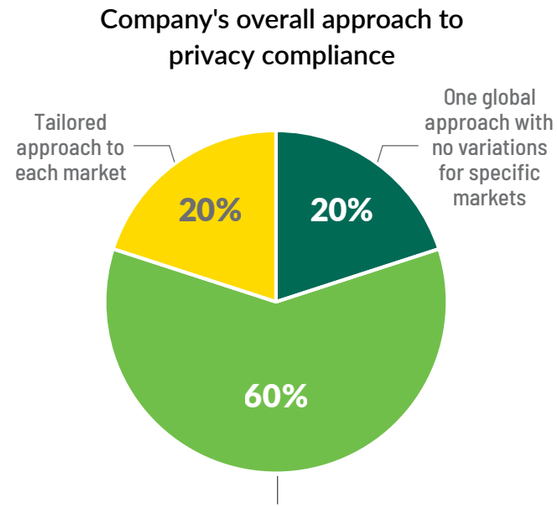
While two in 10 respondents identified they were totally confident in their organization's ability to comply with various privacy regulatory requirements, one in 10 identified they were not at all confident. This may come as no surprise given the enormity of the task facing privacy pros, the pace of change in the regulatory and broader environment, and scale of developments — from the GDPR to Brazil's data protection law, the Lei Geral de Proteção de Dados, to China's Personal Information Protection Law to India's Digital Personal Data Protection Act.

When considering confidence by sector, respondents working in government were among the most confident in their organization's ability to comply with privacy legislation, whereas a greater proportion of respondents working in consumer goods, services and retail reported they were not at all confident in their organization's ability to comply. One reason for this may be the multinational and consumer-facing nature of firms in the consumer goods, services and retail sector, meaning privacy pros are more likely to contend with a wide variety of international privacy laws.

Employee confidence in their company's compliance with privacy laws and policies across jurisdictions overall and by sector







Overall compliance approach

Given the advent and proliferation of major global privacy legislation, we sought to understand further how organizations structure their responses to different global requirements. Six in 10 respondents identified their organization takes a global approach that implements heightened or reduced regulatory requirements where certain jurisdictions allow. Two in 10 respondents identified their organization takes a single global approach regardless of local requirements, while another two in 10 identified their organization does not leverage a global approach, instead taking a per-country tailored approach to privacy compliance.

A significant proportion of respondents in the business services, consumer goods, services and retail, and manufacturing sectors identified their organizations use global approaches with either increased or reduced requirements in certain jurisdictions. No respondents in the manufacturing sector identified their organization takes a single global approach, the only sector to report any option at zero. This trend continues across most sectors and organization sizes, either by revenue or number of employees. Organizations with less than USD100 million in revenue were among the most likely, at three in 10, to take one global approach with no local market variations, whereas organizations with more than USB60 billion in revenue were among the least likely, at one in 10.

Respondents from multinational organizations were more likely to say their company leverages a global approach and identify exceptions based on local requirements instead of using a single fixed global approach. The more markets an organization operates in, the more likely they are to utilize a global baseline with variations. Organizations that operate in 2-20 markets averaged 70%, whereas those in 21-40 markets averaged 84%. While a more flexible approach allows an organization to update its compliance approach to local requirements, it also requires more work for the privacy team to stay on top of and respond to local regulatory requirements.

Company's overall approach to privacy compliance by sector

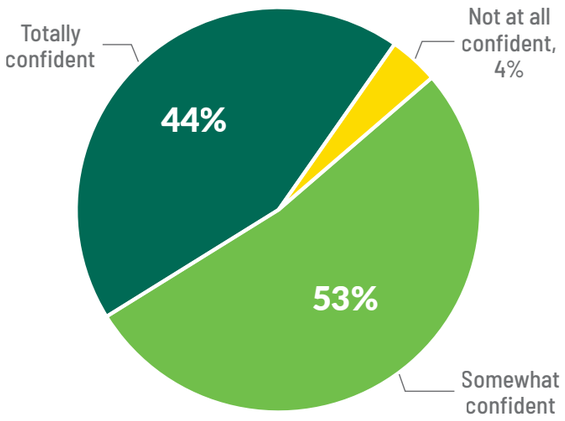
OVERALL APPROACH	SECTOR									
	Banking and insurance	Technology and telecommunications	Education and nonprofits	Business services	Consumer goods, services and retail	Government	Life sciences and health care	Legal	Manufacturing	Other
One global approach with no variations for specific markets	20%	13%	28%	12%	7%	**41% ↑**	27%	11%	**0% ↓**	18%
A global approach that makes use of heightened or reduced regulatory requirements in certain jurisdictions	57%	**71% ↑**	52%	**80% ↑**	**85% ↑**	**19% ↓**	60%	56%	**88% ↑**	62%
A tailored approach to each market	22%	16%	20%	8%	7%	**41% ↑**	13%	33%	13%	20%

Company's overall approach to privacy compliance by number of countries of operation

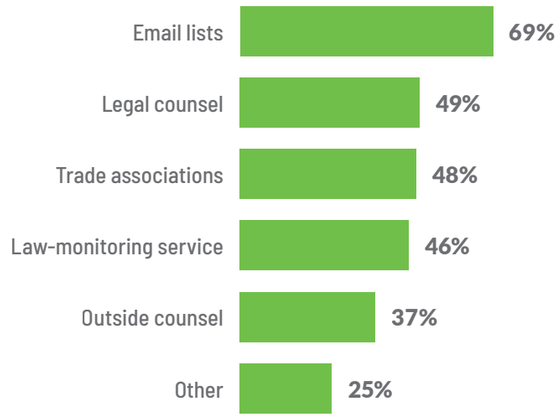
OVERALL APPROACH	NUMBER OF COUNTRIES OF OPERATION						
	1	2-5	6-10	11-20	21-40	41-60	More than 60
One global approach with no variations for specific markets	**43% ↑**	18%	**11% ↓**	15%	**7% ↓**	**5% ↓**	**9% ↓**
A global approach that makes use of heightened or reduced regulatory requirements in certain jurisdictions	**24% ↓**	68%	**74% ↑**	69%	**84% ↑**	73%	**78% ↑**
A tailored approach to each market	**33% ↑**	13%	16%	17%	**10% ↓**	22%	13%

Respondents from multinational organizations were more likely to say their company leverages a global approach and identify exceptions based on local requirements instead of using a single fixed global approach. The more markets an organization operates in, the more likely they are to utilize a global baseline with variations.

Confidence in staying informed about new privacy laws and policy initiatives



Methods of staying informed about new privacy laws and policy initiatives



Staying informed to stay ahead

Keeping up with the velocity and variety of privacy compliance requirements around the world is one of the most vexing privacy governance challenges. Notwithstanding the legal consequences for failing to comply with privacy requirements, the organization's employees, leadership and consumers will not be impressed if the failure is due to its inability to stay informed.

Given this, we sought to understand respondent's confidence in their organization's ability to stay informed about new privacy laws and initiatives, and the methods they use to stay informed.

The majority of respondents, at just over 96%, identified they are confident in their company's ability to stay informed about new privacy laws and policy initiatives, with just over four in 10 identifying total confidence in their company's ability to stay informed.

Privacy pros use a variety of methods to stay informed, with almost seven in 10 using email lists. These respondents were mostly from law firms, the IAPP, or were other subject matter experts like external consultants. Nearly five in 10 use trade associates and advice from internal legal counsel to stay informed, while almost four in 10 use outside counsel.

Overall, organizations use a number of different methods to stay informed. This likely contributes to confidence in their ability to stay informed.

Part II.

Privacy strategy

AI governance has grown in importance and is now a prominent strategic priority across continents.

A well-defined privacy strategy can help an organization efficiently allocate resources to achieve its core privacy goals. If done well, a privacy strategy can serve as a roadmap and framework to guide decision-making and provide a cohesive and coordinated approach to achieving privacy compliance objectives with the available budget and resources. Core elements likely include clear objectives, a long-term vision, and an assessment of current and future resourcing. Also of importance is the need to assess the broader internal and external environment and incorporate resilience measures so organizations can adapt to the impacts of disruptions or unexpected events, including everything from data breaches to new privacy laws to the proliferation of novel use cases of new technologies.

Top five strategic priorities for 2023 versus 2022

2022	2023	Strategic priority	2022	2023
02	01	PIAs, PbD	31%	35%
09	02	AI governance	20% ↓	33% ↑
N/A	03	Cross-border compliance to align privacy program with multiple countries' new privacy laws	N/A	29%
01	04	International transfers	31% ↑	24% ↓
03	05	Data deletion	30% ↑	24% ↓

**N/A: No applicable data, as this section did not appear in the 2022 survey.*

Organizations see the importance of a privacy strategy. In 2022, two-thirds of respondents reported working in organizations that considerably aligned their privacy strategies to the overall corporate strategies. Privacy strategies are, therefore, likely to reflect the vision and strategy pursued by the broader organization. This year's survey further explores the strategic priorities identified by organizations for 2023.

The strategic priorities identified in this year's report reflect changes in the external and internal environments. AI governance significantly increased in priority for respondents, with one in three now identifying it as a strategic priority, rising from ninth in priority in 2022 to second for 2023. Privacy by design remains an important topic and the top priority for privacy pros in 2023. While international transfers and data deletion were in the top three in 2022, these dropped to fourth and fifth, respectively, for 2023. Ranked third in priority for 2023, and as a nod to the complex global privacy puzzle, cross-border compliance with new laws across multiple jurisdictions was a strategic priority for nearly a third of respondents.

Specifically, AI governance is now a prominent strategic priority across continents, prioritized by 40% of respondents in Asia, 38% in Europe and 30% in North America. It was also the biggest climber in North America, jumping up from 11th in 2022 to second in 2023. Given the advent of and progress toward the EU AI Act, along with notable EU enforcement relating to AI, governance is likely to stay top of mind through the rest of 2023. Perhaps reflecting the refocusing of organizations following "Schrems II" remediation activities and progress made on the EU-U.S. Data Privacy Framework, international transfers dropped in priority in 2023 across continents, falling to sixth in North America and fourth in Europe. Cross-border compliance to align privacy programs across multiple countries' new privacy laws is the top priority only in Asia. This is likely due to organizations responding to the multitude of new laws and law reform in Asia over the past year, from India to South Korea.

Top five strategic privacy priorities for 2023 versus 2022 by continent

NORTH AMERICA

2022	2023	Strategic priority	2022	2023
01	01	PIAs, PbD	33%	37% ↑
11	02	AI governance	17% ↓	30% ↑
N/A	03	Cross-border compliance to align privacy program with multiple countries' new privacy laws	N/A	27%
07	04	Privacy risk and controls management	22%	22%
03	05	Incident breach management	26%	22%

EUROPE

2022	2023	Strategic priority	2022	2023
05	01	AI governance	24%	38% ↑
02	02	Data deletion	38%	33%
N/A	03	Cross-border compliance to align privacy program with multiple countries' new privacy laws	N/A	32%
01	04	International transfers	44%	32%
04	05	PIAs, PbD	26%	29%

ASIA

2022	2023	Strategic priority	2022	2023
N/A	01	Cross-border compliance to align privacy program with multiple countries' new privacy laws	N/A	46% ↑
03	02	AI governance	27%	40%
N/A	03	Compliance programs for new privacy-adjacent digital and data laws	N/A	37% ↑
N/A	04	In-country compliance program for new local privacy laws	N/A	34% ↑
04	05	International transfers	26%	31%

OTHER

2022	2023	Strategic priority	2022	2023
01	01	PIAs, PbD	44%	44%
15	02	AI governance	13%	33%
02	03	Data deletion	31%	31%
04	04	Incident and breach management	28%	29%
02	05	Governance and operating model	31%	23%

**N/A: No applicable data, as this section did not appear in the 2022 survey.*

The combination of privacy impact assessments and PbD was the number one priority across four sectors: banking and insurance, government, other, and consumer goods, services, and retail, while cross-border compliance was selected as a top priority in three sectors: business services, life sciences and health care, and manufacturing. PIAs and PbD were in the top five priorities across eight sectors and sixth in the two other sectors, highlighting the relative strategic importance of this topic. AI governance was identified as a strategic priority across eight sectors, but not featured in the top five in the consumer goods, services and retail sector, where it was 11th, or in the manufacturing sector, where it was eighth.

A number of strategic priorities saw significant changes in rank compared to 2022. The variability in which strategic priorities rose or fell highlights that, while organizations may face similar privacy compliance responsibilities, their approaches vary significantly.

The combination of privacy impact assessments and PbD was the number one priority across four sectors (including banking and insurance, consumer goods, services and retail, government), while cross-border compliance was selected as a top priority in three sectors (business services, life sciences and healthcare and manufacturing).

Top five strategic privacy priorities for 2023 versus 2022 by sector

BANKING AND INSURANCE

2022	2023	Strategic priority	2022	2023
02	01	PIAs, PbD	36%	32%
06	02	Privacy risk and controls management	26%	31%
01	03	Data deletion	41%	31%
12	04	AI governance	18%	30% ↑
03	05	Governance and operating model	34%	28%

CONSUMER GOODS, SERVICES AND RETAIL

2022	2023	Strategic priority	2022	2023
04	01	PIAs, PbD	29%	56% ↑
12	02	Data subject rights	14%	30%
N/A	02	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	30%
02	04	Data deletion	31%	26%
12	04	Data minimization	14%	26%

**N/A: No applicable data, as this section did not appear in the 2022 survey.*

Top five strategic privacy priorities for 2023 versus 2022 by sector, *continued*

TECHNOLOGY AND TELECOMMUNICATIONS

2022	2023	Strategic priority	2022	2023
03	01	AI governance	26%	36%
01	02	International transfers	41%	30%
N/A	02	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	30%
03	04	PIAs, PbD	26%	29%
02	05	Data deletion	30%	25%

EDUCATION AND NONPROFITS

2022	2023	Strategic priority	2022	2023
15	01	AI governance	13%	44% ↑
01	02	Data deletion	40%	30%
06	03	Incident and breach management	26%	28%
02	03	PIAs, PbD	38%	28%
17	05	International transfers	11%	26%

GOVERNMENT

2022	2023	Strategic priority	2022	2023
03	01	PIAs, PbD	40%	57%
01	02	Incident and breach management	42%	39%
08	03	Privacy policy management (e.g., update/revision)	20%	37%
04	04	Governance and operating model	34%	28%
08	05	AI governance	20%	26%

BUSINESS SERVICES

2022	2023	Strategic priority	2022	2023
N/A	01	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	48%
05	02	AI governance	21%	40%
03	03	Incident and breach management	26%	36%
01	04	Data deletion	45%	32%
N/A	05	Compliance programs for new privacy-adjacent digital and data laws	N/A	28%

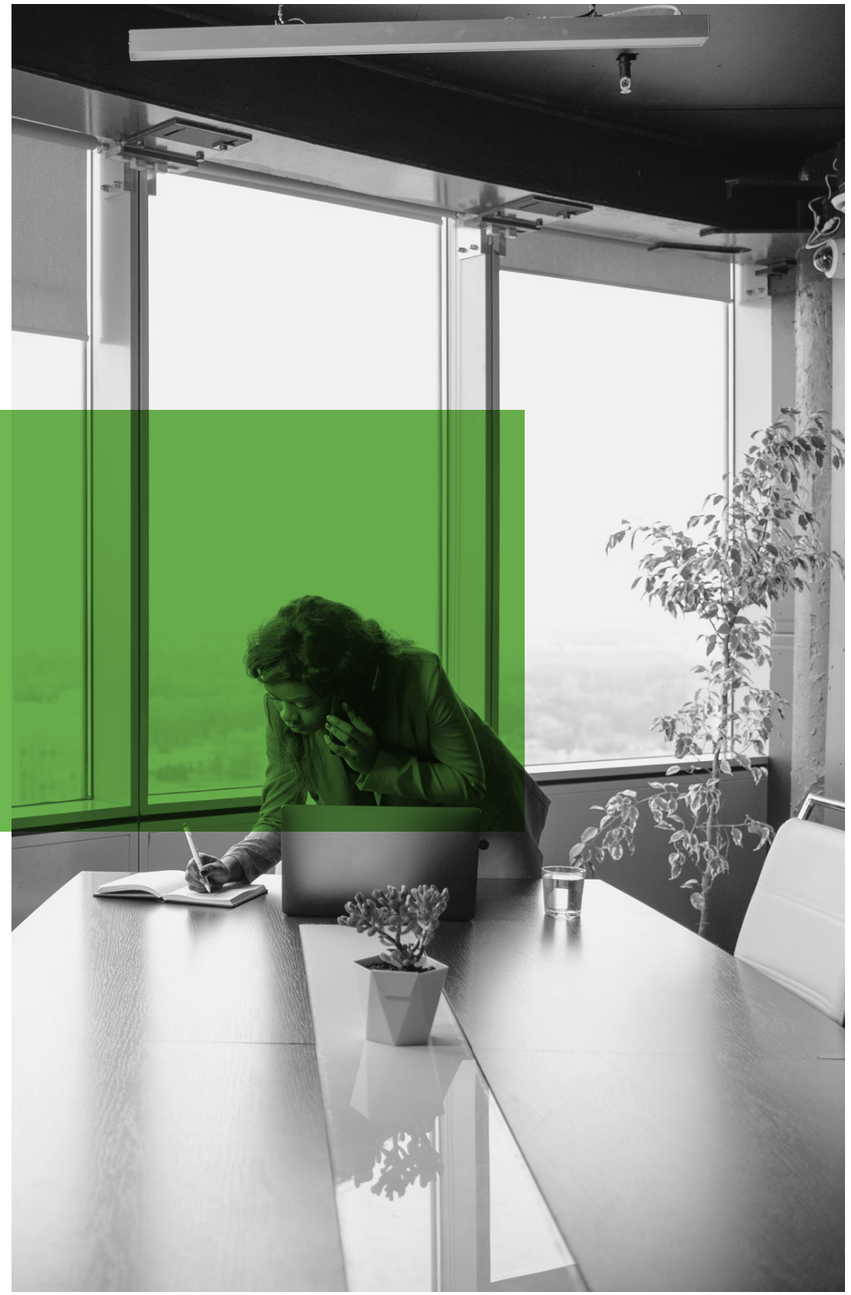
LIFE SCIENCES AND HEALTH CARE

2022	2023	Strategic priority	2022	2023
N/A	01	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	43%
07	02	AI governance	19%	39% ↑
02	03	International transfers	35%	36%
01	03	PIAs, PbD	39%	36%
05	05	Incident and breach management	24%	26%

LEGAL

2022	2023	Strategic priority	2022	2023
N/A	01	Compliance programs for new privacy-adjacent digital and data laws	N/A	44%
N/A	02	In-country compliance program for new local privacy laws	N/A	33%
N/A	02	AI governance	N/A	33%
01	04	Data deletion	32%	22%
19	04	Risk identification and quanitification	11%	22%

**N/A: No applicable data, as this section did not appear in the 2022 survey.*



Top five strategic privacy priorities for 2023 versus 2022 by sector, *continued*

MANUFACTURING

2022	2023	Strategic priority	2022	2023
N/A	01	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	50%
01	02	International transfers	41%	29%
04	02	Notice and consent	22%	29%
07	02	PIAs, PbD	19%	29%
15	05	Governance and operating model	13%	25%

OTHER

2022	2023	Strategic priority	2022	2023
02	01	PIAs, PbD	32%	35%
08	02	AI governance	20%	34% ↑
N/A	03	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	33%
01	04	International transfers	37%	26% ↓
05	05	Inventory (Article 30)	23%	24%

**N/A: No applicable data, as this section did not appear in the 2022 survey.*

In the banking and insurance sector, AI governance and privacy policy management were among the biggest climbers compared to 2022, rising eight and nine places respectively. On the other hand, data minimization dropped the farthest, falling 13 places from eighth in 2022. This may be due to the completion of data minimization projects, or it could reflect the tension between the data minimization principle and the significant data needs of AI-driven products and services.

Data subject rights rose 11 places from 2022 in the life sciences and health care sector to sit at tenth overall. In the consumer goods, services and retail sector it rose 10 places to second overall. This may be in part due to the consumer-facing and data-intensive processing nature of these organizations, changing regulatory requirements as well as the increased consumer understanding of their data-subject rights.

Top five strategic privacy priorities for 2023 versus 2022 by revenue

UNDER USD100 MILLION

2022	2023	Strategic priority	2022	2023
07	01	PIAs, PbD	21%	**34% ↑**
02	02	Data subject rights	29%	31%
N/A	03	Compliance programs for new privacy-adjacent digital and data laws	N/A	**28% ↑**
N/A	04	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	26%
05	05	Data minimization	24%	25%

USD101-999 MILLION

2022	2023	Strategic priority	2022	2023
03	01	PIAs, PbD	30%	33%
13	02	AI governance	17%	31%
02	03	Data deletion	31%	28%
N/A	04	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	25%
10	05	Privacy risk and controls management	17%	24%

USD1-8.9 BILLION

2022	2023	Strategic priority	2022	2023
02	01	PIAs, PbD	35%	37%
N/A	02	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	**36% ↑**
13	03	AI governance	14%	**32% ↑**
03	04	Data deletion	33%	26%
01	05	International transfers	36%	25%

USD9-19.9 BILLION

2022	2023	Strategic priority	2022	2023
03	01	PIAs, PbD	27%	39%
05	02	AI governance	22%	**37% ↑**
02	03	Privacy risk and controls management	29%	29%
05	04	Incident breach management	22%	27%
N/A	05	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	24%

USD20-59.9 BILLION

2022	2023	Strategic priority	2022	2023
03	01	PIAs, PbD	26%	**47% ↑**
02	02	AI governance	33%	**42% ↑**
N/A	03	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	33%
01	04	International transfers	40%	31%
01	05	Data deletion	22%	24%

USD60+ BILLION

2022	2023	Strategic priority	2022	2023
N/A	01	Cross-border compliance to align privacy program across multiple countries' new privacy laws	N/A	33%
04	02	PIAs, PbD	31%	31%
02	03	International transfers	33%	24%
05	04	AI governance	29%	21%
07	04	Governance and operating model	20%	21%

**N/A: No applicable data, as this section did not appear in the 2022 survey.*

PbD, PIAs, AI governance and cross-border compliance continue to be prioritized by organizations regardless of size. When considering organization size by revenue, AI governance climbs in strategic priority across all brackets except USD20-59.9 billion revenue, where where it remains second in priority for the second year running.

Given these shifts in priority, it is clear organizations are responsive to developments and elevate issues that require strategic focus. Organizations that do not take a strategic approach to privacy may be left behind by their peers. Our 2022 privacy governance report identified 13% of respondents either did not have a privacy strategy or had one that did not align with their corporate strategy, and found 11% of respondents updated their privacy strategy less frequently than annually. These respondents may find their privacy functions operate in a more reactive than proactive manner and may be less able to anticipate issues. For instance, privacy pros who do not anticipate their organizations taking a growth by question approach may find privacy risk is not effectively assessed as part of these acquisitions, or they cannot complete other privacy activities due to unanticipated work on privacy due diligence as part of mergers and acquisitions activities. Privacy pros working in organizations that do not have a privacy strategy may therefore need to consider whether their time, resources and budgets are effectively focused.

Part III.

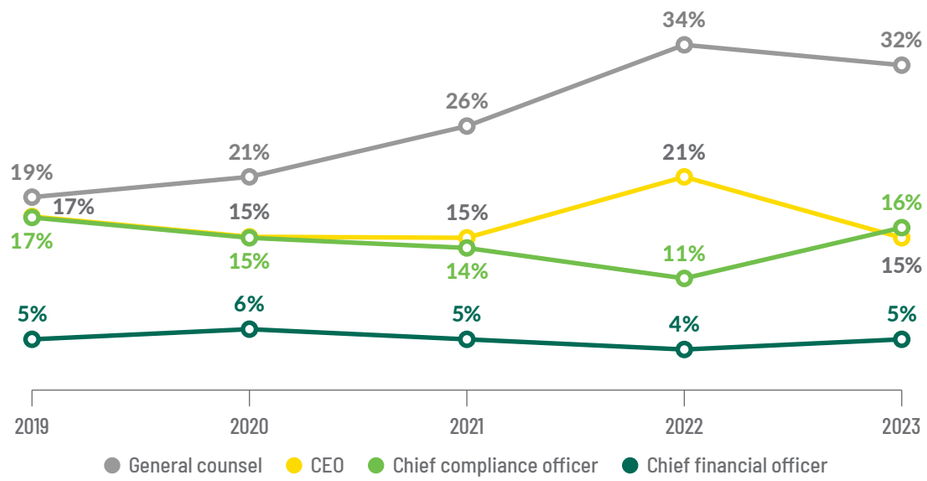
Reporting lines

The structure of the formal chain of command directly impacts the path decisions and tasks take through an organization.

The more formal the reporting line, the more likely there is greater clarity of responsibilities, accountabilities, communication and decision-making. The opportunity to report to a more senior privacy leader may offer increased exposure to strategic decision-making and the chance to influence and drive positive change within the organization. Privacy regulations continue to do their part by mandating designated privacy roles and reporting structures, often to the highest management level.

This year's report again looked at the reporting line of the most senior privacy pro in organizations.

Trend of the reporting line for the most senior privacy pro within an organization over five years



Reporting line for the most senior privacy pro within an organization by sector

REPORTING LINE	Overall	SECTOR									
		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	32%	23% ↑	42% ↑	30%	48%	63% ↑	15% ↓	34%	22%	17%	34%
Chief compliance officer	16%	23% ↑	9%	6%	0% ↓	11%	11%	30% ↑	22%	17%	14%
CEO	15%	11%	12%	18%	24%	4%	24%	16%	22%	21%	16%
Other	11%	11%	8%	18%	4%	4%	22% ↑	7%	11%	8%	12%
Chief information officer	5%	3%	4%	10%	8%	4%	7%	1%	0%	8%	5%
Chief information security officer	5%	7%	5%	4%	0%	4%	6%	0% ↓	22% ↑	4%	7%
Chief risk officer	5%	13% ↑	5%	2%	8%	0%	0%	1%	0%	8%	3%
Chief financial officer	5%	4%	7%	6%	8%	7%	4%	4%	0%	8%	3%
Chief technology officer	3%	3%	4%	2%	0%	4%	0%	0%	0%	8%	5%
Chief operating officer	2%	2%	1%	4%	0%	0%	9% ↑	4%	0%	0%	1%
Chief people officer/ head of HR	0%	0%	0%	0%	0%	0%	2% ↑	0%	0%	0%	0%
Chief consumer officer/ head of consumer	0%	0%	0%	0%	0%	0%	0%	1%	0%	0%	1%
Chief product officer	0%	0%	3% ↑	0%	0%	0%	0%	0%	0%	0%	0%

Similar to 2022, general counsel/head of legal tops the list for the most common reporting line of the senior privacy individual. This trend stays fairly consistent across sectors. The banking and insurance sector shifts away from general counsel/head of legal to other roles, with respondents in the sector among the most likely to select chief risk officer. At three in 10, respondents in the life sciences and health care sector were among the most likely to select chief compliance officer for the most common reporting line. In every sector surveyed, other than the government and manufacturing sectors, the most senior privacy pro reports to the general counsel.

The second most common reporting line across sectors tended to be the CEO role. For organizations with under 100 employees or less than USD100 million in annual revenue, the CEO tended to be the most common reporting line. This suggests those in smaller organizations have a greater chance to report directly into the highest levels of the organization. However, in larger organizations by both amount of employees and revenue, the most senior privacy individual tends to report to the general counsel/ head of legal.

Of respondents, 78% identified their organization's most senior privacy leader was in the five highest levels of the organization, while 21% were in the two highest levels.

Reporting line for the most senior privacy pro within an organization by number of employees and total annual revenue in USD

		NUMBER OF EMPLOYEES						REVENUE					
REPORTING LINE	Overall	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+	Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
General counsel/ head of legal	32%	18%	24% ↓	35%	35%	37%	37%	22% ↓	32%	36%	34%	47% ↑	29%
Chief compliance officer	16%	10%	7% ↓	18%	18%	21%	19%	10%	12%	18%	17%	20%	29% ↑
CEO	15%	38% ↑	23% ↑	12%	11% ↓	9%	15%	27% ↑	17%	11%	7%	7%	17%
Chief information officer	5%	5%	5%	4%	7%	5%	0%	5%	6%	4%	8%	0%	0%
Chief information security officer	5%	5%	2%	8%	6%	2%	7%	3%	3%	8% ↑	7%	7%	5%
Chief risk officer	5%	0%	3%	8% ↑	5%	4%	4%	3%	5%	5%	8%	4%	2%
Chief financial officer	5%	5%	8%	4%	3%	9%	2%	5%	6%	5%	2%	2%	2%
Chief technology officer	3%	3%	6% ↑	1%	3%	4%	2%	4%	3%	2%	3%	4%	2%
Chief operating officer	2%	3%	7% ↑	0% ↓	1%	2%	2%	4%	3%	1%	3%	0%	2%
Chief people officer/ head of HR	0%	0%	1%	0%	0%	0%	0%	1% ↑	0%	0%	0%	0%	0%
Chief consumer officer/ head of customer	0%	0%	0%	0%	1% ↑	0%	0%	0%	1%	1%	0%	0%	0%
Chief product officer	0%	0%	1%	0%	0%	2%	0%	1%	0%	0%	0%	0%	2% ↑
Other	11%	13%	12%	12%	11%	7%	13%	15%	12%	9%	10%	9%	10%

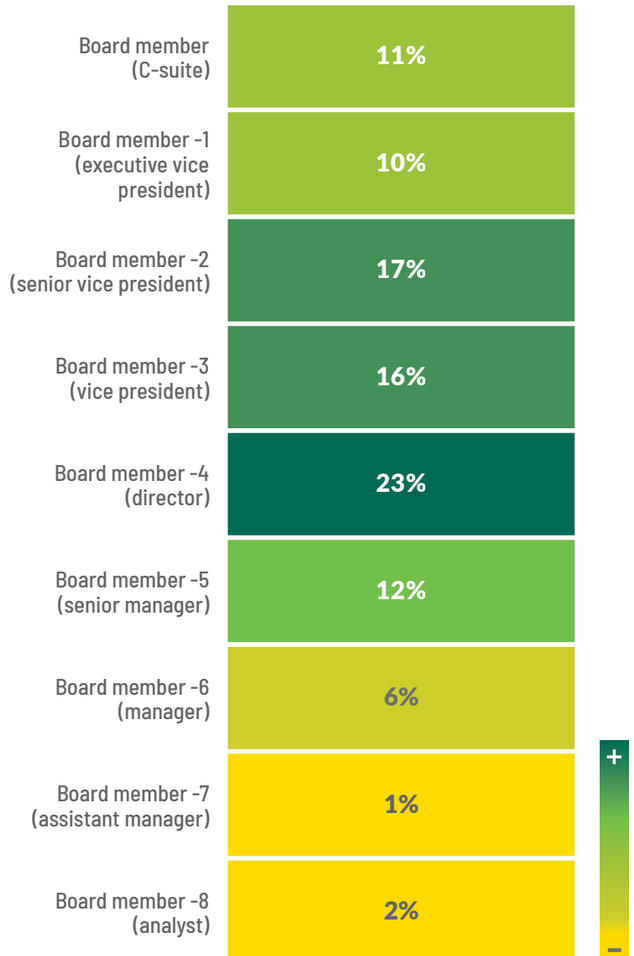
Reporting line for the most senior privacy pro within an organization by continent for the selected roles

REPORTING LINE	Overall	CONTINENT			
		North America	Europe	Asia	Other
General counsel/head of legal	32%	38% ↑	23% ↓	14% ↓	29%
Chief compliance officer	16%	16%	14%	29% ↑	8%
CEO	15%	10% ↓	26% ↑	26%	17%
Other	5%	7%	2%	0%	8%
Chief information security officer	5%	3% ↓	8% ↑	11%	4%
Chief risk officer	5%	5%	7%	0%	2%
Chief financial officer	5%	4%	7%	6%	8%

The most common reporting line for senior privacy individuals varied by continent where their organization is headquartered. In North America, general counsel was the most common top reporting line, matching last year's result, while in Europe it was the CEO and in Asia it was the chief compliance officer.

When looking at the seniority of the privacy leader relative to the board, results stayed fairly consistent with those found in the 2022 report. This year, 78% of respondents identified their most senior privacy leader was in the five highest levels of the organization, while just over one in five respondents identified their most senior privacy leader was in the top two levels.

Seniority of the most senior privacy employee at respondent's companies

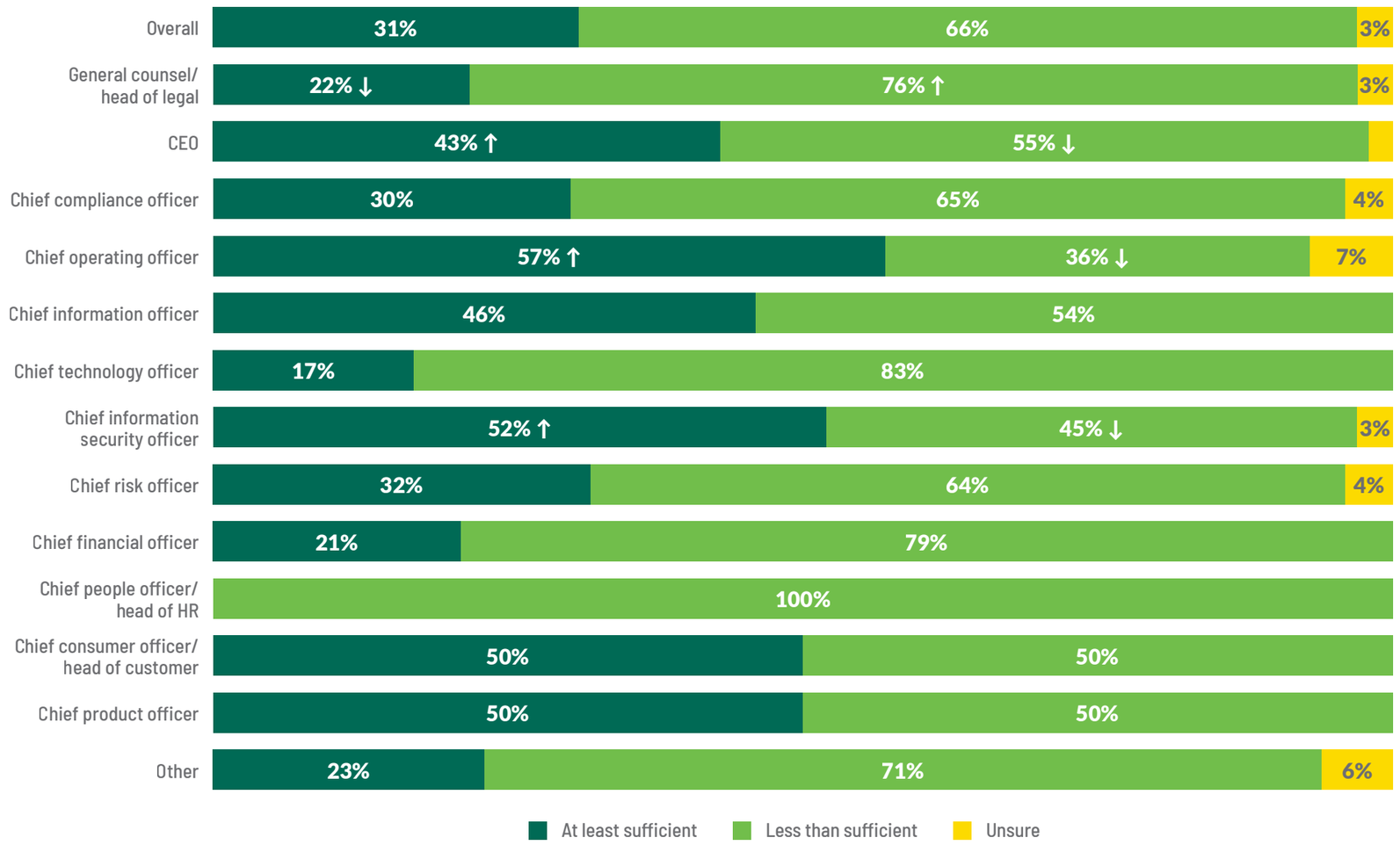


Seniority of the most senior privacy employee by number of employees and total annual revenue in USD

		NUMBER OF EMPLOYEES						REVENUE					
SENIORITY LEVEL	Overall	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+	Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
Board member (C-suite)	11%	**28% ↑**	14%	12%	**6% ↓**	4%	13%	**17% ↑**	**16% ↑**	**6% ↓**	**3% ↓**	7%	10%
Board member -1 (executive vice president)	10%	10%	9%	11%	11%	12%	9%	8%	12%	14%	10%	4%	5%
Board member -2 (senior vice president)	17%	**3% ↓**	12%	17%	19%	21%	**28% ↑**	**7% ↓**	15%	17%	**31% ↑**	24%	**29% ↑**
Board member -3 (vice president)	16%	8%	12%	17%	16%	21%	**26% ↑**	11%	12%	19%	24%	20%	21%
Board member -4 (director)	23%	21%	20%	22%	28%	25%	20%	23%	24%	23%	22%	29%	19%
Board member -5 (senior manager)	12%	15%	**18% ↑**	12%	10%	11%	4%	**19% ↑**	10%	11%	8%	13%	5%
Board member -6 (manager)	6%	5%	9%	5%	8%	5%	**0% ↓**	7%	9%	6%	2%	2%	7%
Board member -7 (assistant manager)	1%	3%	2%	1%	1%	2%	0%	2%	1%	2%	0%	0%	2%
Board member -8 (analyst)	2%	**8% ↑**	**5% ↑**	3%	**0% ↓**	0%	0%	**5% ↑**	2%	2%	0%	0%	2%

Smaller organizations, such as those with less than USD100 million in revenue or under 100 employees, were more likely to have their most senior privacy employee as a board member than larger organizations. In organizations with annual revenues greater than USD60 billion, 43% of respondents identified their most senior privacy employee is within the highest three levels of the organization. This number rose to one in two respondents for organizations with more than 80,000 employees. Organizations headquartered in North America tended to have a greater proportion of senior privacy leaders within the top five levels compared to other continents. Four in 10 respondents working for organizations headquartered in North America, Europe or Asia identified their most senior privacy leader is in the highest three levels.

Reporting line for the most senior privacy pro within an organization by respondent satisfaction with their budget



This year, respondents reporting to the chief operating officer and chief information security officer were more likely to identify they were happy with their budget allocation than not.

Therefore, one may conclude these reporting lines are beneficial in securing greater funding for an organization's privacy program.

The unique nature of every organization, along with legal requirements that vary by jurisdiction, means there is no one-size-fits-all answer for reporting lines. Privacy pros should consider how different reporting lines may alter decision-making, accountability, proximity and access to senior leadership, and potential onward impacts on budget. This year, respondents reporting to the chief operating officer and chief information security officer were more likely to identify they were happy with their budget allocation than not. Therefore, one may conclude these reporting lines are beneficial in securing greater funding for an organization's privacy program.

However, several other factors, such as organization size, data processing risk and compliance environment, are likely to influence current budget and perception of budget sufficiency. Respondents who said their company's most senior privacy pro reports to the chief compliance officer or chief technology officer were more likely to have experienced an increase in the size of their privacy team. Respondents who said their company's most senior privacy pro reports to the chief compliance officer, COO, chief technology officer, chief information security officer or chief risk officer were more likely to report higher-than-average net increases in team size.

Ultimately, however, confidence in compliance with privacy laws and policies across jurisdictions was largely unaffected by the different reporting line structures.

Part IV. Activities of the function

More than 85% of privacy pros reported working regularly with three or more other teams within the organization.

It is no secret that privacy teams work on a wide range of issues and across multiple departments. In particular, the rise and integration of AI technologies mixed with a tightening economy have forced privacy functions to contend with a wider range of governance issues with fewer resources.

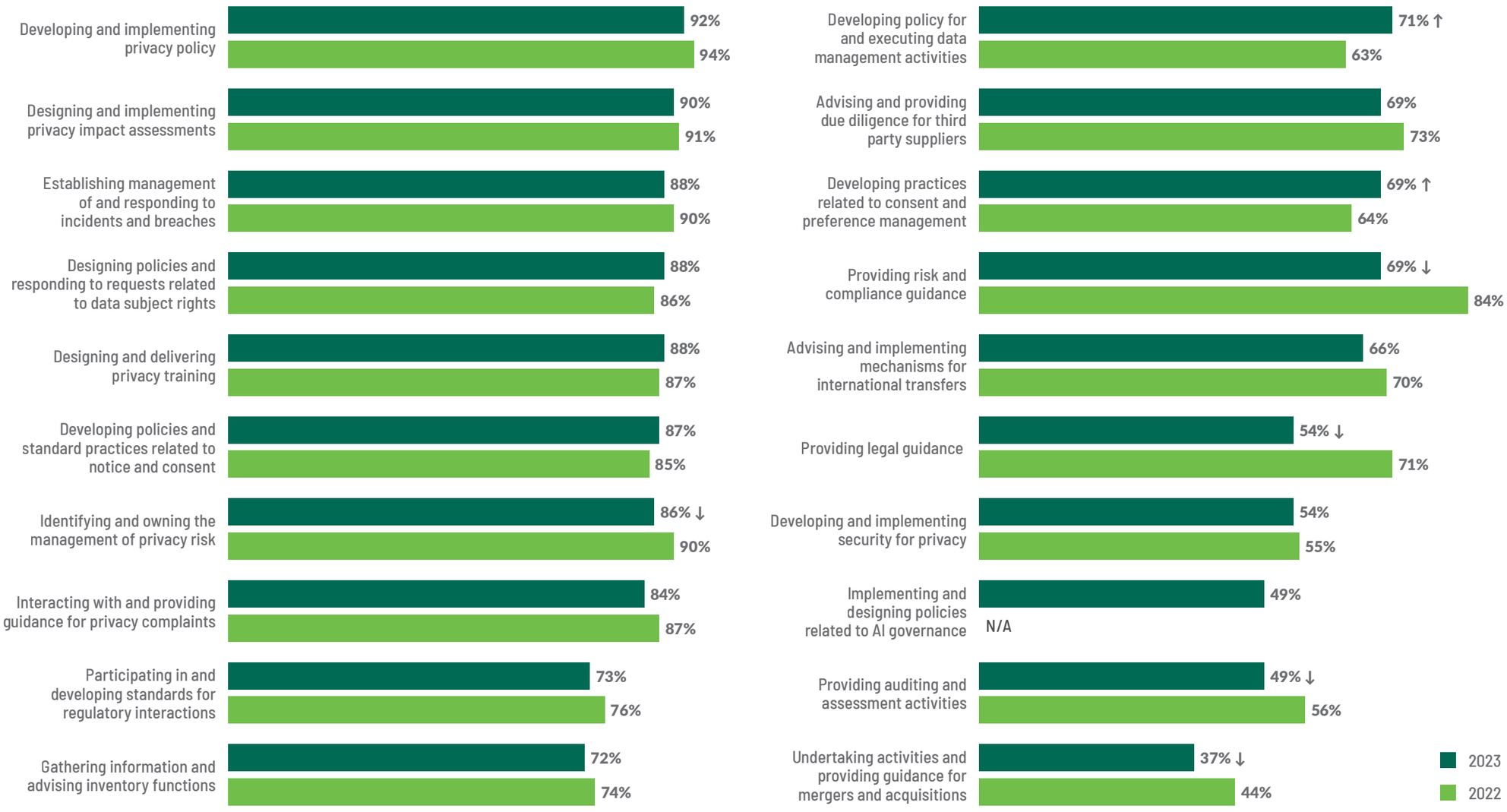
What is the focus?

Like last year, respondents indicated the types of activities their privacy function undertakes. The top three topics from 2022 carried into 2023 in the same order: developing privacy policies, conducting PIAs, and managing incidents and breaches. These results are not surprising, as all three activities are foundational for nascent and mature privacy programs.

AI governance was added to this year's survey, and 49% of respondents indicated their privacy function is working on AI governance. This is likely because the privacy and AI governance spaces overlap in many areas, like fairness and data security. Some of the privacy function's tools are also applicable to the AI governance function.

Still, respondents indicated their company's privacy functions do a great deal of work. In fact, the most popular combination of options selected by respondents was, by a significant margin, all 20 of them. Of respondents, 7% indicated their organization performs all 20 activities listed in the survey, and 86% said it performs at least 10 of them. While some activities may have matured and found a home in other functions, privacy teams should still expect to be nimble and cover a wide range of privacy governance activities.

Activities performed by a company's privacy function in 2023 versus 2022



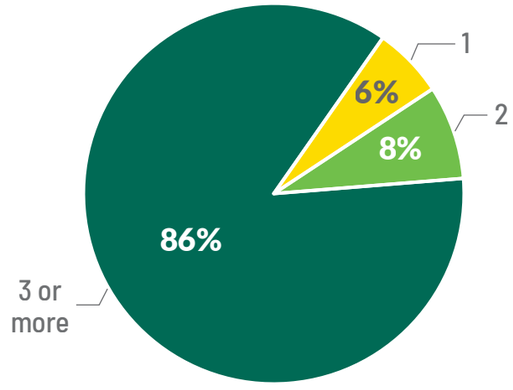
**N/A: No applicable data, as this section did not appear in the 2022 survey.*

Teamwork makes the dream work

We also ventured to find out which teams the average privacy team works with the most. Historically, privacy teams were born out of and worked within legal and compliance departments. This is not so today, as the expanding amount of interdisciplinary and cross-team work means the privacy team spreads across the organization more than ever before.

Specifically, we asked respondents to choose the three teams they collaborate with most. At 62%, the majority of respondents indicated legal and compliance, followed by the information technology and security teams, tied at 46%. This three-team combination was also the most popular, chosen by 8% of respondents overall. Only 14% of respondents reported their privacy function works with fewer than three other teams.

Percentage of organizations that work with the number of teams listed



Percentage of privacy pros organizations that work with each team

Percentage of organizations that work with each team by annual revenue in USD

TEAM	Overall	REVENUE					
		Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
Legal and compliance	62%	56%	57%	68%	71%	60%	64%
Security	46%	37% ↓	52%	53% ↑	39%	42%	36%
Information technology	46%	47%	50%	44%	44%	42%	48%
Data governance	20%	16%	19%	15%	24%	29%	36% ↑
Human resources	15%	13%	12%	16%	15%	22%	17%
Marketing	14%	11%	15%	15%	10%	22%	19%
Product development	13%	9%	19% ↑	10%	12%	13%	7%
Risk management	13%	18%	12%	11%	19%	13%	5%
Vendor management	12%	9%	9%	18% ↑	12%	13%	7%
Ethics and compliance	10%	7%	5% ↓	13%	17% ↑	13%	7%
Audit/internal control	9%	10%	8%	11%	7%	7%	5%
Customer support	7%	8%	8%	6%	14%	2%	2%
Executive leadership	6%	16% ↑	6%	4%	2%	2%	2%
Public relations/communications	2%	3%	2%	0%	0%	2%	5%
Other	5%	8%	3%	4%	3%	7%	7%

At 62%, the majority of respondents indicated collaboration with legal and compliance, followed by the information technology and security teams, tied at 46%. This three-team combination was also the most popular, chosen by 8% of respondents overall.

Breaking this up by yearly revenue, organizations with less than USD 100 million in revenue work with executive leadership significantly more than average, at 16% compared to just 6%. Companies on the other side of the spectrum, generating USD60 billion or more in revenue, work with data governance teams significantly more than average, at 36% compared to just 20%. Smaller organizations are less likely to have separate data governance functions — consider that 20% of respondents identified doing this exact activity — which explains why respondents who indicated they work with the data governance team generally increased with reported annual revenue.

These differences exemplify that, although several factors affect with whom and how often cross-team collaboration occurs, the average privacy function can still expect to work with nearly every team in the organization.

Part V.

Resourcing

Despite challenging economic conditions, 33% of organizations saw their privacy teams grow in the past year. Only 14% saw a decrease in their number of privacy staff.

Many hands make light work. With no such thing as light work in the privacy profession, resourcing is crucial, as appropriate consideration is needed for team size and the skills possessed by team members. Also of vital importance is the need to plan ahead, considering the organization's broader strategic direction, the privacy team's strategy and the broader compliance landscape. The cost of getting it wrong is great — too few team members could result in overwork and burnout, as well as the increased likelihood that privacy risks are not appropriately managed. At the same time, too many team members risks inefficiency and challenges in coordination. The need for a privacy team with the right skills to help the privacy function manage its compliance burden is of equal importance.
The balance between numbers and expertise is an ongoing challenge. In this year's survey, we sought to further understand the composition of staff in privacy functions, perceptions on resourcing, privacy team growth and recruitment plans.

Privacy team changes in 2023

Privacy function staffing

We first sought to understand the composition of privacy teams — what mix of roles are privacy teams comprised of?

Of respondents, 99% work in organizations with at least one internal privacy role, suggesting only 1% have outsourced the role entirely. This is up from 2022, when 96% reported at least one internal privacy role. In 2023, 31% of respondents said their company appointed external advisers. Internally appointed DPOs were the most popular role in a privacy team, selected by 51% of respondents. Internally appointed privacy lawyers and privacy managers tied for second place, with 47% of respondents selecting each option.

The most popular externally appointed role was the privacy lawyer, with 14% of respondents identifying their organization instructed privacy lawyers to assist with the privacy function. This was closely followed by externally appointed DPOs with just over one in 10 selecting this option. One in five respondents identified their organization appointed specific AI governance professionals, highlighting the role's recent growth in importance.

Overall composition of roles in privacy functions

ROLE	FUNCTION	
	Internal	External
Overall	99%	31%
Accountable privacy exec (i.e., board member)	45%	4%
Chief privacy officer (Global 250 organization)	10%	1%
Global CPO	29%	1%
Country-specific CPO	27%	2%
Regional privacy officer	16%	2%
Privacy office risk and compliance	31%	2%
Privacy champion/guru	33%	1%
Privacy auditor	16%	3%
Subject rights controller/administrator	27%	2%
Privacy engineer	16%	2%
Privacy lawyer	47%	14%
Cybersecurity	43%	5%
Data protection officer	51%	11%
Privacy manager	47%	2%
Privacy analyst	46%	3%
AI governance professional	18%	2%

When considering results by number of employees, as seen on the following page, smaller organizations tend to rely more on external resources. More than half, or 54%, of respondents working for organizations with less than 100 employees identified their organizations appointed at least one external resource to support privacy compliance. Notably, those respondents also identified their organization appointed external resources more than the overall average.

Results from respondents working for organizations with more than 80,000 employees highlighted how their organizations were more likely to have a broad spectrum of appointed roles and at least one individual in the majority of the survey roles. However, respondents in this category identified their company's privacy functions were less likely to have appointed cybersecurity professionals, which suggests privacy functions rely more on other functions within the organization to provide this expertise.

At least half of organizations with more than 1,000 employees have appointed a DPO internally. Privacy managers were more likely to be appointed by organizations with more than 5,000 employees, as more than six in 10 said their organization did so. Internal privacy lawyers were more likely to be appointed by organizations with more than 5,000 employees, as almost six in 10 respondents said their organization had done so.

Privacy engineers were more likely to be appointed at larger organizations. Respondents working for organizations with more than 5,000 employees identified their organization had this role more than average.

Somewhat logically, roles considered privacy leadership were more likely to be present in organizations with more employees. Roles such as global or in-country chief privacy officers and regional privacy officers were more likely to be found in organizations with more than 5,000 employees.

Composition of internal roles in privacy teams by number of employees

	ROLE	Overall	NUMBER OF EMPLOYEES: Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+
INTERNAL	Overall internal roles	99%	100%	98%	100%	99%	98%	98%
	Accountable privacy exec (i.e., board member)	45%	54%	43%	43%	40%	49%	59% ↑
	Chief privacy officer (Global 250 organization)	10%	5%	2% ↓	4% ↓	8%	21% ↑	39% ↑
	Global CPO	29%	8% ↓	17% ↓	23%	36% ↑	47% ↑	46% ↑
	Country-specific CPO	27%	26%	16% ↓	26%	30%	39% ↑	39% ↑
	Regional privacy officer	16%	5% ↓	6% ↓	13%	17%	32% ↑	39% ↑
	Privacy office risk and compliance	31%	44%	21% ↓	27%	27%	47% ↑	46% ↑
	Privacy champion/guru	33%	31%	25% ↓	29%	37%	42%	46% ↑
	Privacy auditor	16%	18%	11%	16%	12%	25%	30% ↑
	Subject rights controller/administrator	27%	28%	24%	23%	25%	37%	44% ↑
	Privacy engineer	16%	21%	10%	9% ↓	18%	26% ↑	26% ↑
	Privacy lawyer	47%	13% ↓	29% ↓	46%	57% ↑	60% ↑	67% ↑
	Cybersecurity	43%	44%	47%	47%	42%	33%	33%
	Data protection officer	51%	36% ↓	45%	53%	55%	60%	54%
	Privacy manager	47%	33%	33% ↓	32% ↓	60% ↑	65% ↑	61% ↑
	Privacy analyst	46%	23% ↓	36% ↓	37% ↓	55% ↑	63% ↑	63% ↑
	AI governance professional	18%	13%	16%	14%	16%	28% ↑	31% ↑

HIGHER THAN OVERALL AVERAGE

Composition of external roles in privacy teams by number of employees

	ROLE	Overall	NUMBER OF EMPLOYEES: Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+
EXTERNAL	Overall external roles	31%	54% ↑	36%	27%	26%	25%	31%
	Accountable privacy exec (i.e., board member)	4%	18% ↑	4%	2%	2%	4%	6%
	Chief privacy officer (Global 250 organization)	1%	3%	0%	0%	1%	2%	6% ↑
	Global CPO	1%	8% ↑	0%	0%	1%	2%	4%
	Country-specific CPO	2%	5%	0%	0%	2%	2%	6% ↑
	Regional privacy officer	2%	8% ↑	1%	0%	2%	0%	4%
	Privacy office risk and compliance	2%	5%	3%	0%	1%	4%	6%
	Privacy champion/guru	1%	3%	0%	1%	1%	4%	4%
	Privacy auditor	3%	8%	6% ↑	1%	2%	2%	4%
	Subject rights controller/administrator	2%	5%	2%	1%	1%	2%	6% ↑
	Privacy engineer	2%	5%	0%	0%	2%	2%	9% ↑
	Privacy lawyer	14%	28% ↑	17%	12%	11%	12%	9%
	Cybersecurity	5%	13% ↑	5%	4%	3%	2%	9%
	Data protection officer	11%	13%	8%	12%	11%	5%	17%
	Privacy manager	2%	8% ↑	2%	1%	0% ↓	2%	6% ↑
	Privacy analyst	3%	10% ↑	2%	1%	2%	5%	7%
	AI governance professional	2%	10% ↑	0%	0%	1%	0%	7% ↑

HIGHER THAN OVERALL AVERAGE

Similar results were identified when considering the composition of privacy teams broken down by annual revenue of the organization, as seen on the following page. Respondents working for organizations with more than USD9 billion in revenue were more likely to have appointed individuals across the majority of surveyed roles.

Here, too, respondents working for larger organizations by revenue, more than USD1 billion, said their company was less likely to appoint cybersecurity professionals within the privacy function. Almost six in 10 respondents working for organizations with more than USD9 billion in revenue identified their organization appointed privacy managers and privacy analysts. A higher-than-average proportion of respondents working for organizations with more than USD1 billion in revenue identified their organization appointed internal privacy lawyers.

Almost six in 10 respondents working for organizations with more than USD9 billion in revenue identified their organization appointed privacy managers and privacy analysts.

Composition of internal roles in privacy teams by annual revenue in USD

	ROLE	Overall	REVENUE					
			Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
INTERNAL	Overall internal roles	99%	99%	99%	100%	98%	98%	98%
	Accountable privacy exec (i.e., board member)	45%	48%	44%	41%	47%	40%	57%
	Chief privacy officer (Global 250 organization)	10%	6%	2% ↓	7%	8%	29% ↑	40% ↑
	Global CPO	29%	12% ↓	21% ↓	38% ↑	39%	53% ↑	38%
	Country-specific CPO	27%	25%	23%	29%	32%	31%	33%
	Regional privacy officer	16%	4% ↓	10% ↓	19%	31% ↑	33% ↑	26%
	Privacy office risk and compliance	31%	35%	22% ↓	27%	41%	40%	43%
	Privacy champion/guru	33%	30%	31%	32%	39%	47%	36%
	Privacy auditor	16%	17%	13%	14%	20%	33% ↑	12%
	Subject rights controller/administrator	27%	24%	24%	27%	44% ↑	36%	21%
	Privacy engineer	16%	15%	10% ↓	15%	20%	27% ↑	24%
	Privacy lawyer	47%	30% ↓	37% ↓	57% ↑	58%	73% ↑	55%
	Cybersecurity	43%	50%	48%	40%	37%	36%	31%
	Data protection officer	51%	47%	55%	46%	54%	53%	60%
	Privacy manager	47%	31% ↓	39% ↓	51%	63% ↑	67% ↑	62% ↑
	Privacy analyst	46%	31% ↓	38% ↓	48%	66% ↑	73% ↑	57%
	AI governance professional	18%	15%	17%	16%	19%	27%	29%

HIGHER THAN OVERALL AVERAGE

Composition of external roles in privacy teams by annual revenue in USD

	ROLE	Overall	REVENUE					
			Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
EXTERNAL	Overall external roles	31%	35%	31%	30%	22%	33%	31%
	Accountable privacy exec (i.e., board member)	4%	7%	2%	3%	2%	7%	7%
	Chief privacy officer (Global 250 organization)	1%	1%	0%	1%	2%	2%	5% ↑
	Global CPO	1%	3%	0%	1%	2%	0%	2%
	Country-specific CPO	2%	2%	1%	3%	2%	0%	5%
	Regional privacy officer	2%	3%	1%	1%	3%	0%	2%
	Privacy office risk and compliance	2%	3%	2%	1%	2%	0%	7% ↑
	Privacy champion/guru	1%	2%	0%	2%	2%	0%	5% ↑
	Privacy auditor	3%	5%	3%	3%	3%	0%	2%
	Subject rights controller/administrator	2%	1%	2%	1%	3%	0%	7% ↑
	Privacy engineer	2%	1%	2%	1%	2%	0%	10% ↑
	Privacy lawyer	14%	20% ↑	13%	13%	7%	18%	10%
	Cybersecurity	5%	7%	4%	3%	5%	4%	5%
	Data protection officer	11%	8%	10%	13%	12%	13%	10%
	Privacy manager	2%	4% ↑	0% ↓	1%	2%	0%	5%
	Privacy analyst	3%	3%	1%	4%	5%	2%	7%
	AI governance professional	2%	3%	0%	0%	2%	2%	10% ↑

HIGHER THAN OVERALL AVERAGE

Overall, when looking at the composition of privacy teams by sector, respondents working in the technology and telecommunications and banking and insurance sectors were more likely to identify that their company's internal privacy teams included a diverse composition of the listed roles. Almost two in 10 respondents in the banking and insurance sector identified their company appointed AI governance professionals to the privacy function. A higher-than-average proportion of respondents in the banking and insurance, technology and telecommunications, education and nonprofit, and business services sectors identified their organizations appointed individuals to the AI governance role.

Respondents in the technology and telecommunications, business services, and manufacturing industries identified their organizations appointed privacy auditors within the privacy function significantly more than other sectors.. On the other hand, respondents in the life sciences and health care industries identified their organizations appointed individuals in this role the least.

At almost six in 10, a significant number of respondents in the education and nonprofit and business services sectors reported their privacy functions incorporated cybersecurity professionals.

Externally, a lower-than-average proportion of respondents in the banking and insurance, education and nonprofit, and government sectors identified their organizations appointed external resources. More than four in 10 respondents in the technology and telecommunications, and consumer goods, services and retail sectors identified their organizations appointed external resources. Companies in the banking and insurance, education and nonprofit, and government sectors were the least likely to have appointed external DPOs. Less than 5% of respondents in these sectors said their organizations did so.

A higher-than-average proportion of respondents in the banking and insurance, technology and telecommunications, education and nonprofit, and business services sectors identified their organizations appointed individuals to the AI governance role.

Composition of internal roles in privacy teams by sector

	ROLE	Overall	SECTOR: 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
	Overall internal roles	99%	99%	99%	100%	96%	96%	96% ↓	100%	100%	100%	100%
INTERNAL	Accountable privacy exec (i.e., board member)	45%	46%	47%	46%	48%	44%	46%	37%	22%	42%	47%
INTERNAL	Chief privacy officer (Global 250 organization)	10%	9%	14%	2%	8%	15%	7%	10%	11%	13%	10%
INTERNAL	Global CPO	29%	33%	37%	6% ↓	44%	33%	11% ↓	31%	11%	46%	31%
INTERNAL	Country-specific CPO	27%	37% ↑	22%	20%	16%	22%	41% ↑	33%	33%	21%	22%
INTERNAL	Regional privacy officer	16%	18%	24%	2% ↓	28%	15%	6% ↓	24%	11%	21%	15%
INTERNAL	Privacy office risk and compliance	31%	38%	41% ↑	16% ↓	36%	41%	28%	24%	22%	33%	27%
INTERNAL	Privacy champion/guru	33%	35%	37%	34%	44%	48%	19% ↓	24%	33%	42%	34%
INTERNAL	Privacy auditor	16%	14%	29% ↑	8%	32% ↑	4%	24%	4% ↓	11%	38% ↑	13%
INTERNAL	Subject rights controller/administrator	27%	32%	36%	22%	24%	33%	22%	23%	11%	33%	25%
INTERNAL	Privacy engineer	16%	16%	32% ↑	10%	16%	22%	11%	10%	22%	17%	12%
INTERNAL	Privacy lawyer	47%	42%	59% ↑	34%	56%	74% ↑	44%	39%	44%	46%	47%
INTERNAL	Cybersecurity	43%	41%	51%	58% ↑	64% ↑	41%	31%	34%	22%	50%	40%
INTERNAL	Data protection officer	51%	53%	54%	52%	64%	48%	43%	47%	56%	63%	50%
INTERNAL	Privacy manager	47%	52%	57%	42%	44%	63%	39%	37%	44%	54%	44%
INTERNAL	Privacy analyst	46%	56% ↑	55%	32% ↓	36%	52%	59% ↑	36%	22%	46%	42%
INTERNAL	AI governance professional	18%	19%	28% ↑	18%	24%	11%	17%	17%	11%	17%	14%

HIGHER THAN OVERALL AVERAGE

A lower-than-average proportion of respondents in the banking and insurance, education and nonprofit, and government sectors identified their organizations appointed external resources.

Composition of external roles in privacy teams by sector

	ROLE	Overall	SECTOR: 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
	Overall external roles	31%	23%	**45% ↑**	24%	44%	**48% ↑**	**11% ↓**	33%	56%	42%	29%
EXTERNAL	Accountable privacy exec (i.e., board member)	4%	5%	5%	8%	4%	4%	2%	0%	**22% ↑**	4%	3%
EXTERNAL	Chief privacy officer (Global 250 organization)	1%	2%	3%	0%	0%	0%	0%	0%	**11% ↑**	0%	1%
EXTERNAL	Global CPO	1%	1%	3%	0%	4%	0%	2%	0%	**11% ↑**	0%	1%
EXTERNAL	Country-specific CPO	2%	1%	1%	0%	0%	0%	2%	3%	**22% ↑**	0%	2%
EXTERNAL	Regional privacy officer	2%	1%	**7% ↑**	0%	0%	0%	0%	0%	**11% ↑**	0%	1%
EXTERNAL	Privacy office risk and compliance	2%	2%	4%	0%	0%	4%	6%	1%	11%	0%	1%
EXTERNAL	Privacy champion/guru	1%	1%	1%	0%	0%	0%	**6% ↑**	3%	**11% ↑**	0%	0%
EXTERNAL	Privacy auditor	3%	3%	7%	4%	4%	7%	2%	1%	11%	0%	2%
EXTERNAL	Subject rights controller/administrator	2%	2%	**7% ↑**	2%	0%	0%	0%	0%	**11% ↑**	0%	1%
EXTERNAL	Privacy engineer	2%	3%	4%	2%	0%	**7% ↑**	2%	1%	11%	0%	**0% ↓**
EXTERNAL	Privacy lawyer	14%	13%	18%	10%	24%	26%	**4% ↓**	11%	22%	25%	12%
EXTERNAL	Cybersecurity	5%	6%	4%	6%	4%	4%	7%	3%	**22% ↑**	13%	**1% ↓**
EXTERNAL	Data protection officer	11%	**5% ↓**	16%	**2% ↓**	12%	15%	**2% ↓**	13%	22%	17%	15%
EXTERNAL	Privacy manager	2%	1%	4%	2%	4%	0%	4%	1%	**11% ↑**	0%	0%
EXTERNAL	Privacy analyst	3%	3%	**8% ↑**	0%	4%	0%	6%	3%	11%	0%	3%
EXTERNAL	AI governance professional	2%	1%	**7% ↑**	2%	0%	0%	2%	0%	**11% ↑**	0%	0%

HIGHER THAN OVERALL AVERAGE

Internal privacy team size by number of employees and by annual revenue in USD

	ROLE	Overall	NUMBER OF EMPLOYEES						REVENUE					
			Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+	Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
	Overall internal roles	38.2	14.6	7.5 ↓	12.6 ↓	41.9	88.8 ↑	127.1 ↑	11.7	14.1 ↓	28.7	79.3	81.0	146.0 ↑
INTERNAL	Accountable privacy exec (i.e., board member)	0.8	1.0	0.6	0.6	0.6	0.6	3.0 ↑	0.7	0.7	0.5	2.4 ↑	0.7	1.1
INTERNAL	Chief privacy officer (Global 250 organization)	0.4	0.1	0.0	0.0	0.2	0.2	3.6 ↑	0.1	0.0	0.1	1.8 ↑	0.5	2.0 ↑
INTERNAL	Global CPO	0.5	0.1	0.2	0.2	0.4	0.5	2.5 ↑	0.1	0.2	0.4	2.1 ↑	0.7	0.4
INTERNAL	Country-specific CPO	1.5	0.3	0.2	0.3	3.4	0.8	3.0	0.4	0.3	3.7	2.2	1.0	1.1
INTERNAL	Regional privacy officer	0.7	0.2	0.1	0.2	0.7	1.1	3.4 ↑	0.1	0.3	0.5	2.9 ↑	1.3	0.9
INTERNAL	Privacy office risk and compliance	1.4	2.0	0.6	0.8	0.7	1.4	7.1 ↑	1.6	0.5 ↓	0.5 ↓	2.7	2.4	5.2 ↑
INTERNAL	Privacy champion/guru	9.9	1.7	1.0 ↓	3.1	14.9	20.0	26.8 ↑	1.4 ↓	4.4	10.9	15.9	32.8 ↑	18.9
INTERNAL	Privacy auditor	0.7	1.0	0.2	0.2	0.3	1.1	3.8 ↑	0.5	0.2	0.3	2.1 ↑	1.3	2.1
INTERNAL	Subject rights controller/administrator	1.4	0.4	0.6	1.3	1.1	1.1	5.9 ↑	0.7	1.2	0.5	3.9 ↑	1.9	3.8
INTERNAL	Privacy engineer	7.0	0.5	0.2	0.3	3.4	35.6 ↑	25.7	0.3	0.8	0.3	10.5	1.0	76.5 ↑
INTERNAL	Privacy lawyer	2.7	1.3	0.4	0.8	1.7	10.6 ↑	9.0 ↑	0.9	0.7	1.8	3.5	3.2	18.0 ↑
INTERNAL	Cybersecurity	5.9	1.1	1.2	2.1	9.0	2.2	24.2 ↑	1.4	1.7	5.4	14.7	19.5 ↑	10.6
INTERNAL	Data protection officer	1.4	0.8	0.8	0.8	1.5	2.0	4.2 ↑	0.7	1.2	1.1	2.9 ↑	3.4 ↑	1.5
INTERNAL	Privacy manager	3.0	1.7	0.6	0.5	1.3	8.6	15.3 ↑	0.9	0.7	1.0	3.6	2.6	25.3 ↑
INTERNAL	Privacy analyst	3.5	0.8	0.5	1.0	2.3	2.4	24.6 ↑	1.0	1.0	1.3	6.1	7.7	21.5 ↑
INTERNAL	AI governance professional	0.8	1.4	0.3	0.4	0.5	0.7	3.5 ↑	0.8	0.3	0.4	2.1 ↑	1.0	2.0

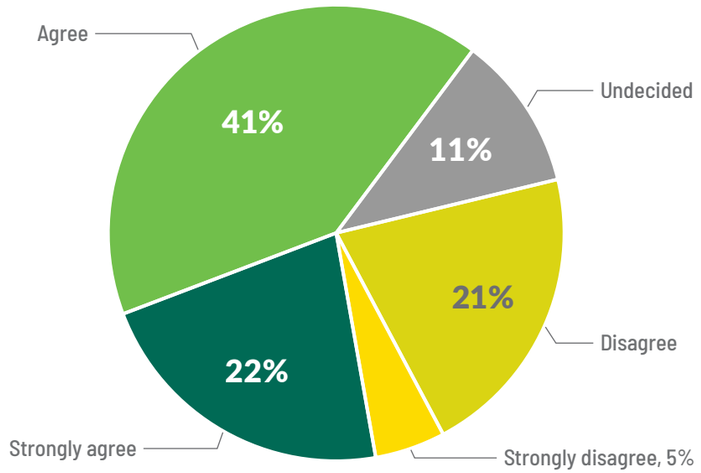
Considering the extent to which organizations appoint various privacy roles, the survey also looked at the number of privacy pros appointed to each role and the overall sizes of privacy functions.

External privacy team size by number of employees and by annual revenue in USD

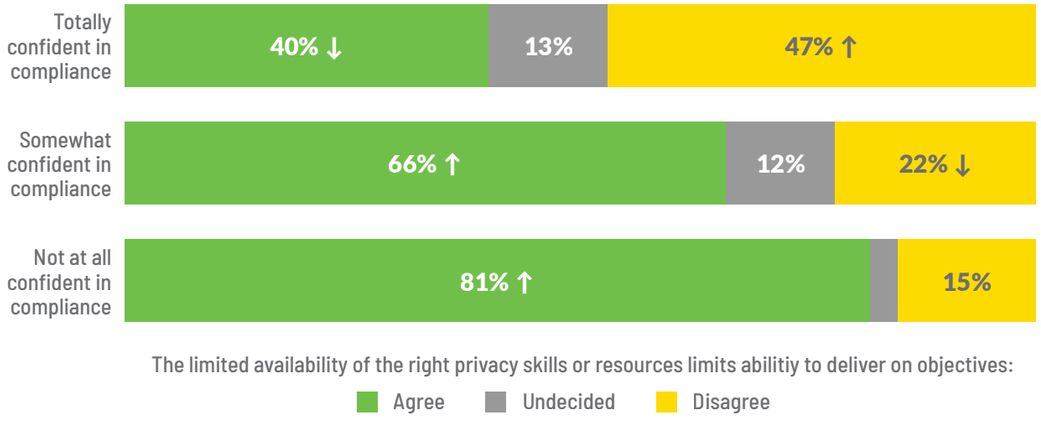
			NUMBER OF EMPLOYEES						REVENUE					
	ROLE	Overall	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+	Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
EXTERNAL	Overall external roles	5.4	11.8	1.9	1.3	2.0	1.2	**34.8 ↑**	4.8	1.6	2.1	**27.7 ↑**	3.7	4.7
	Accountable privacy exec (i.e., board member)	0.3	1.4	0.0	0.0	0.0	0.1	**1.9 ↑**	0.5	0.0	0.0	**1.7 ↑**	0.2	0.1
	Chief privacy officer (Global 250 organization)	0.2	0.1	0.0	0.0	0.0	0.0	**1.9 ↑**	0.0	0.0	0.0	**1.7 ↑**	0.0	0.1
	Global CPO	0.2	0.2	0.0	0.0	0.0	0.0	**1.9 ↑**	0.1	0.0	0.0	**1.7 ↑**	0.0	0.0
	Country-specific CPO	0.3	0.3	0.0	0.0	0.2	0.0	**1.9 ↑**	0.1	0.0	0.2	**1.7 ↑**	0.0	0.1
	Regional privacy officer	0.2	0.4	0.0	0.0	0.0	0.0	**1.9 ↑**	0.2	0.0	0.0	**1.7 ↑**	0.0	0.0
	Privacy office risk and compliance	0.5	1.3	0.8	0.0	0.0	0.1	**2.0 ↑**	0.5	0.6	0.0	1.7	0.0	0.3
	Privacy champion/guru	0.5	0.9	0.0	0.2	0.8	0.2	1.9	0.5	0.0	1.0	1.7	0.0	0.3
	Privacy auditor	0.3	0.9	0.1	0.0	0.0	0.0	**1.9 ↑**	0.3	0.0	0.0	**1.7 ↑**	0.0	0.0
	Subject rights controller/administrator	0.3	0.1	0.4	0.0	0.0	0.1	**1.9 ↑**	0.0	0.3	0.0	**1.7 ↑**	0.0	0.3
	Privacy engineer	0.2	0.4	0.0	0.0	0.1	0.0	**2.0 ↑**	0.1	0.1	0.0	**1.7 ↑**	0.0	0.4
	Privacy lawyer	0.6	1.4	0.2	0.5	0.3	0.3	**2.0 ↑**	1.0	0.2	0.2	1.8	0.8	0.2
	Cybersecurity	0.5	0.4	0.1	0.2	0.3	0.0	**3.9 ↑**	0.2	0.2	0.2	1.9	**2.3 ↑**	0.1
	Data protection officer	0.4	0.9	0.1	0.2	0.2	0.1	**2.1 ↑**	0.4	0.1	0.2	**1.8 ↑**	0.1	0.1
	Privacy manager	0.3	1.3	0.0	0.0	0.0	0.0	**2.0 ↑**	0.5	0.0	0.0	**1.7 ↑**	0.0	0.2
	Privacy analyst	0.4	0.7	0.0	0.1	0.0	0.2	**3.5 ↑**	0.2	0.0	0.2	**1.8 ↑**	0.1	**2.0 ↑**
	AI governance professional	0.2	0.9	0.0	0.0	0.0	0.0	**2.1 ↑**	0.3	0.0	0.0	**1.7 ↑**	0.0	0.3

The majority of privacy functions tended to vest accountability internally, however organizations with less than 100 employees or under USD100 million in annual revenue notably outsourced senior roles accountable for privacy.

The lack of resources limits the ability to deliver on objectives



Confidence in compliance with privacy laws and policies across jurisdictions by respondent's perception of whether the limited availability of the right skills or resources impacts their organization's ability to deliver on its objectives

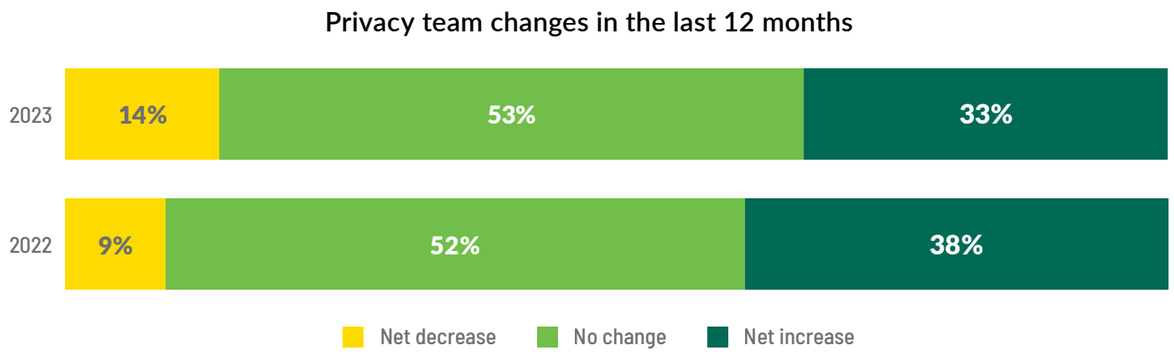


Doing more, with not enough

Given the importance of getting the right individuals with the right skills on the team, we sought to further understand respondent's perceptions of whether lack of resources impacts the ability to deliver on objectives.

In this year's survey, 63% of respondents agreed the limited availability of resources within their organization impacts its ability to deliver on privacy objectives. These results are similar to the 2022 survey, in which 62% of respondents agreed with the same statement. This trend persists regardless of the size of organization and rises to 76% for organizations with more than 80,000 employees. In Europe, a greater proportion of respondents, six in 10 compared to five in 10 in 2022, identified the limited availability of privacy resources impacts their ability to deliver on objectives. The challenges also persist by sector. In the consumer goods, services and retail sector, 78% of respondents agreed the limited availability of privacy resources impacts their ability to deliver on objectives.

One area where a lack of resources could have impact is an organization's ability to stay compliant with its privacy compliance obligations. Eight in 10 respondents who were not at all confident in their organization's ability to comply were dissatisfied with the availability of resourcing to meet objectives. Conversely, respondents who were totally confident in their organization's ability to remain compliant with privacy obligations were more likely to find its resourcing sufficient to meet objectives.

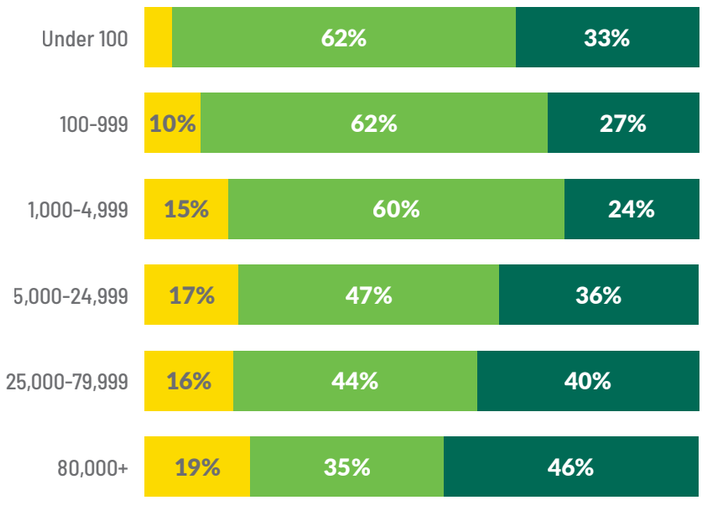


Growing privacy functions

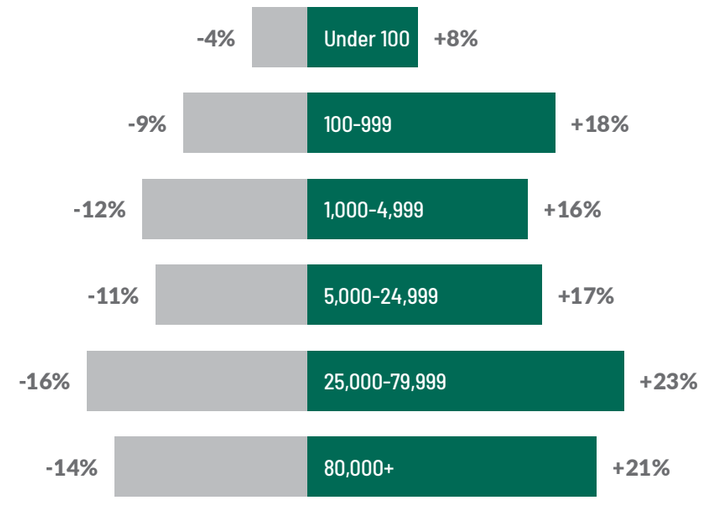
Privacy teams continue to evolve to meet the ever-growing list of privacy compliance requirements, from the GDPR to the California Consumer Privacy Act to China's PIPL to India's DPDPA. There's no pressing pause on the variety of privacy laws and requirements privacy pros need to contend with. At the same time, like many other areas of the organization, they are subject to the broader economic headwinds and trends impacting recruitment and headcount across the industry. In 2022, respondents identified their privacy teams grew by 12% on average. The 2023 survey, therefore, looked at the extent to which privacy teams grew or shrunk over the last 12 months and compared this to the 2022 survey results.

Overall, the average growth of privacy teams was less than in 2022. In 2023, the average privacy team grew by 6%, half of its growth in 2022. There was also a small increase of 5% in the proportion of respondents who reported their privacy functions had a net decrease in size over the previous 12 months.

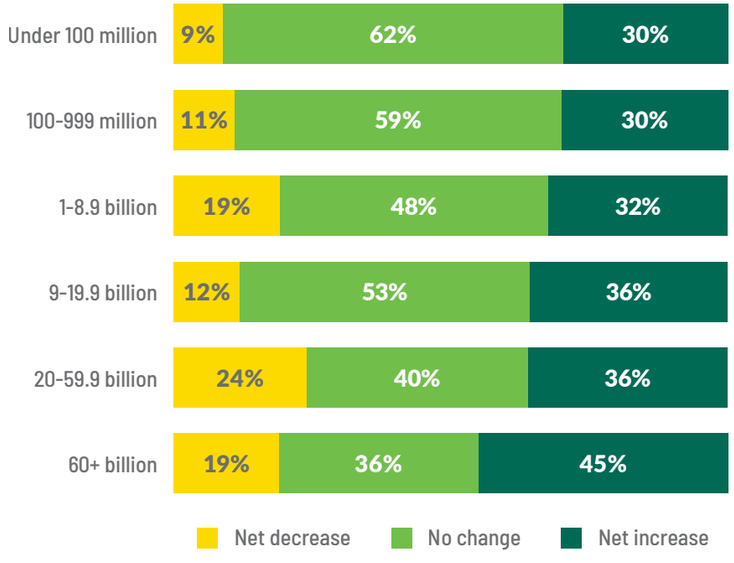
Privacy team changes in the last 12 months by number of employees



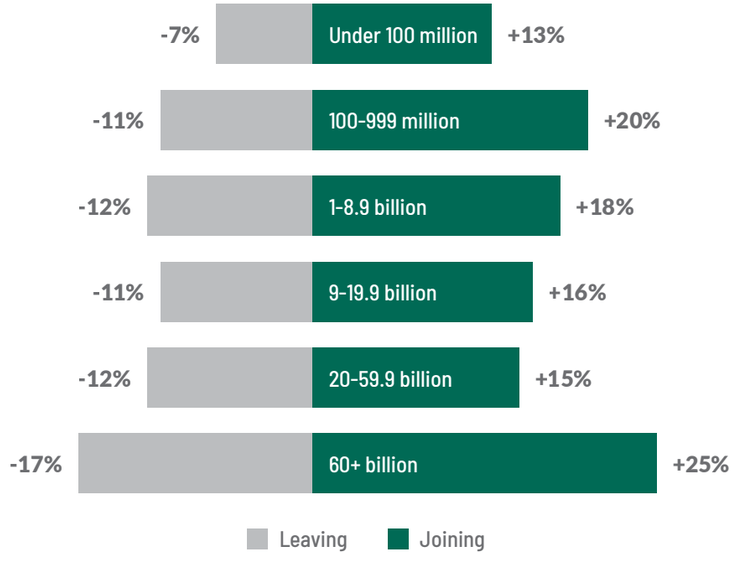
Percent joining and leaving in last 12 months by number of employees



Privacy team changes in the last 12 months by annual revenue in USD



Percent joining and leaving in last 12 months by annual revenue in USD

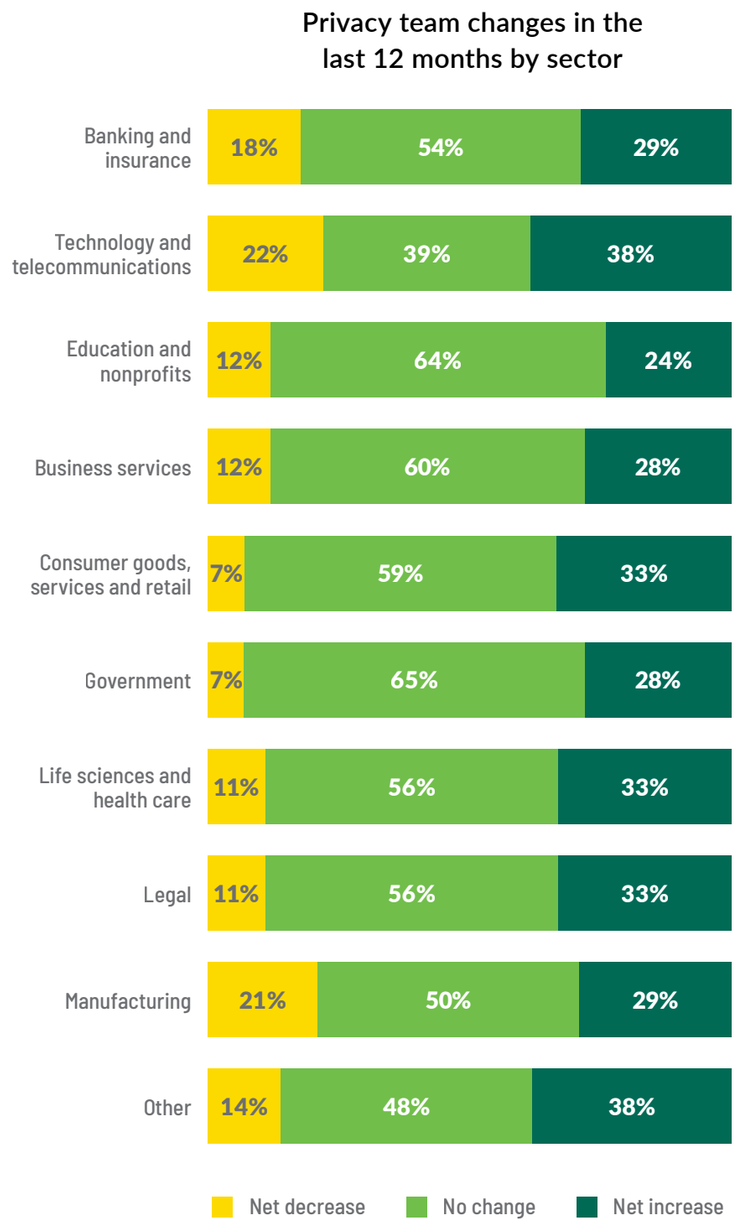


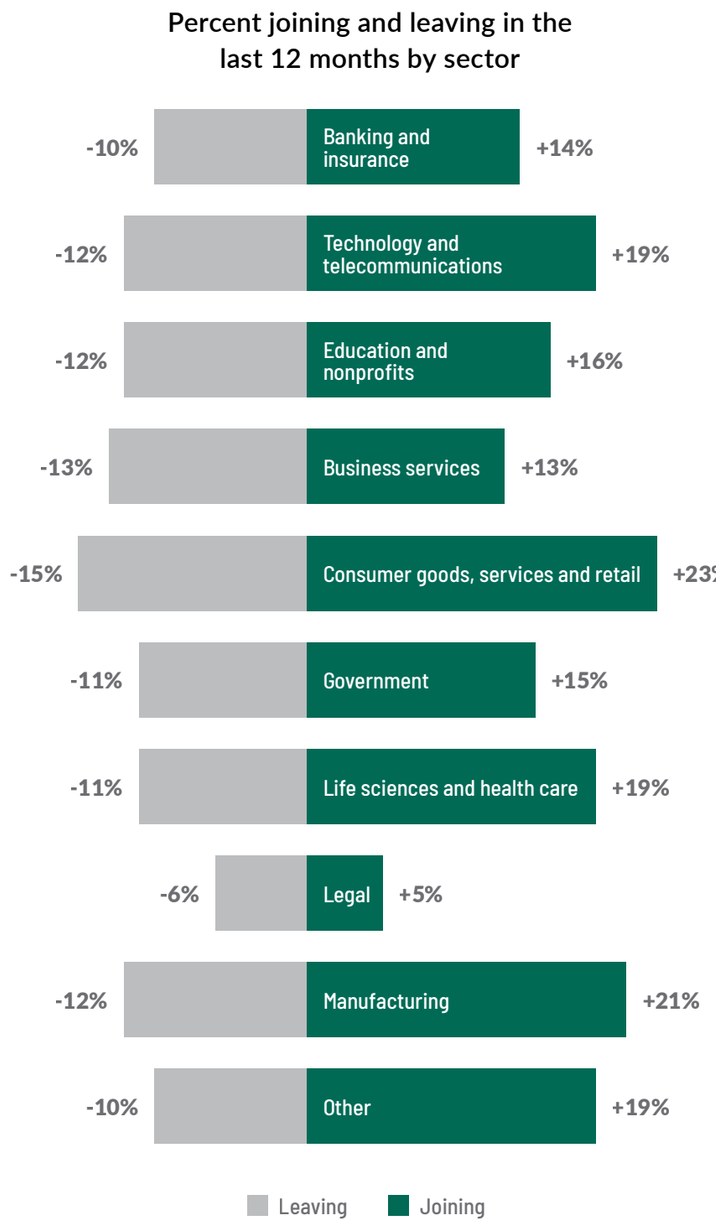
When considering organizations by size, respondents working for the largest organizations by number of employees or by annual revenue were most likely to be part of teams that went through changes in size. Organizations with annual revenues of more than USD60 billion had the greatest turnover, seeing on average 17% of staff departing and 25% being newly hired. Only those working in organizations with revenue between USD101-999 million saw greater net change, at an average of 9% growth.

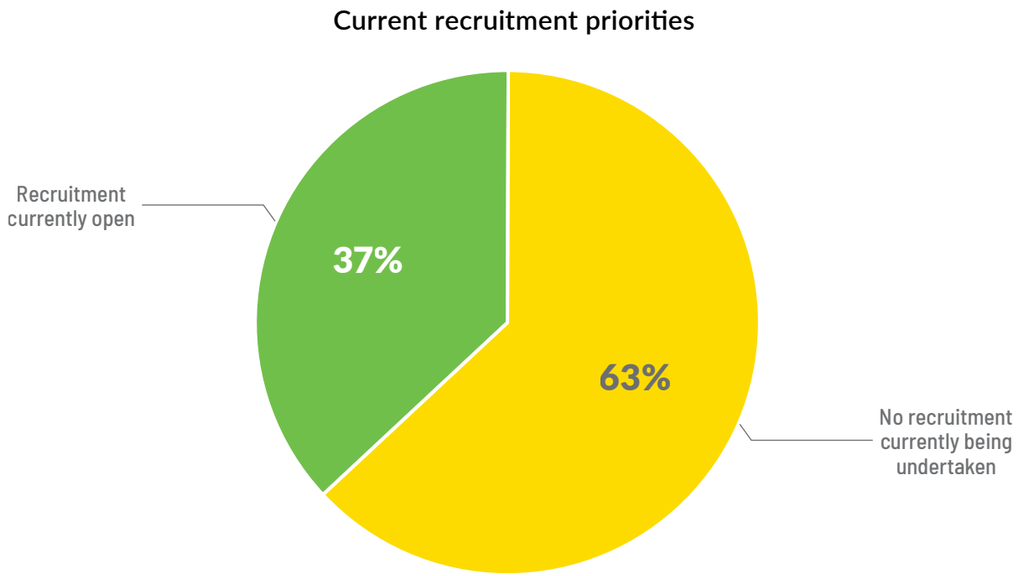
Respondents working in privacy functions at smaller organizations, those with less than 4,999 employees or with less than USD999 million in revenue, were more likely to report the size of their privacy team did not change over the last 12 months. Respondents working in organizations with more than 5,000 employees were most likely to experience above average growth in their privacy teams, at more than 6%.

Respondents across the majority of sectors identified their privacy team grew in in size. The largest net increases were reported by privacy functions in manufacturing, at 9% increase, and the consumer goods, services and retail and life sciences and health care sectors, both at 8%.

On the other hand, respondents from the business services sector reported no net change, with 13% of employees on average joining and leaving their company in the last 12 months. Respondents in the legal sector reported a 1% decrease in team size on average, with 6% leaving and 5% joining overall. Respondents working in the government and education and nonprofit sectors experienced the most stability, with the highest proportion of respondents, at just over six in 10, reporting their privacy team had no change in staffing over the previous 12 months.







Future talent pipeline

As privacy teams expand and the privacy profession matures, organizations may look to diversify their benches by hiring more privacy specialists. The 2022 survey highlighted how organizations looked to hire privacy risk and compliance experts, privacy engineers, and privacy champions. Recruitment strategies that balance the need for future talent with broader economic challenges are as important as ever this year. With this in mind, we sought to understand the types of roles privacy functions are recruiting for.

Overall, over six in 10 respondents identified their organization is not currently recruiting privacy resources. When viewed by organizational size, five in 10 respondents working for organizations with more than 25,000 employees identified their company is open to recruitment. This rose to almost seven in 10 respondents at organizations with 80,000 employees or more. By revenue, seven in 10 respondents working for organizations with less than USD999 million in annual revenue said their organizations are not recruiting. At least six in 10 respondents working for organizations with more than USD20 billion in annual revenue said their organizations are still recruiting.

Percentage of respondents currently recruiting for each privacy role

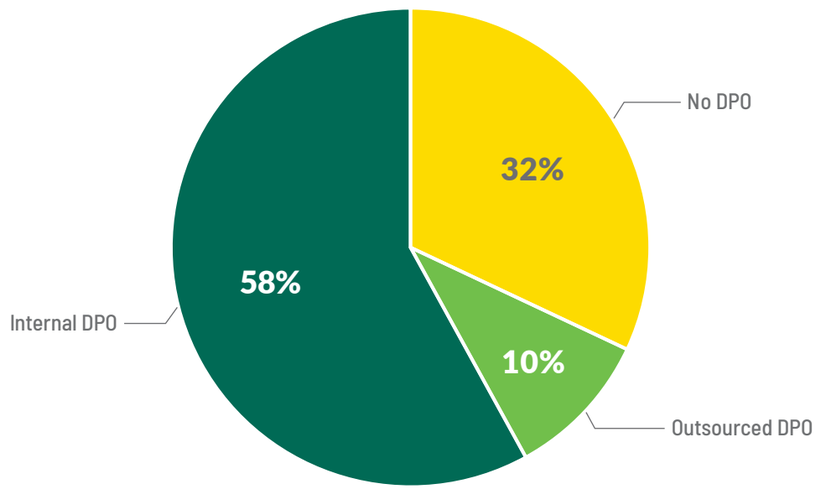
Of respondents who identified their organizations are recruiting, privacy analysts were the most popular role, identified by just over three in 10 respondents. This was followed closely by privacy manager, internal privacy lawyer and privacy engineer.

Part VI.
The year of the DPO

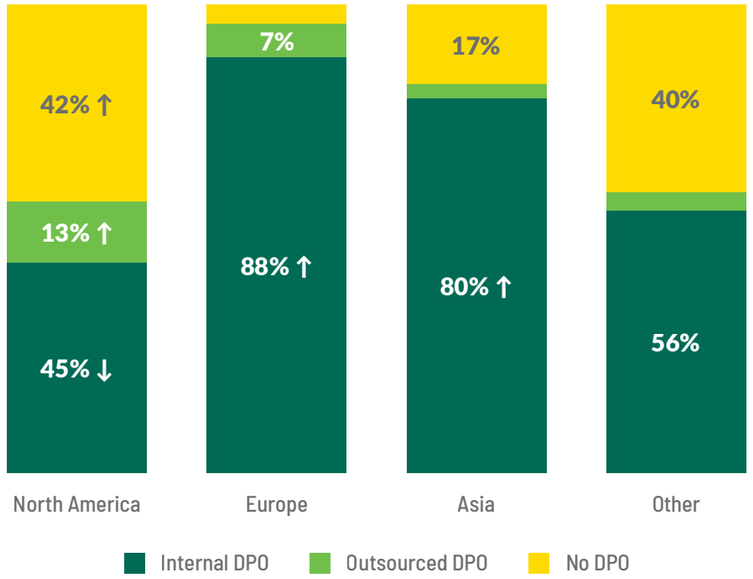
Of respondents at organizations with a DPO, 70% are confident in their compliance efforts, compared to only 30% of those without a DPO.

At the beginning of the year, the European Data Protection Board announced its 2023 coordinated enforcement action would focus on the role of the GDPR DPO. Specifically, data protection authorities across Europe will investigate whether organizations have appointed DPOs — where mandated by GDPR Articles 37-39 — and are sufficiently supporting them with enough resources to fulfil their work. IAPP research puts the number of DPO registrations in Europe at more than 700,000. Combined with the GDPR's fifth anniversary, it was time to explore what this role looks like in the typical privacy function.

Existence of DPO in an organization

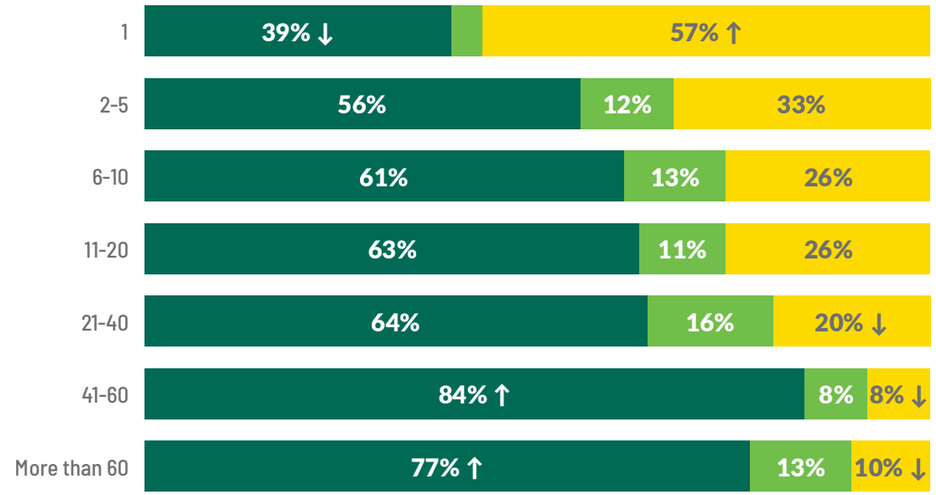


Existence of DPO by continent

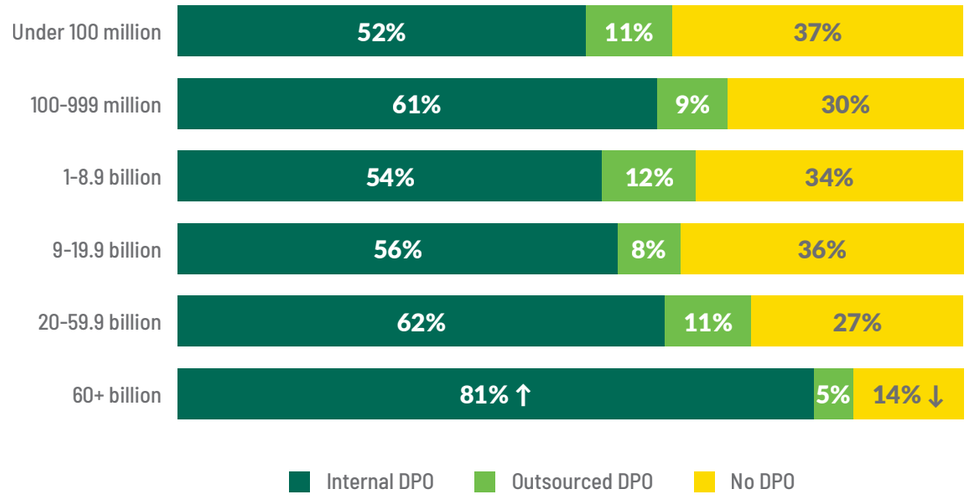


Approximately 68% of respondents reported their organization has at least one DPO, though this percentage varies heavily depending on the location in which it operates. In Europe, 96% of respondents reported their organization has a DPO, compared to just 58% in North America. Additionally, the more countries in which an organization operates, the more likely it is to have a DPO. Only 43% of organizations that operate in one country have a DPO, compared to 90% of those that operate in more than 60 countries. Most DPOs are internal to the organization, as only 10% of surveyed respondents reported their organization relies on an outsourced DPO. When looking at both revenue and number of employees, this percentage stays rather consistent, meaning the size of an organization has little effect on whether it chooses to outsource its DPO.

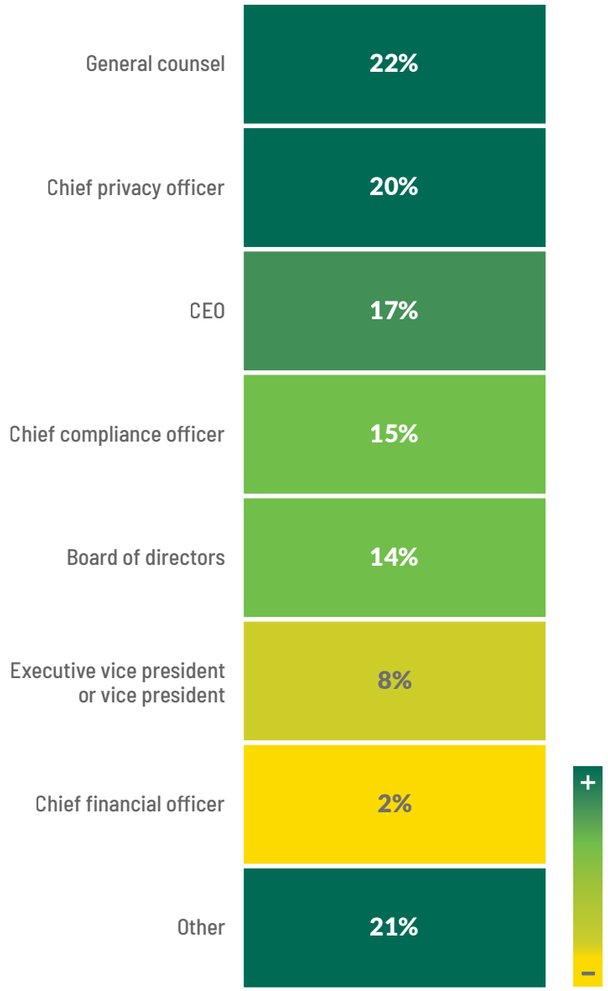
Existence of DPO by number of countries where a company operates



Existence of DPO by annual revenue in USD



Who does the DPO report to?



DPO reporting line by continent

DPO REPORTING LINE	Overall	CONTINENT			
		North America	Europe	Asia	Other
General counsel	22%	25%	18%	10%	24%
Chief privacy officer	20%	28% ↑	8% ↓	17%	17%
CEO	17%	8% ↓	29% ↑	28%	21%
Chief compliance officer	15%	12%	16%	28% ↑	17%
Board of directors	14%	10% ↓	23% ↑	7%	10%
Executive vice president or vice president	8%	9%	5%	14%	10%
Chief financial officer	2%	1%	5%	3%	0%
Other	21%	19%	22%	17%	28%

When it comes to the reporting line of DPOs, there is no standout approach. Reporting to general counsel is the most common, at 22%, followed closed by the CPO, at 20%. Location matters, however. In North America, it is most common for DPOs to report to the CPO whereas in Europe, reporting to the CEO is most common, likely due to the GDPR DPO reporting and independence requirements. In Asia, it is most common for DPOs to report to the chief compliance officer. This points to the differing role of the DPO depending on jurisdiction, as well as the difference in organizational structures between continents.

The existence of a DPO within an organization significantly affects confidence in its ability to maintain compliance with privacy laws and regulations. Approximately, 70% of respondents working at organizations with a DPO are at least somewhat confident in their compliance efforts, compared to only 30% of those at organizations without one. In other words, organizations feel more compliant — perhaps because they are — when they have a DPO.

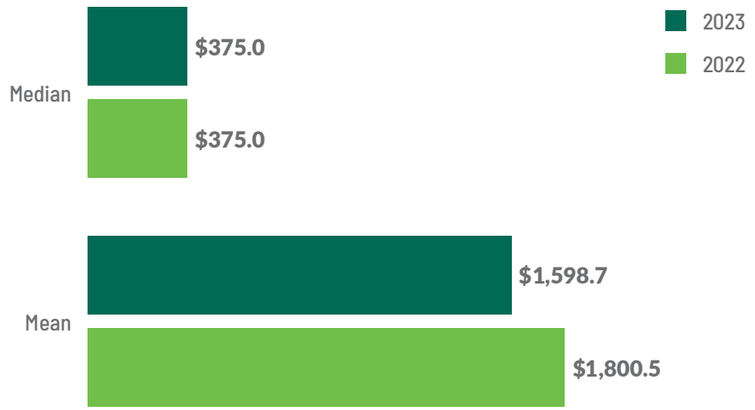
Our examination of the role of the DPO highlights that it is still a crucial part of a privacy governance program. While the EU and more than two dozen other jurisdictions legally require organizations to have an assigned DPO or similar role, organizations outside of those jurisdictions may realize benefits by appointing one. Organizations could feel more confident in their ability to keep pace with compliance efforts and have less trouble communicating privacy efforts to the board due to the DPO's proximity. The appointment of a DPO can also be a sign to customers the organization takes data protection seriously, possibly increasing goodwill and public reputation. In short, DPOs shine in a year marked by efficiency and doing more with less.

Part VII. Budgeting

While the 2023 average mean privacy budget, USD1,598,729, is down compared to 2022, the median privacy budget, USD375,000, remained identical.

Nearly every organization is facing economic headwinds, with factors such as inflation, rising interest rates and layoffs causing budget and resource strain. These are important factors to keep in mind when looking at historical budget data. Even organizations fortunate enough to realize a moderate increase in their average privacy budget may not feel as though they received an increase when economic conditions are factored in. For this reason, both the mean and median budget numbers for 2023 are included in this report.

Median and mean average overall privacy budgets (USD $000) in 2023 versus 2022



The average privacy budget

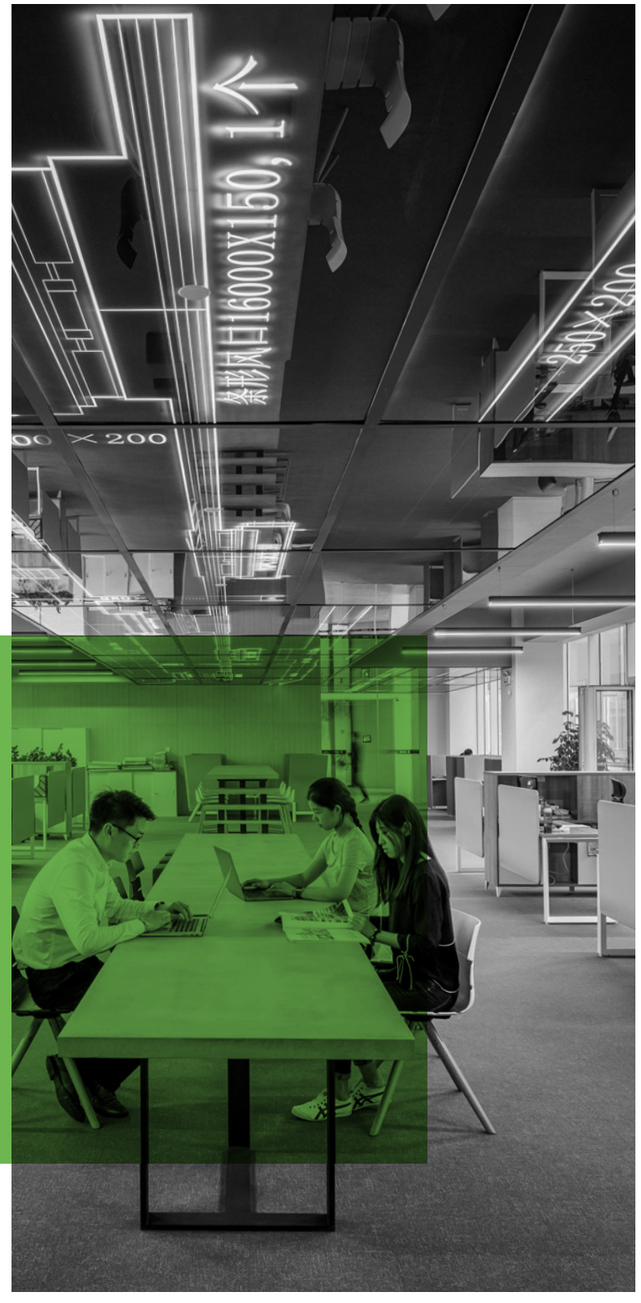
The average mean privacy budget for 2023 is USD1,598,729, down from USD1,800,530 in 2022. The median privacy budget for 2023 is USD375,000, which is the same as it was in 2022. Taken together, the budgets for most privacy functions reflect the weakened economy in 2023.

In looking at the average budget by sector, some have significantly higher budgets. The technology and telecommunications sector had an average mean privacy budget of USD2,692,105, more than a million dollars higher than the 2023 average. Organizations in the consumer goods, services and retail sector had an average mean privacy budget of USD3,785,185, which is impressively more than USD2 million above the overall average. Additionally, both sectors have increased privacy budgets compared to last year. These sectors comprise organizations that performed well despite economic conditions, which may partially explain their uncharacteristic budget sizes compared to the average.

The boost in budgets for technology and telecommunications organizations could also be in response to the increasing regulatory burden of handling, processing and transferring consumer data, with a number of organizations subject to consequential enforcement in 2023 due to GDPR violations. Remedying these requires a myriad of resources directed at privacy teams. Paired with the increased investment in AI governance and deployment, it becomes clear that technology companies in particular need budgets commensurate to the consequential nature of privacy enforcement and regulatory scrutiny. In contrast, budgets for the banking and insurance, life sciences and health care, legal, and manufacturing sectors are all down, most likely due to the current economic climate. Legal suffered the least, with the average mean budget shrinking by around USD150,000. The average manufacturing firm suffered the worst, shrinking by around USD2 million.

Median and mean budgets (USD $000) by sector in 2022 versus 2023

SECTOR	YEAR	MEDIAN	MEAN
Overall	2022	$375.0	$1,800.5
	2023	$375.0	$1,598.7
Banking and insurance	2022	$375.0	$1,935.6
	2023	$750.0	$1,520.4
Technology and telecommunications	2022	$750.0	$2,392.3
	2023	$750.0	$2,692.1
Education and non-profit	2022	$225.0	$1,214.6
	2023	$175.0	$1,390.5
Business Services	2022	$175.0	$1,468.4
	2023	$225.0	$1,585.0
Consumer goods, services and retail	2022	$375.0	$1,930.1
	2023	$1,250.0	$3,785.2
Government	2022	$225.0	$1,443.5
	2023	$375.0	$1,795.4
Life sciences and health care	2022	$750.0	$1,781.9
	2023	$375.0	$1,257.1
Legal	2022	$50.0	$390.1
	2023	$225.0	$230.6
Manufacturing	2022	$300.0	$2,869.5
	2023	$375.0	$830.2
Other	2022	$375.0	$1,821.3
	2023	$375.0	$1,062.2



Median and mean budgets (USD $000)
by total number of employees in 2022 versus 2023

NUMBER OF EMPLOYEES	YEAR	MEDIAN	MEAN
Overall	2022	$375.0	$1,800.5
	2023	$375.0	$1,598.7
Under 100	2022	$50.0	$241.3
	2023	$50.0	$1,427.6
100-999	2022	$125.0	$265.1
	2023	$175.0	$494.6
1,000-4,999	2022	$375.0	$661.8
	2023	$375.0	$696.4
5,000-24,999	2022	$375.0	$1,427.6
	2023	$750.0	$1,196.6
25,000-79,999	2022	$1,750.0	$2,797.2
	2023	$1,250.0	$4,140.4
80,000+	2022	$2,250.0	$8,039.3
	2023	$1,750.0	$5,215.7

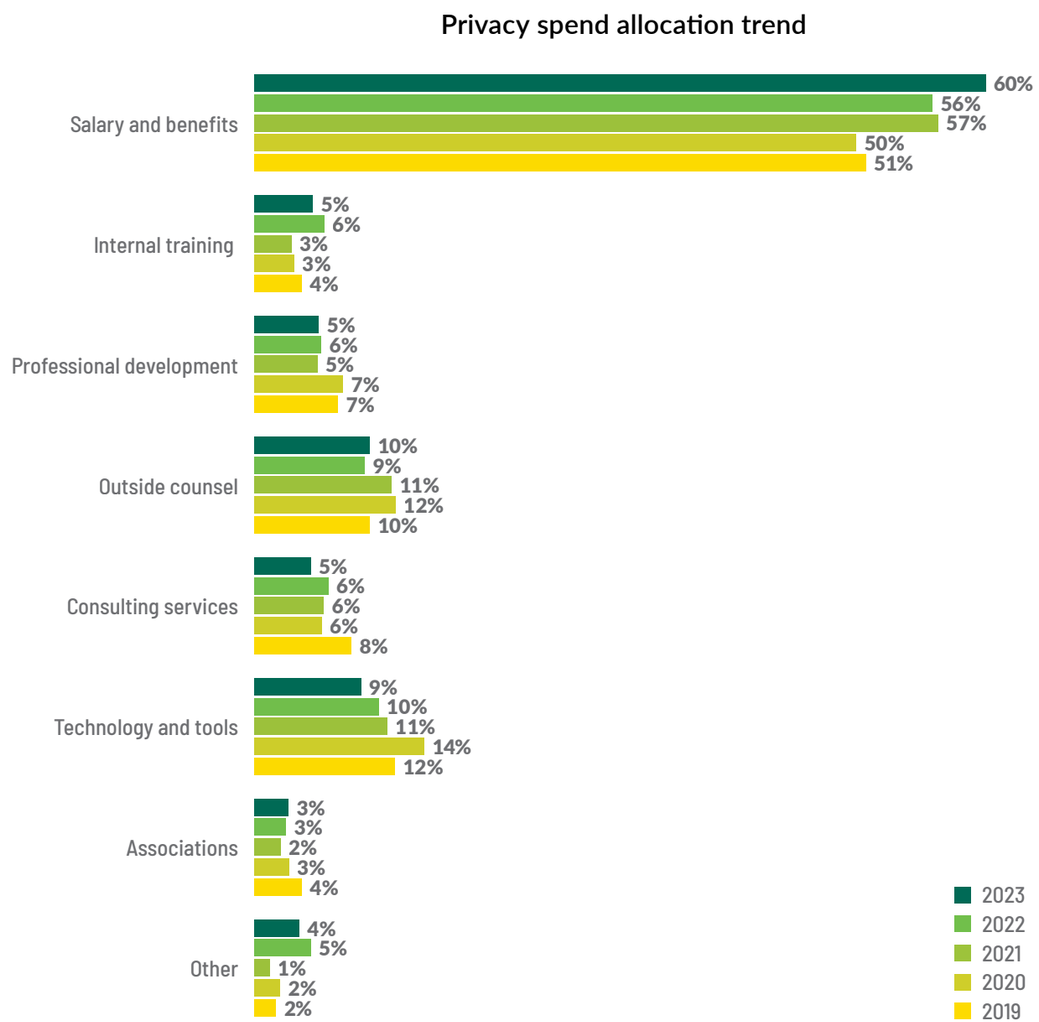
Generally speaking, companies with fewer employees saw privacy budget increases compared to 2022. Companies with less than 5,000 employees, on average, saw an increase in their mean privacy budgets in 2023, whereas companies with 5,000-24,999 employees and more than 80,000 employees saw their budgets decrease. Significantly, no respondents in organizations with more than 80,000 employees indicated having a privacy budget of more than USD50 million this year, compared to 7% of these organizations in 2022.

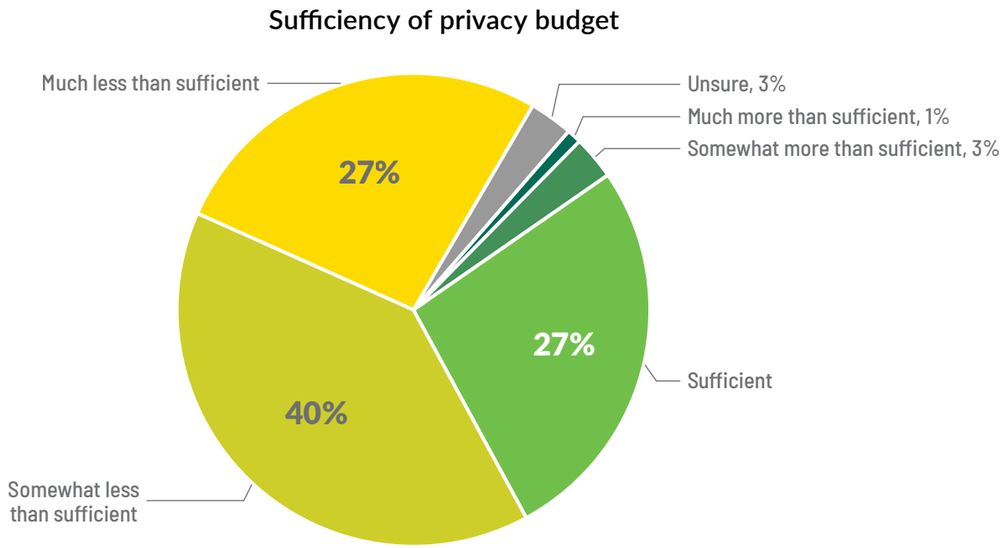
How is it allocated?

Additionally, like in 2022, we asked respondents how their organizations allocated this budget. As expected, the majority is allocated to salary and benefits. In fact, the percentage allotted to salary and benefits increased significantly this year, from 56% in 2022 to 60.4% in 2023. This aligns with conclusions from the 2023 IAPP Privacy Professionals Salary Survey in that the average privacy pros salary rose by 7% from 2022 to 2023. In decreases, the amount allotted to consulting services went from 6.1% in 2022 to 4.7% in 2023, and the amount for technology and tools went from 10.3% in 2022 to 8.8% in 2023. Other components stayed relatively consistent compared to years past.

There were some significant increases in organizational revenue compared to 2022, for the percentage of budget allotted or salary and benefits, with organizations generating USD101 million-USD8.9 billion in revenue. There was a similar significant increase for organizations with between 100 and 24,999 employees. In short, privacy budgets seem to be most beneficial for individual privacy pros at organizations in the "middle of the pack." There were similar significant allotment decreases across the board for consulting services, technology and tools.

Overall, these results reinforce the notion that organizations are increasing spending for recruitment purposes. While the money for salary and benefits must be taken from somewhere, the decrease for technology and tools is also likely due to the decreased cost of such tools, especially as AI integration makes things more efficient.





Is it sufficient?

Finally, respondents described their company's privacy budget with respect to organizational obligations: 67% indicated the budget is less than sufficient and only 27% stated it is sufficient. Again, this reflects the poor state of the economy, with budgets generally tightened across the organization and privacy pros finding themselves responsible for an increasing spread of activities. Leaders who find their privacy budget insufficient should determine the best way to bring the case for a larger budget to higher-ups in the organization. For example, implementing governance systems that provide quantitative metrics may make a case more persuasive.

On average, organizations experiencing negative team churn — that is, losing more people than they hired — were more likely to describe their privacy budget as insufficient than those with zero or positive team churn. On the other hand, organizations with positive team churn were significantly more likely to identify their budgets as somewhat more than sufficient. In other words, a likely factor for a dwindling privacy function is an insufficient budget to properly pay or otherwise support the function.

Since the economic climate may remain fraught for a while, privacy pros may want to focus on refining their governance functions in an effort to make them more efficient and effective. Teams dealing with new tasks, like AI governance, may be able to leverage this to request additional resources from leadership.

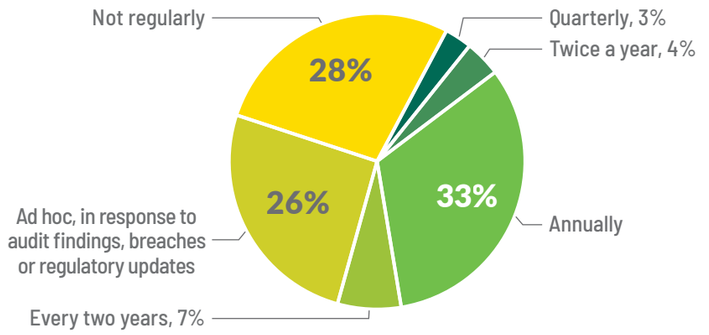
Part VIII. Emerging risk management

Organizations continue to proactively identify potential risks and challenges that could impact business objectives and/or individual's privacy risk.

Effective organizational privacy risk management can help manage adverse legal and regulatory consequences, protect business reputation, and support business continuity efforts. Organizations that balance individual privacy risk against organizational privacy risk management may further demonstrate trust in their brand's ability to safeguard personal data and advocate for its ethical use.

This year's survey further explores the approach organizations take to organizational privacy risk management, both through enterprise risk-management efforts and PIAs. We also sought to further understand the approach to technology-enabled compliance and approaches to third-party risk management.

Frequency of enterprise-wide or business-unit-wide privacy compliance risk assessments



Enterprise privacy risk management

Respondents identified PIAs and PbD as the top priorities for 2023. With this in mind, it is important to explore how organizations are currently tackling enterprise privacy risk management and what further work may be envisaged in this area.

Almost four in 10 respondents identified their organizations undertake enterprise-wide privacy compliance risk assessments once annually, twice a year or quarterly. On the other hand, 28% of respondents indicated their organizations do not undertake regular enterprise risk assessments, while 26% identified these may only be triggered in response to key events such as audit findings, data breaches or changes in regulatory requirements. The majority of respondents indicated their organizations do not undertake regularly scheduled enterprise-wide privacy compliance risk assessments.

By sector, respondents in banking and insurance, technology and telecommunications, and business services said their organizations were more likely to undertake enterprise risk assessments annually than not. At least two out of 10 respondents in each sector identified their organizations only undertook enterprise privacy risk assessments in response to various triggers.

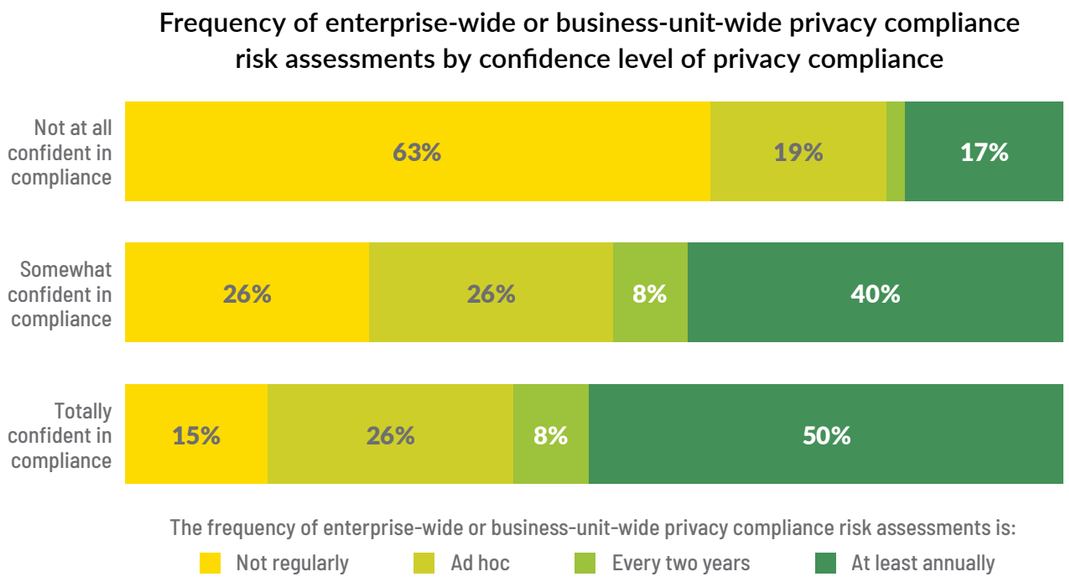
Frequency of enterprise-wide or business-unit-wide privacy compliance risk assessments by sector

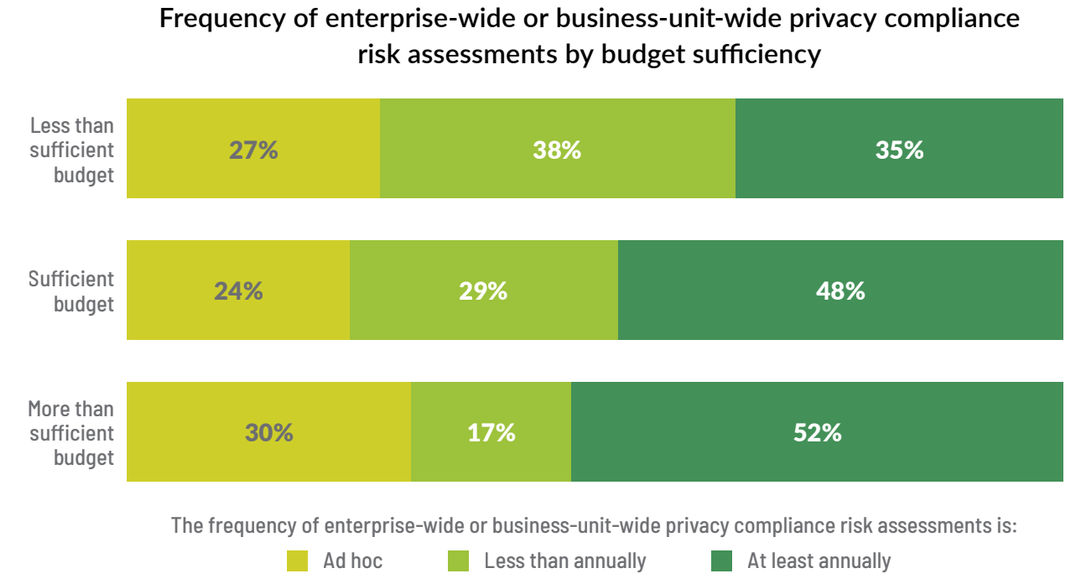
		SECTOR									
FREQUENCY	Overall	Banking and insurance	Technology and telecommunications	Education and nonprofit	Business services	Consumer goods, services and retail	Government	Life sciences and health care	Legal	Manufacturing	Other
Not regularly	28%	17% ↓	22%	44% ↑	20%	37%	31%	31%	22%	29%	29%
Every two years	7%	9%	4%	2%	12%	7%	7%	6%	11%	13%	9%
Less than annually	35%	26%	26%	46%	32%	44%	39%	37%	33%	42%	38%
Annually	33%	43% ↑	41%	28%	36%	19%	19% ↓	29%	33%	17%	34%
Twice a year	4%	6%	8% ↑	2%	0%	4%	6%	0%	0%	4%	2%
Quarterly	3%	1%	5%	0%	8%	7%	0%	1%	0%	8%	4%
At least annually	40%	50% ↑	54% ↑	30%	44%	30%	24% ↓	30%	33%	29%	40%
Ad hoc, in response to audit findings, breaches or regulatory updates	26%	24%	20%	24%	24%	26%	37% ↑	33%	33%	29%	22%

Frequency of enterprise-wide or business-unit-wide privacy compliance risk assessments by number of employees and total annual revenue in USD

		NUMBER OF EMPLOYEES						REVENUE					
FREQUENCY	Overall	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+	Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
Not regularly	28%	26%	29%	32%	31%	23%	7% ↓	28%	31%	32%	22%	20%	12% ↓
Every two years	7%	3%	7%	6%	9%	7%	11%	3%	6%	4%	17% ↑	11%	17% ↑
Less than annually	35%	28%	36%	38%	40%	30%	19%	31%	37%	37%	39%	31%	29%
Annually	33%	41%	35%	29%	29%	28%	44%	37%	33%	32%	29%	22%	40%
Twice a year	4%	3%	4%	2%	3%	7%	6%	3%	4%	2%	3%	11% ↑	5%
Quarterly	3%	3%	4%	4%	1%	7%	2%	3%	5%	1%	0%	7%	2%
At least annually	40%	46%	44%	35%	33%	42%	52% ↑	43%	41%	35%	32%	40%	48%
Ad hoc, in response to audit findings, breaches or regulatory updates	26%	26%	20%	27%	27%	28%	30%	26%	22%	28%	29%	29%	24%

When considering organizational size, there is a similar theme across both revenue and number of employees. Respondents working in organizations with less than USD999 million in annual revenue or less than 999 employees and those working in organizations with more than USD20 billion in annual revenue or 25,000 employees identified their organizations undertake enterprise privacy compliance risk assessments at least annually. Those who work at organizations that operate in more than 20 countries also identified their organizations conduct enterprise privacy compliance risk assessments at least annually.



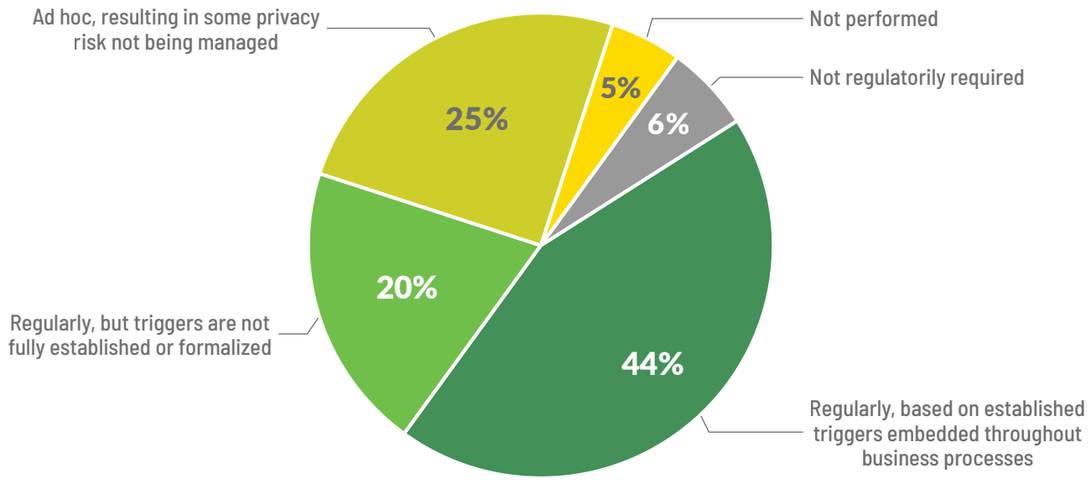


The trend, when considering confidence in compliance, is stark. Respondents who said they are totally confident in their organization's privacy compliance capabilities are more likely to work in organizations that undertake enterprise privacy compliance risk assessments at least annually. Those working in organizations that do not regularly undertake enterprise privacy compliance risk assessments were more likely to say they have no confidence their organization's level of privacy compliance.

One reason for varying approaches may be the cost of enterprise privacy compliance risk assessments.. Those who identified their company's budgets were more than sufficient were more likely to work for organizations that conduct enterprise privacy compliance risk assessments at least annually. In contrast, those who identified their company's budgets were less than sufficient were more likely to work for organizations that undertake enterprise privacy risk assessments on a less than annual basis.

Those with total confidence in their organization's privacy compliance are more likely to work in organizations that undertake enterprise privacy compliance risk assessments at least annually.

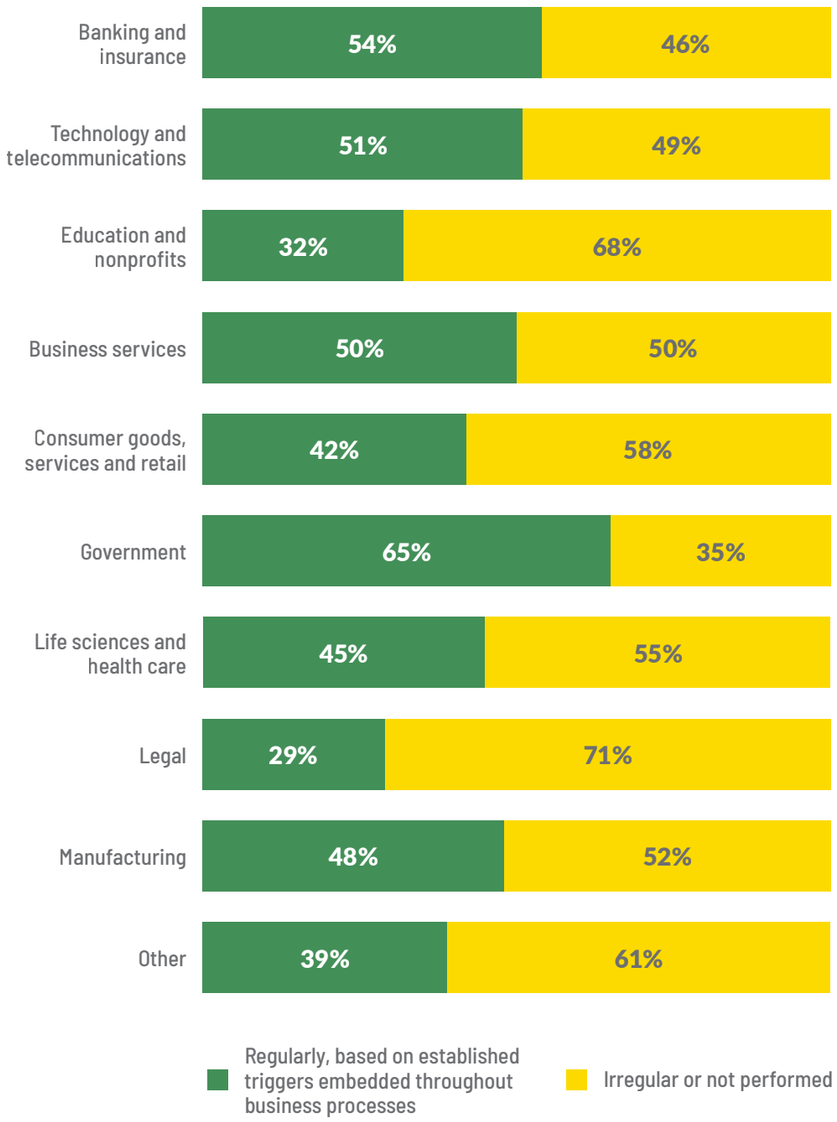
Privacy impact assessment frequency by sector



Almost eight years ago, the IAPP sought to understand the extent to which organizations were using PIAs. With the GDPR just around the corner, it seemed like a timely exercise in understanding organizational readiness for a key tool and process in every privacy practitioner's toolkit. In 2015, six in 10 respondents identified their organizations used PIAs and, of these respondents, a further six in 10 identified PIAs were part of the software development life cycle process.

Fast forward to 2023, almost nine in 10 respondents said their company uses PIAs. However, one in four respondents disclosed that their organization conducts PIAs in an ad-hoc manner. A further two in 10 said, while their organizations conduct PIAs, the triggers are not fully established or formalized, suggesting there may be instances where the PIA process does not occur effectively for these organizations. Almost five in 10 respondents suggested their PIA processes are not fully established or working effectively to manage risk.

Privacy impact assessment frequency by sector, excluding respondents who identified that PIAs were not a regulatory requirement

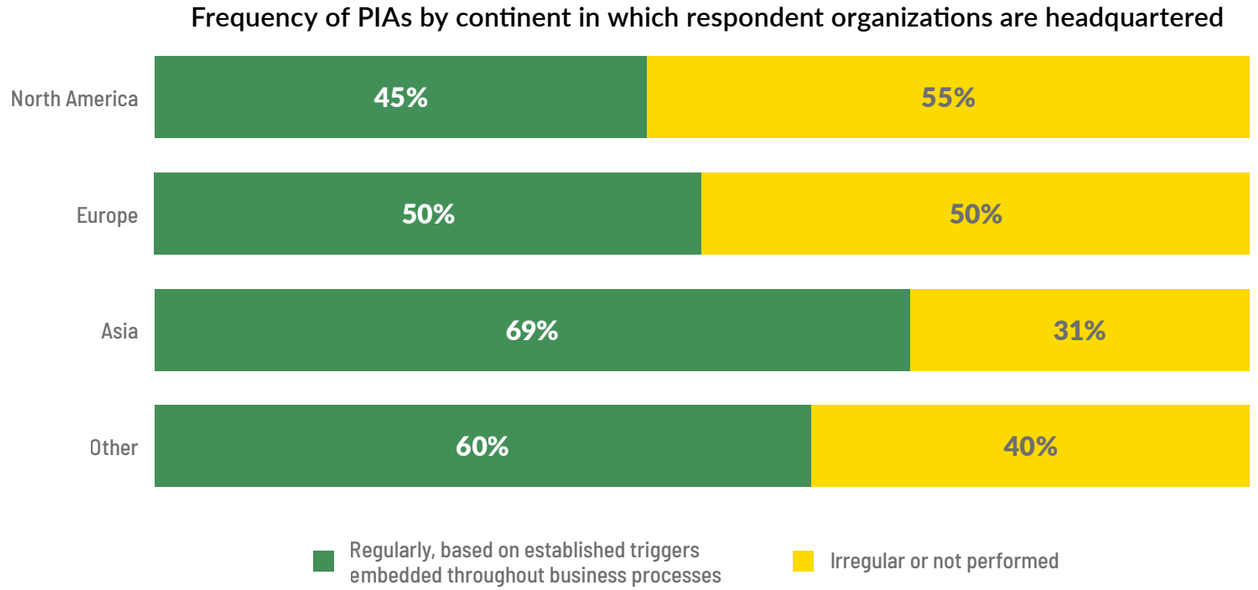


Privacy impact assessment frequency by sector

FREQUENCY	Overall	SECTOR: 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
Regularly, based on established triggers embedded throughout business processes	44%	47%	49%	30% ↓	48%	41%	65% ↑	41%	22%	42%	37%
Regularly, but triggers are not fully established or formalized	20%	22%	22%	12%	8%	15%	17%	19%	22%	17%	27% ↑
Ad hoc, resulting in some privacy risk not being managed	25%	13% ↓	24%	40% ↑	36%	33%	15%	29%	33%	25%	27%
Not performed	5%	6%	0% ↓	12% ↑	4%	7%	4%	4%	0%	4%	5%
Not regulatorily required	6%	12% ↑	5%	6%	4%	4%	0% ↓	7%	22% ↑	13%	3%

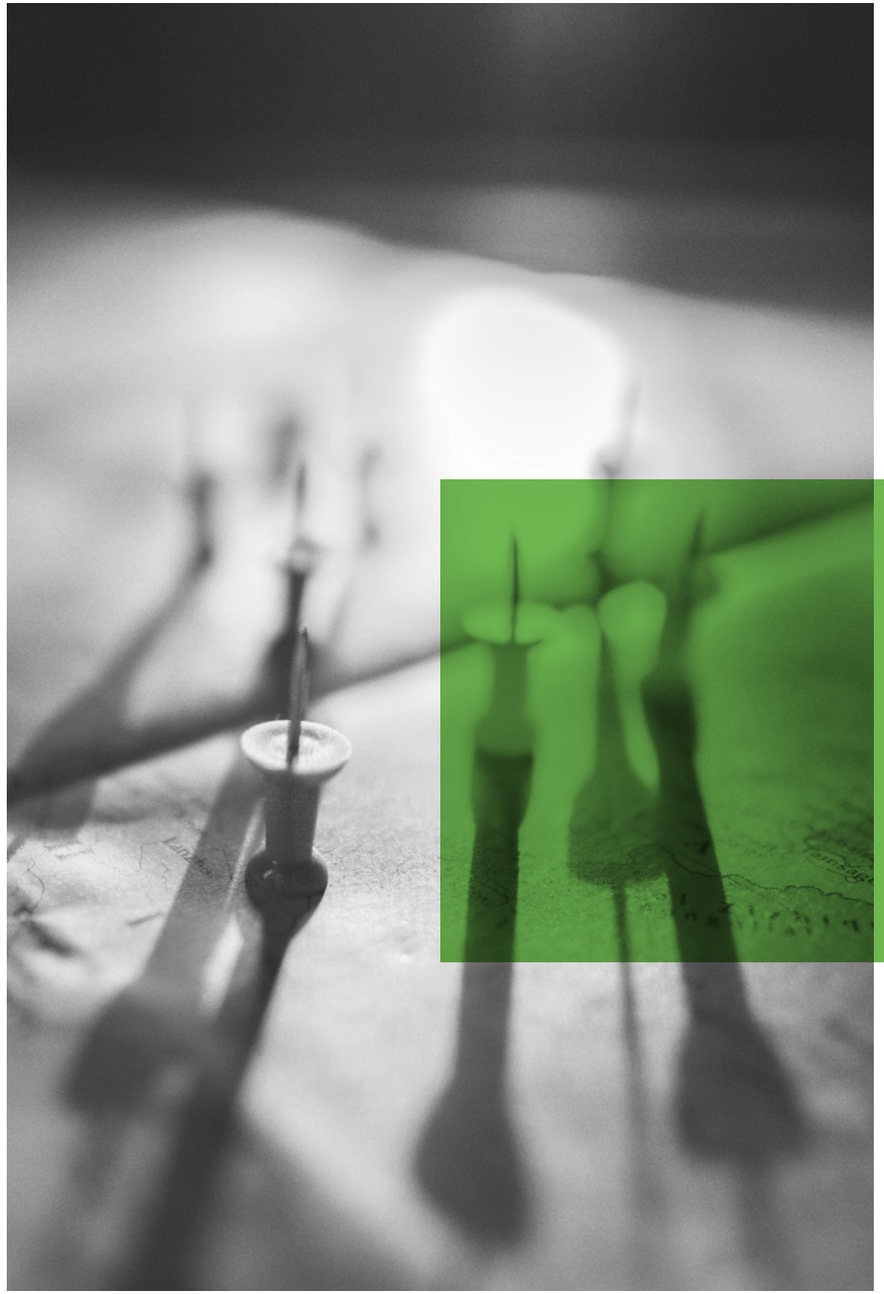
A similar trend exists when considering the breakdown by sector: 65% of respondents working in the government sector identified their organizations had established PIA processes.

Organizations subject to regulatory requirements in the banking and insurance and technology and telecommunications sectors, alongside government organizations, were more likely to undertake PIAs in an established manner. Respondents across the remaining sectors were more likely to identify their organizations either do not have fully established PIA process, conduct PIAs in an ad-hoc manner or do not perform PIAs. Respondents in the education and nonprofit sector were among the most likely to work for organizations that have yet to fully establish a PIA process. Only three in 10 respondents identified their organization conducted PIAs regularly based on established triggers. The same trend of regular versus irregular performance of PIAs persists across sectors when we further exclude those who identified PIAs are not performed at their organization alongside those who said PIAs are not a regulatory requirement.



The difference in regulatory environment could also drive the extent to which PIA processes are established and operating effectively.

When considering headquarters locations, PIAs are still not performed regularly in markets like Europe, where requirements for data protection impact assessments and PbD has been formalized through regulation. For this analysis, respondents who selected their organizations are not required to conduct PIAs by regulation and those who identified they are not performed because privacy risk is not high enough within the data processing environment are excluded. Only five in 10 respondents working for organizations headquartered in Europe identified their organization regularly conducts PIAs based on established triggers. This figure drops to 45% when considering organizations headquartered in North America. Organizations headquartered in Asia led the pack, with 69% of respondents identifying that their organizations regularly conduct PIAs based on established triggers.



Privacy impact assessment frequency by annual revenue in USD, by number of employees and by number of countries of operation

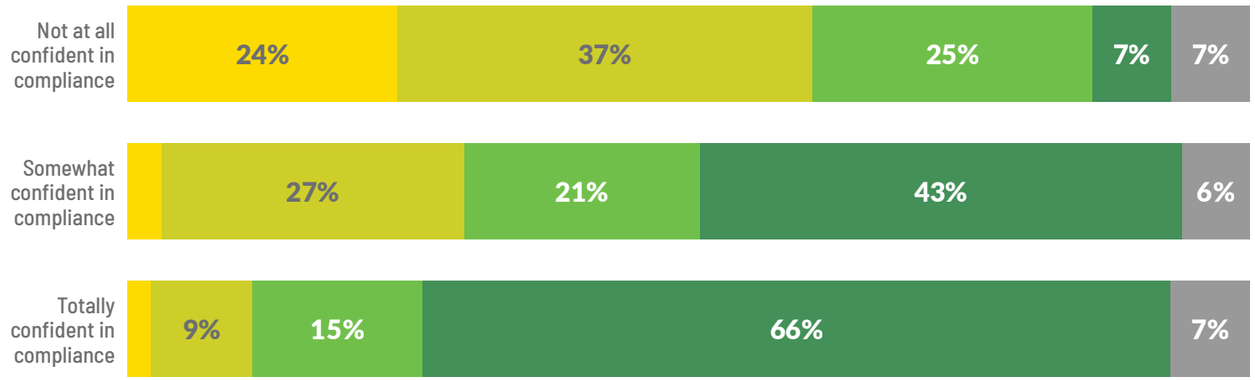
		NUMBER OF EMPLOYEES						REVENUE						NUMBER OF COUNTRIES OF OPERATION						
FREQUENCY	Overall	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+	Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion	1	2-5	6-10	11-20	21-40	41-60	More than 60
Regularly, based on established triggers embedded throughout business processes	44%	38%	36% ↓	41%	53%	62% ↑	64% ↑	33%	31% ↓	37%	49%	53%	69% ↑	41%	38%	37%	46%	34%	51%	62% ↑
Regularly, but triggers are not fully established or formalized	20%	15%	21%	20%	29%	29%	12%	18%	18%	19%	24%	25%	15%	17%	19%	25%	15%	36% ↑	24%	14%
Ad hoc, resulting in some privacy risk not being managed	25%	31%	31% ↑	27%	10% ↓	7% ↓	17%	21%	40% ↑	30%	18% ↓	16%	13% ↓	20%	30%	32%	30%	28%	19%	20%
Not performed	5%	7%	5%	5%	3%	2%	5%	10%	4%	6%	5%	4%	2%	9% ↑	6%	4%	2%	2%	3%	2%
Not regulatorily required	6%	9%	8%	6%	5%	0%	2%	18% ↑	7%	7%	5%	4%	2%	12% ↑	8%	3%	7%	0% ↓	3%	2%

By organization size, either in revenue or number of employees, or by number of countries of operation a similar picture emerges: those working in larger organizations or operating in more countries are more likely to have established PIA processes. Almost seven in 10 respondents working for organizations with more than 80,000 employees and just over six in 10 respondents working in organizations with more than USD60 billion in revenue or more than 60 countries of operation identified their organizations conduct PIAs regularly based on established triggers. On the other hand, those working for smaller organizations, either by revenue, number of employees or number of countries of operation, were more likely to work for organizations that have yet to fully establish PIA processes.

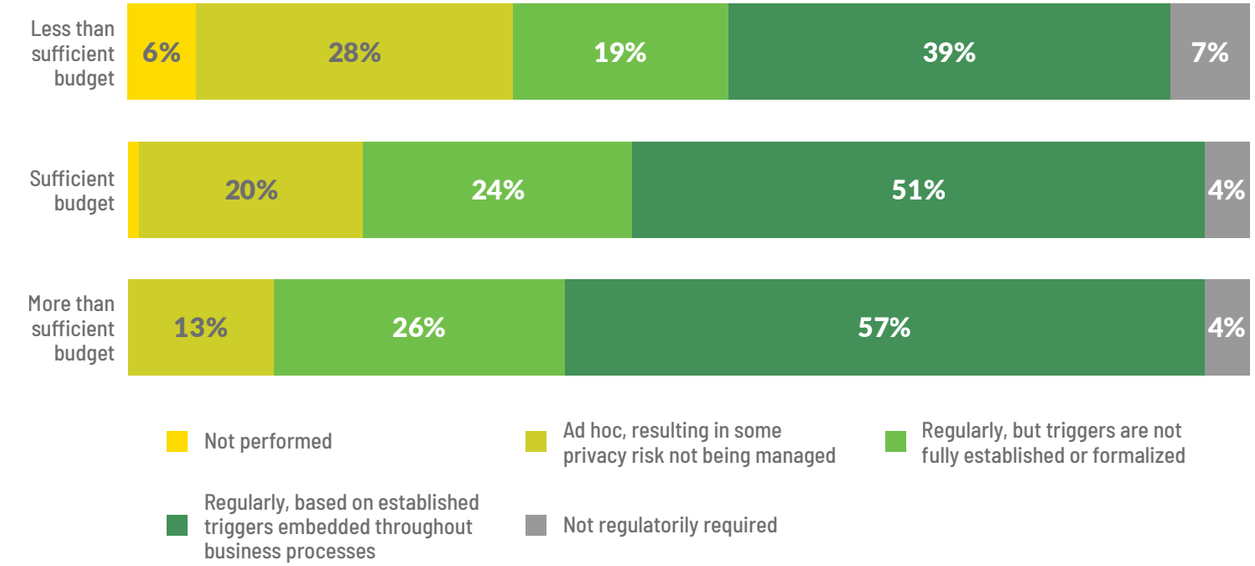
When looking at confidence in compliance, the picture is clear: respondents who identified confidence in their organization's privacy compliance work in organizations that are more likely to regularly undertake PIAs based on established triggers. More specifically, 66% of respondents who identified total confidence in their organization's privacy compliance practices said their organization regularly conducts PIAs based on established triggers. On the other hand, 86% of those who identified no confidence in their organization's ability to comply with privacy requirements said the PIA process does not occur regularly at their organizations.

The extent to which an organization has sufficient budget to undertake regular PIAs could play a role in this break down. While PIAs likely form a core part of how organizations manage privacy risk and a key tool in a privacy practitioners toolkit, those who identified their company's privacy budgets as less than sufficient were less likely to work in organizations that regularly conducted PIAs. More specifically, where respondents identified privacy budgets as less than sufficient, only 39% of respondents identified their organizations conducted PIAs regularly, as opposed to 57% who identified their privacy budgets are more than sufficient.

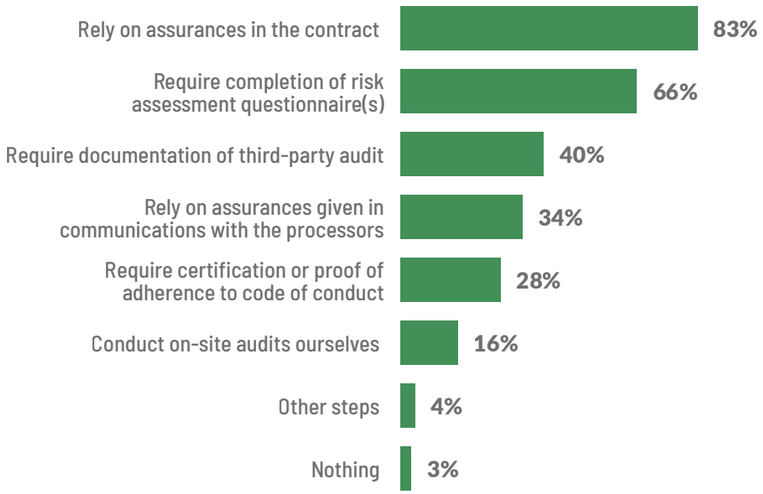
Privacy impact assessment frequency by confidence in privacy compliance



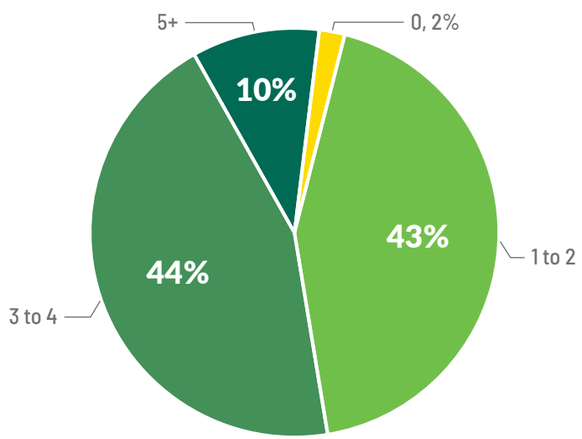
Privacy impact assessment frequency by budget sufficiency



Overall approach to third-party risk management



Number of third-party risk management measures taken



Third-party privacy risk management

Organizations continue to rely on third parties to provide various products and services. The ability to outsource to a third party and take advantage of specific expertise, obtain cost efficiencies and scale operations as needed enables organizations to meet core business objectives. However, the absence of a risk-based approach to third-party risk management can be costly. In particular, where personal data and sensitive personal data are shared, the third party's privacy risk posture should be a core part of how an organization manages its own privacy risk exposure. Effective third-party privacy risk management now relies upon undertaking due diligence processes commensurate with the level of potential risk faced, effective contracting processes that include privacy requirements, and post-contracting reviews and audits that monitor the privacy risk present in ongoing third-party relationships.

With this in mind, we sought to understand the steps organizations take to manage their third-party privacy risk exposures.

Of respondents, 83% identified they rely on assurance provided by contracting with third parties. The completion of risk-assessment questionnaires is the second most popular measure, selected by almost seven in 10 respondents and, rounding out the top three, at 40%, but lagging some way behind is required third-party evidence of completed audits.

Curiously, of those who reported not relying on contracts, 10% appear to rely instead on the completion of risk-assessment questionnaires, 5% require certification or proof of adherence to a code of conduct and 3% conduct on-site reviews. The extent to which these measures are effective in the absence of formalized contracts, however, remains to be seen.

Looking further at the number of measures implemented, only one in 10 respondents identified their organization implemented five or more of the listed third-party privacy risk measures. Meanwhile just over four in 10 identified their organization implemented between one and two of the listed measures.

Given the variation in the number of measures implemented by organizations, we sought to further investigate the combinations of measures used.

The most common measure, used by just over 12% of respondents, was sole reliance on contracts. A further 12% relied solely on assurance provided by the contract and completion of risk-assessment questionnaires. An additional 45% relied on assurance provided by the contract, completion of risk-assessment questionnaires and one other measure, making these the two most popular measures used by organizations.

Top 20 combinations (making up 80% of the sample) of methods used by organizations to manage privacy risk from personal data processed by third parties

Percentage of sample who chose this combination of options	METHODS USED					
	Rely on assurances in the contract	Require completion of risk-assessment questionnaires	Require documentation of third-party audit	Rely on assurances given in communications with the processors	Require certification or proof of adherence to code of conduct	Conduct on-site audits ourselves
12% ↑	×					
12% ↑	×	×				
8% ↑	×	×	×			
8% ↑	×	×		×		
5% ↑	×			×		
5% ↑	×	×	×	×		
5% ↑	×	×	×		×	
4% ↑	×	×	×	×	×	
3% ↑		×				
3%	×	×			×	
2%	×	×	×		×	×
2%	×	×	×	×	×	×
2%	×		×	×		
2%	×				×	
2%		×	×		×	
2%				×		
1%	×		×			
1%	×		×		×	
1%	×	×				×
1%	×	×		×	×	

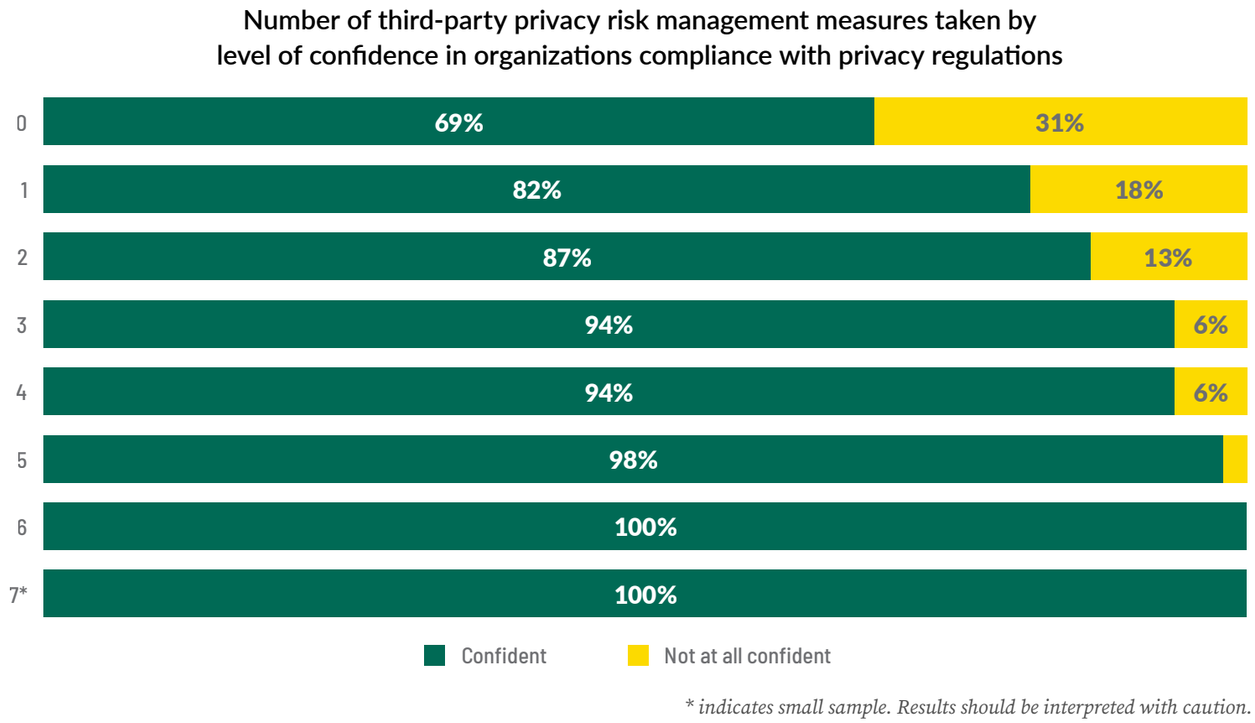
Approach to third-party privacy risk management by number of employees and by annual revenue in USD

		NUMBER OF EMPLOYEES						REVENUE					
APPROACH	Overall	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	80,000+	Under 100 million	101-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	60+ billion
Rely on assurances in the contract	83%	62% ↓	88%	84%	88% ↑	72% ↓	78%	80%	83%	85%	86%	84%	79%
Require completion of risk assessment questionnaire(s)	66%	44% ↓	55% ↓	72%	73% ↑	63%	76%	47% ↓	68%	71%	76%	82% ↑	67%
Require documentation of third-party audit	40%	38%	43%	43%	35%	44%	39%	38%	41%	39%	37%	47%	38%
Rely on assurances given in communications with the processors	34%	31%	44% ↑	29%	38%	26%	24%	37%	38%	31%	34%	33%	24%
Require certification or proof of adherence to code of conduct	28%	13% ↓	25%	34%	26%	30%	37%	26%	30%	23%	25%	42% ↑	36%
Conduct on-site audits ourselves	16%	13%	10% ↓	11%	18%	23%	28% ↑	13%	11%	15%	22%	24%	26%
Other steps	4%	8%	4%	4%	2%	9%	4%	3%	5%	4%	2%	7%	5%
Nothing	3%	8% ↑	1%	3%	1%	7% ↑	2%	2%	2%	3%	0%	2%	10% ↑

When considering the size of an organization, there is a similar preference to rely on contractual assurance across all sizes. Additional measures are, however, less popular among smaller organizations. Compared to the average, risk-assessment questionnaires are relatively less likely to be used in organizations with less than 999 employees or less than USD100 million in revenue. On the other hand, at least two in 10 respondents working for organizations with more than 25,000 employees or greater than USD9 billion in revenue conducted on-site audits to monitor third-party privacy risk. This suggests larger organizations, likely to have more resources and budget, can undertake more expensive mitigation measures to address third-party risk. Almost six in 10 respondents working in organizations with less than 100 employees or less than USD100 million in revenue identified their organization only implemented one measure to tackle third-party privacy risk. At the same time, one in five respondents working in organizations with greater than 80,000 employees or more than USD60 billion in revenue identified their organization implemented at least five measures to manage third-party privacy risk.

Where does this leave privacy pros' confidence in their organization's ability to comply with privacy requirements?

There was a notable increase in the proportion of respondents who identified confidence in their organization's level of compliance based on the number of third-party privacy risk management measures implemented. When three or more measures were implemented, at least nine in 10 respondents identified confidence in their organization's compliance with privacy requirements. Privacy pros could consider the extent to which their organization takes a multifaceted approach to managing third-party privacy risk. The argument that the more lines of defense against a third-party privacy risk, the better an organization can manage risks from data sharing with other organizations could prevail. The key to identifying which measures to implement should be the consideration of privacy regulatory requirements data transfers to third parties are subject to, any risks presented by these transfers and processing by third parties.



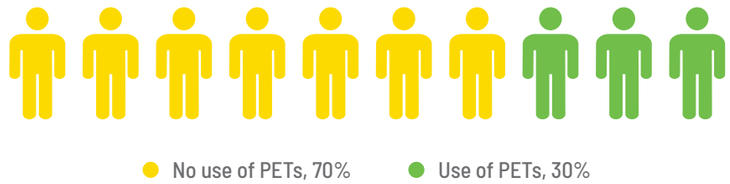
When three or more measures were implemented, at least nine in 10 respondents identified confidence in their organization's compliance with privacy requirements.

Part IX. Technology-enabled compliance

Increasingly, a variety of emerging and maturing PETs are being used to aid privacy governance. However, we are in the foothills of widespread take-up, as seven in 10 respondents said their organization has yet to use emerging PETs.

The realms and roles of technology have expanded from convenience to more transformational and accelerative changes in how organizations approach core business activities. In a paradigm shift away from technology as solely a source of privacy risk to be managed, a number of PETs have emerged and are maturing. Technologies have enabled privacy compliance functions to streamline operations and, in some cases, mature further by automating processes and embedding real-time monitoring to revolutionize how organizations meet privacy compliance requirements. In this year's survey, we sought to understand the extent to which organizations utilize technology to aid or enhance privacy governance, the evolving landscape of emerging PETs and the extent to which organizations look to support privacy compliance using AI.

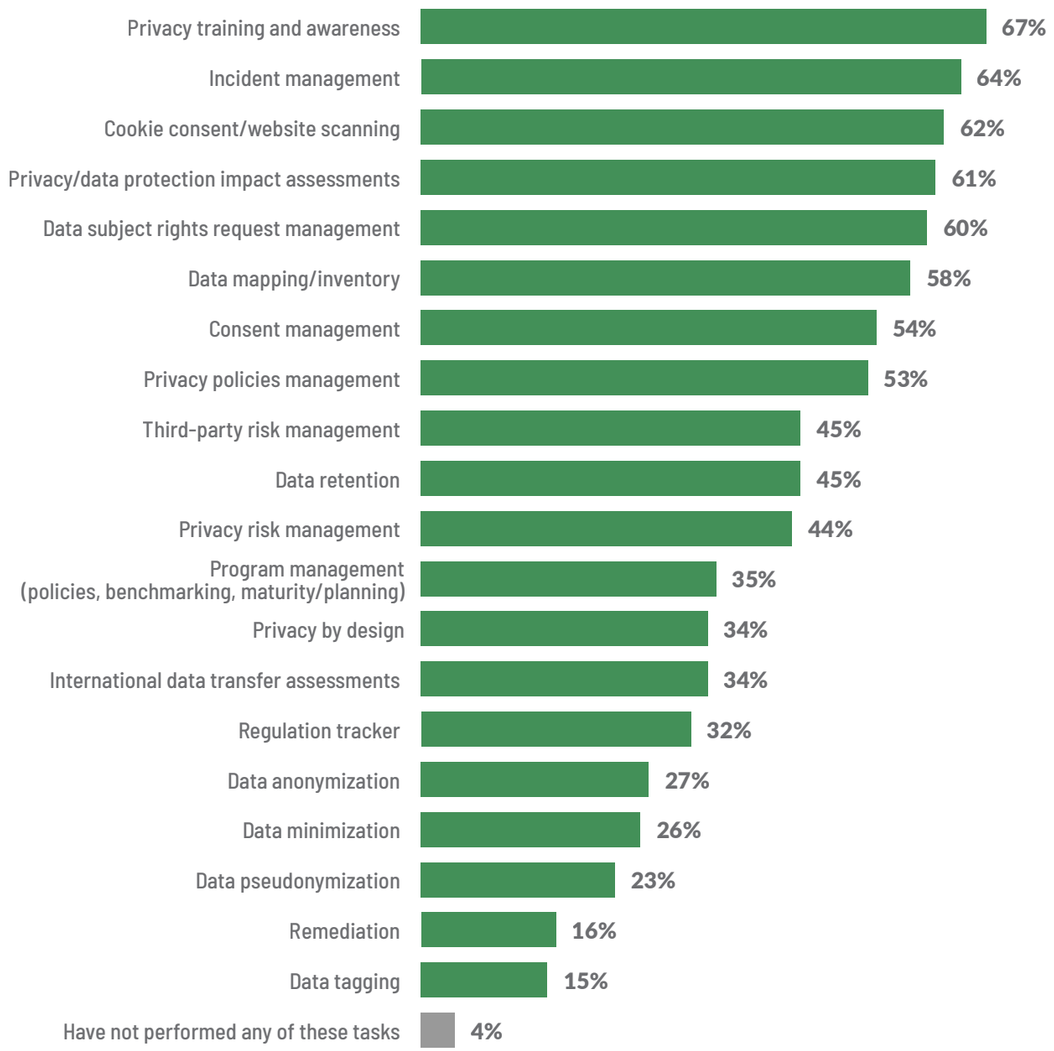
Respondents' use of emerging PETs



Privacy training and awareness, incident management, and cookie consent/website scanning formed the top three areas that were more likely to be technology enabled rather than manual. Consent management is another area where organizations appear to rely on technology solutions more than manual implementations, with technology well placed to help manage the potentially large number of touchpoints where consent can be collected.

According to this year's survey, larger organizations use more technology to support privacy compliance. For instance, 65% of respondents who work for organizations with more than 80,000 employees identified their organizations use technology to manage data subject rights requests, as opposed to 44% of those working for organizations with less than 100 employees. Larger organizations may be subject to a greater volume of data subject rights requests, so it is no surprise they tend to use technology to assist other, more traditional governance measures. The opposite trend appeared when looking at data retention and privacy policy management: smaller organizations tend to use technology more than manual methods. For example, 54% of respondents working for organizations with less than USD100 million in annual revenue identified their organizations use technology to support and manage data retention, as opposed to only 29% of respondents working for organizations with more than USD60 billion in revenue. Complexities of the data landscape require larger organizations to spend more time grappling to identify, apply and manage data retention requirements, so they may be less likely to be in a position to use technology to optimize these processes. Smaller organizations may also rely upon third-party data retention technology providers to provide data retention requirements that larger organizations may develop internally through larger privacy functions.

Proportion of respondents using technology, as opposed to manual methods, to support privacy compliance



Proportion of respondents using technology, as opposed to manual methods to support privacy compliance by sector

METHODS USED	Overall	SECTOR: 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
Consent management	54%	60%	54%	52%	56%	67%	24% ↓	57%	44%	63%	56%
Cookie consent/website scanning	62%	60%	66%	58%	76%	85% ↑	22% ↓	56%	67%	79%	69% ↑
Data mapping/inventory	58%	56%	64%	52%	72%	89% ↑	37% ↓	53%	78%	67%	59%
Third-party risk management	45%	59% ↑	59% ↑	32%	44%	44%	15% ↓	43%	22%	42%	46%
Privacy/data protection impact assessments	61%	58%	63%	62%	64%	78%	61%	59%	44%	58%	61%
Data subject rights request management	60%	63%	57%	66%	60%	85% ↑	30% ↓	53%	56%	71%	67% ↑
Remediation	16%	17%	25% ↑	20%	12%	30%	15%	9%	0%	17%	13%
Data minimization	26%	25%	39% ↑	24%	20%	26%	20%	19%	11%	29%	26%
Data retention	45%	50%	54%	40%	44%	52%	33%	29% ↓	56%	54%	47%
Data anonymization	27%	27%	37% ↑	32%	24%	44% ↑	19%	20%	11%	25%	24%
Data pseudonymization	23%	23%	29%	22%	32%	37%	11% ↓	20%	11%	21%	22%
Data tagging	15%	20%	24% ↑	8%	12%	26%	7%	4% ↓	0%	17%	18%
Program management (policies, benchmarking, maturity/planning)	35%	42%	39%	26%	32%	48%	31%	24%	11%	42%	35%
Privacy by design	34%	34%	50% ↑	30%	28%	56% ↑	28%	16% ↓	0% ↓	42%	35%
Privacy risk management	44%	51%	50%	44%	36%	48%	41%	26% ↓	33%	67% ↑	45%
Privacy training and awareness	67%	69%	61%	78%	64%	74%	63%	61%	56%	71%	69%
Privacy policies management	53%	59%	53%	52%	44%	56%	46%	40% ↓	44%	71%	54%
International data transfer assessments	34%	29%	43%	30%	40%	48%	11% ↓	29%	22%	46%	39%
Incident management	64%	69%	59%	68%	72%	78%	57%	61%	33%	67%	64%
Regulation tracker	32%	49% ↑	34%	22%	24%	52% ↑	6% ↓	17% ↓	33%	33%	35%
Have not performed any of these tasks	4%	3%	1%	2%	0%	0%	6%	9% ↑	11%	0%	5%

When considering sector, respondents identified the consumer goods, services and retail sector, technology and telecommunications sector, manufacturing sector, and banking and insurance sector are ahead of the pack in supporting privacy compliance with technology. Notably, respondents working in the government sector and life sciences and health care sector identified their organizations used less technology on average to support privacy compliance processes.

Almost one in 10 respondents working in life sciences and health care organizations, and just over one in 10 in the legal sector, identified their organizations have yet to use technology to support management of any of the listed privacy compliance activities. Respondents working in the government sector identified their organizations used technology significantly less than others.

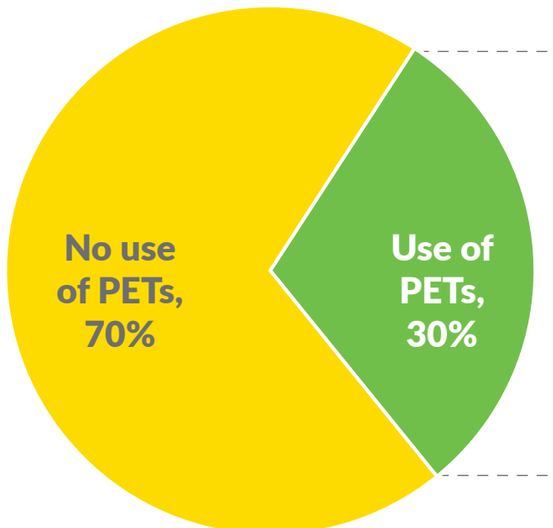
HIGHER THAN OVERALL AVERAGE

Emerging PETs

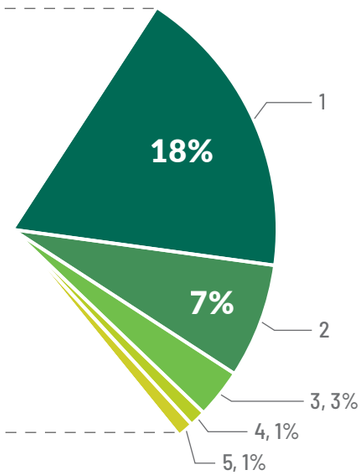
Emerging PETs continue to rise to the forefront of discussions surrounding tools that preserve the security and privacy of personal data while maintaining the utility of the analyzed information. At the same time, their relative infancy, lack of formalized use cases and saturation of off-the-shelf solutions makes comparing and contrasting diverse implementation more challenging. With this in mind, understanding the extent to which PETs are currently used could help explore the proliferation and maturing of the PET landscape in future years. Overall, seven in 10 respondents identified their organization has yet to implement an emerging PET. Of respondents who identified their organization has implemented PETs, the most commonly selected emerging PET was synthetic data, chosen by 12% of respondents overall. The second most popular was trusted execution environments at 10%, with homomorphic encryption rounding out the top three at 7%.

Of those who said emerging PETs have been implemented by their organization, the majority have only implemented one emerging PET. Synthetic data was the most popular option, chosen by 5% of respondents. Around 5% of respondents identified their organizations had implemented three or more different types of emerging PETs.

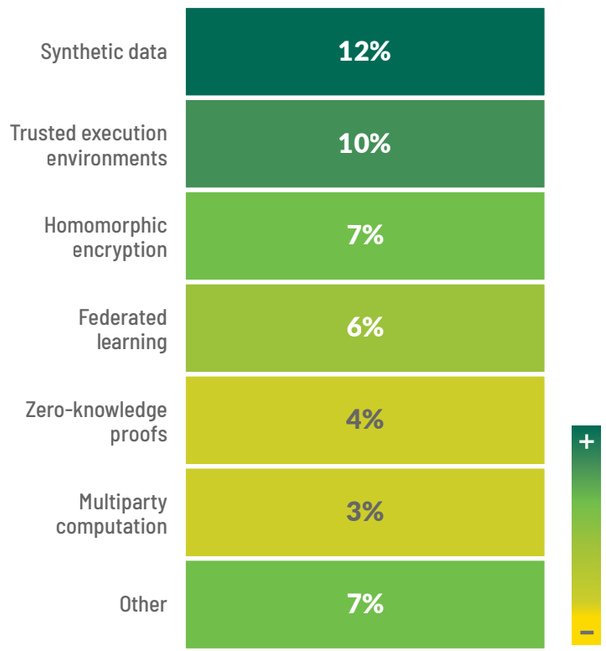
Use of emerging PETs versus no use of PETs



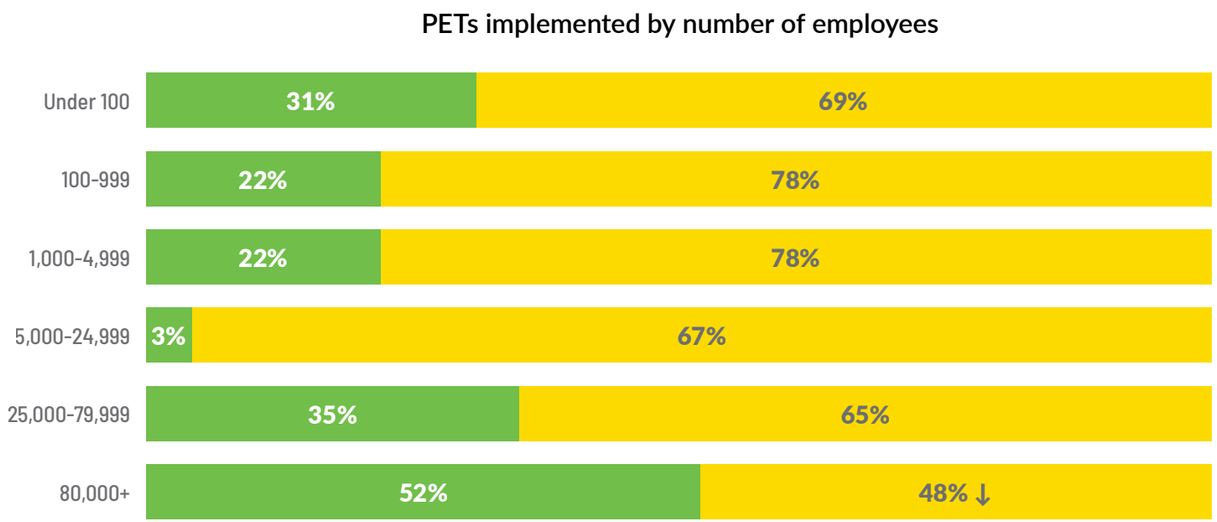
Combinations of emerging PETs implemented by organizations

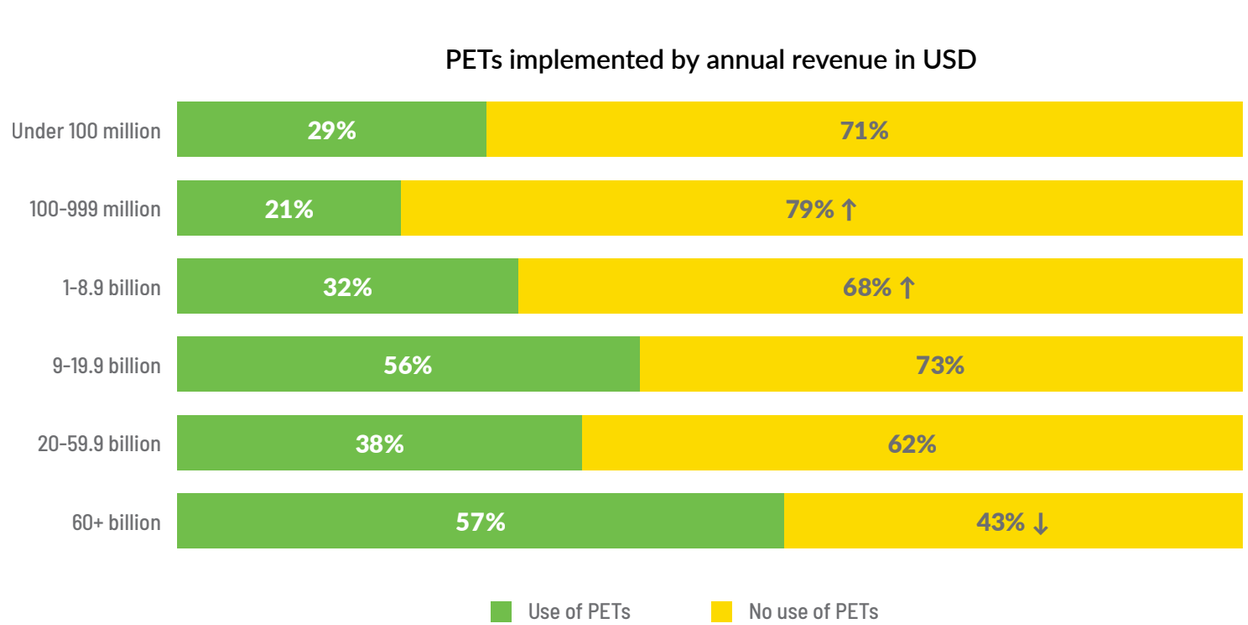


Emerging PETs implemented



The most commonly selected emerging PET was synthetic data, chosen by 12% of respondents overall. The second most popular was trusted execution environments at 10%, with homomorphic encryption rounding out the top three at 7%.





When considering organization size, the largest surveyed organizations are more likely to use PETs than not: 52% of respondents at organizations with more than 80,000 employees and 57% of respondents are organizations with more than USD60 billion in revenue identified their organization implemented emerging PETs. On the other hand, smaller organizations are less likely to have implemented emerging PETs, with three in 10 respondents from organizations with less than 100 employees or under USD100 million in revenue identifying their organization implemented emerging PETs.

While the uptake in emerging PETs is low, it is promising to see several organizations have taken steps toward implementing a variety of emerging PETs alongside traditional technical and organizational measures. In the coming years, we will explore developments and growth in this area further.

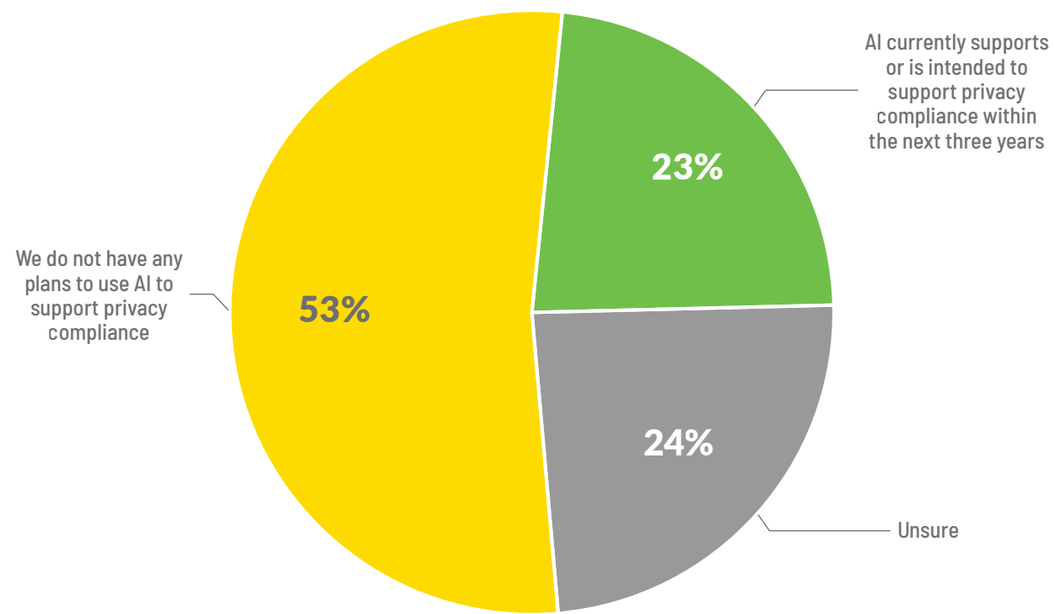
Use of AI to support privacy compliance

Privacy compliance is an area that could likely benefit from AI, whether through AI-enabled tooling that identifies potential privacy risks, finds trends in privacy compliance metadata, monitors privacy compliance programs or automates privacy compliance tasks.

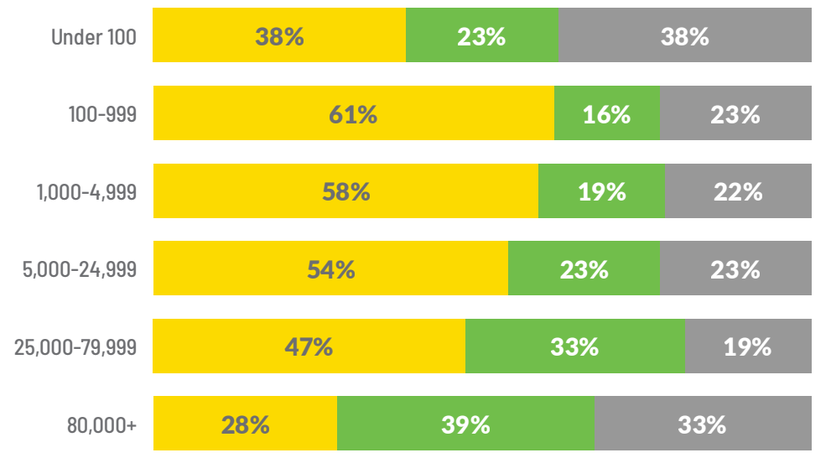
Just over five in 10 respondents identified their organization does not have any plans to use AI to support privacy compliance, while just over two in 10 identified their organization either currently uses AI for compliance purposes or intends to within the next three years.

When considering organizational size, a slightly different picture emerges between smaller and larger organizations. Those working in organizations with more than USD9 billion in revenue or more than 25,000 employees identified a higher-than-average incidence of either using AI to support privacy compliance or intending to do so within the next three years. This figure rises to almost four in 10 when considering the largest organizations either by revenue or number of employees.

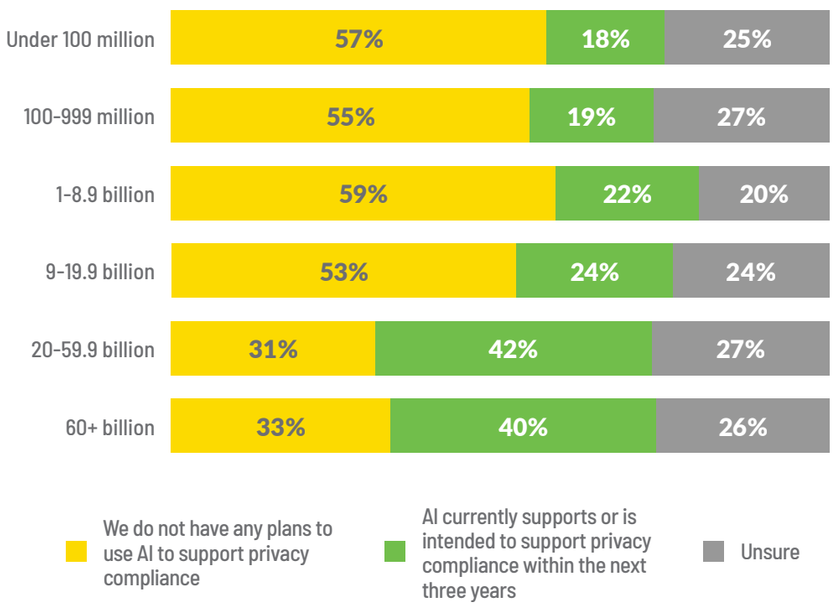
Use of AI to support privacy compliance

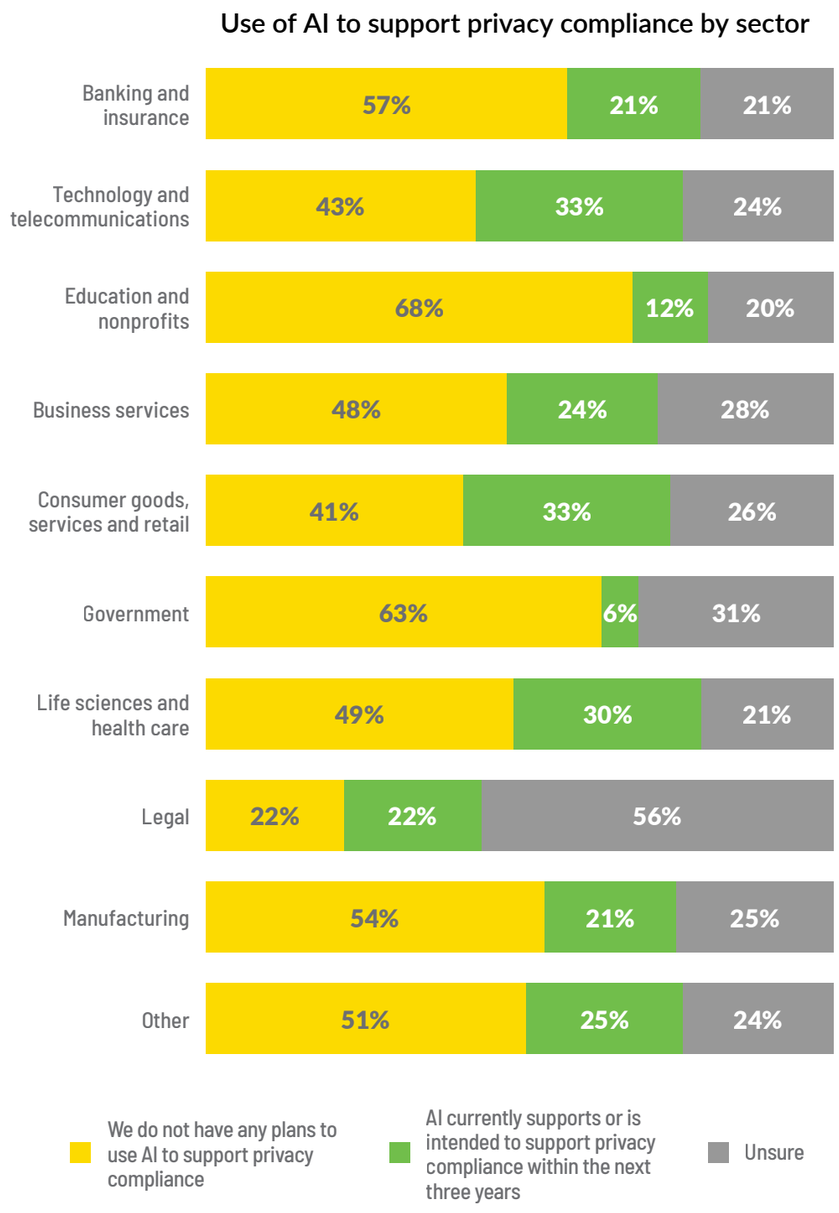


Use of AI to support privacy compliance by number of employees



Use of AI to support privacy compliance by annual revenue in USD





When considering the breakdown by sector, the technology and telecommunications sector, business services sector, consumer goods, services and retail sector, and life sciences and health care sector reported higher-than-average incidences of AI currently supporting or intended to support privacy compliance within the next three years. Over six in 10 respondents working in the education and nonprofit sector and government sector identified their organization does not have plans to support privacy compliance with AI.

Privacy compliance technologies continue to evolve, partly due to the pursuit of innovation by vendors and partly due to evolving use-cases and demands from organizations. Competition in the privacy vendor market and the complex web of new and evolving regulatory requirements likely add to the supply of and demand for AI-enabled privacy compliance tools. Given this, privacy pros need to prepare to contend with AI as a product brought by other business functions, while being aware of issues in deploying AI as a compliance tool.

Part X. Gathering metrics

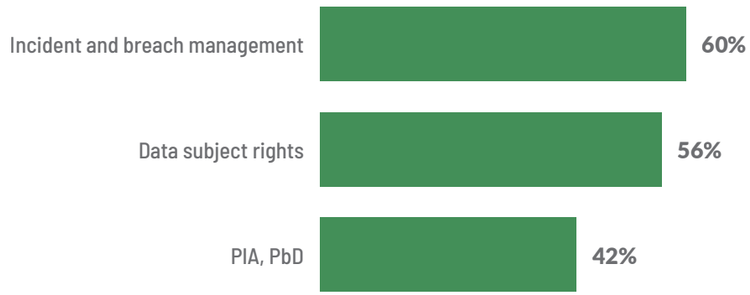
Of respondents, 57% flagged the lack of metrics or metrics without a link to business margins as a key challenge

Metrics help privacy functions benchmark to peers and report key performance indicators across the organization at large. Privacy is oftentimes more art than science, which can lead to difficulties collecting tangible, meaningful and actionable metrics.

Top privacy metric topics of 2023

This year, the top three topics on which organizations gathered privacy metrics were incident and breach management, at 60%, data subject rights, at 56%, and PIAs/Pbd, at 42%. These topics were also last year's top three, in the same order, though the percentages of respondents who indicated recording metrics on these topics have increased. It is important to note, in addition to their strategic importance, these topics may have remained in the lead because they are easier concepts to quantify, benchmark and report on compared to others on the list. Many tools on the market help manage and automate these specific topics, thus making it easier to gather metrics on them.

Top three topics about which privacy metrics are gathered in 2023



Topics about which privacy metrics are gathered in 2023 versus 2022

	2023	2022
Incident and breach management	60% ↑	54%
Data subject rights	56%	51%
PIA, PbD	42% ↑	32%
Third-party management	28%	27%
Inventory (Article 30)	26%	26%
Data deletion	26%	26%
Privacy program	26% ↓	31%
Privacy risk and controls management	23%	25%
Privacy policy management (e.g., update/revision)	22%	20%
Notice and consent	21%	20%

	2023	2022
Risk identification and quantification	19%	21%
International transfers	19%	18%
Data sharing	18%	15%
Security for privacy	18%	18%
Governance and operating model	15% ↓	20%
Data minimization	13%	11%
Consumer privacy (e.g., profiling and automated decision-making)	12%	10%
Privacy and customer (customer trust/privacy in customer journey, etc.)	10%	10%
Data localization	10% ↑	3%
Data utilization	9%	N/A

	2023	2022
Implementation of PETs	8%	9%
Privacy enabling tech performance (data scanning, process automation, etc.)	7%	6%
Privacy in cloud	7%	7%
Data ethics	5%	5%
AI governance	5%	6%
Children's consent	5% ↑	3%
Privacy in mergers and acquisitions	5%	5%
Privacy in internet of things/personal devices	3%	3%
Other	6% ↑	3%
Privacy metrics are not gathered	12%	N/A

**N/A: No applicable data, as this section did not appear in the 2022 survey.*

Asian organizations lead the way as far more metrics-based and metrics-mature than their North America counterparts. In Asia, 21 topics for metrics have significantly higher percentages than the overall average.

Operating location is important for metrics, as it affects whether organizations collect metrics at all. Asian organizations lead the way as far more metrics-based and metrics-mature than their North America counterparts. In Asia, 21 topics for metrics have significantly higher percentages than the overall average. The reason for this is not completely clear, though it is likely based on differences in organizational structure, culture and metrics maturity between regions. There are only two metrics topics for which the average percentage is higher for North American organizations compared to the overall average of organizations.

The number of countries where an organization operates is a contributing factor. Organizations that operate in only one country are less likely to gather metrics on various topics compared to those that operate in more than 60 countries. This is especially true for topics involving international compliance, like data localization and international transfers.

Topics about which privacy metrics are gathered by continent

TOPICS	Overall	CONTINENT			
		North America	Europe	Asia	Other
AI governance	5%	5%	3%	11%	2%
Data utilization	9%	9%	4% ↓	20% ↑	8%
Children's consent	5%	4%	3%	17% ↑	10%
Consumer privacy (e.g., profiling and automated decision-making)	12%	11%	11%	29% ↑	8%
Data deletion	26%	24%	27%	43% ↑	21%
Data ethics	5%	5%	4%	9%	10%
Data minimization	13%	12%	14%	37% ↑	6%
Data sharing	18%	17%	17%	31% ↑	15%
Data localization	10%	8%	12%	26% ↑	4%
Data subject rights	56%	54%	67% ↑	60%	38% ↓
Governance and operating model	15%	13%	17%	20%	15%
Implementation of PETs	8%	9%	6%	20% ↑	2%
Incident and breach management	60%	56% ↓	67%	69%	63%
International transfers	19%	16% ↓	24%	46% ↑	8% ↓
Inventory (Article 30)	26%	21% ↓	40% ↑	34%	15%

There is location variance when it comes to which topics are chosen for metrics. Of European organizations, 67% gather metrics on data subject rights, which is significantly higher than the overall average of 56%. This is not necessarily surprising, as the GDPR mandates specific processes for data subject access rights, etc. Nearly half of Asian organizations collect metrics on both international transfers and notice and consent, compared to just 19% and 21% for the overall average, respectively. While the collection of incident and breach management metrics is significantly lower in North America, this may actually signal an increase in privacy maturity. Organizations with a more mature privacy function may collect nuanced metrics, whereas less mature organizations may focus mostly on foundational metrics, like incident and breach management.

Of European organizations, 67% gather metrics on data subject rights, which is significantly higher than the overall average of 56%.

Topics about which privacy metrics are gathered by continent, *continued*

TOPICS	Overall	CONTINENT			
		North America	Europe	Asia	Other
Privacy program	26%	26%	19%	37%	33%
Notice and consent	21%	21%	18%	49% ↑	15%
Privacy and customer (customer trust/ privacy in customer journey, etc.)	10%	9%	9%	20% ↑	15%
Privacy-enabling tech performance (data scanning, process automation, etc.)	7%	7%	5%	20% ↑	2%
PIA, PbD	42%	39%	41%	63% ↑	48%
Privacy in cloud	7%	7%	3% ↓	23% ↑	6%
Privacy in internet of things/ personal devices	3%	1% ↓	2%	14% ↑	6%
Privacy in mergers and acquisitions	5%	4%	4%	17% ↑	2%
Privacy policy management (e.g., update/revision)	22%	21%	20%	37% ↑	27%
Privacy risk and controls management	23%	21% ↓	25%	40% ↑	27%
Risk identification and quantification	19%	19%	17%	37% ↑	15%
Security for privacy	18%	18%	14%	40% ↑	13%
Third-party management	28%	30%	23%	43% ↑	23%
Privacy metrics are not gathered	12%	12%	9%	9%	17%
Other	6%	6%	8%	0%	4%

Topics about which privacy metrics are gathered by sector

TOPICS	Overall	SECTOR: 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
AI governance	5%	1% ↓	11% ↑	4%	0%	4%	2%	6%	11%	0%	7%
Data utilization	9%	6%	16% ↑	4%	4%	11%	7%	6%	11%	13%	10%
Children's consent	5%	3%	9%	14% ↑	0%	0%	4%	0% ↓	0%	0%	7%
Consumer privacy (e.g., profiling and automated decision-making)	12%	15%	16%	6%	4%	22%	2% ↓	7%	22%	17%	14%
Data deletion	26%	29%	38% ↑	24%	24%	33%	13% ↓	13% ↓	33%	17%	29%
Data ethics	5%	4%	4%	8%	0%	4%	4%	4%	22% ↑	4%	7%
Data minimization	13%	10%	21% ↑	10%	8%	15%	7%	9%	0%	13%	19% ↑
Data sharing	18%	17%	20%	12%	12%	22%	24%	13%	33%	21%	19%
Data localization	10%	6%	13%	2%	8%	11%	4%	13%	0%	21%	13%
Data subject rights	56%	61%	62%	56%	60%	85% ↑	20% ↓	43% ↓	44%	50%	65% ↑
Governance and operating model	15%	15%	18%	18%	8%	4%	19%	4% ↓	0%	29% ↑	16%
Implementation of PETs	8%	5%	11%	4%	4%	7%	7%	7%	11%	13%	12% ↑
Incident and breach management	60%	69% ↑	59%	56%	68%	52%	52%	60%	44%	58%	59%
International transfers	19%	16%	30% ↑	8% ↓	12%	30%	7% ↓	20%	11%	33%	21%
Inventory (Article 30)	26%	20%	28%	16%	32%	37%	9% ↓	34%	11%	33%	31%

Industry sector is relevant, too. Banking and insurance firms focus significantly more on incident and breach management compared to the average.

Topics about which privacy metrics are gathered by sector, *continued*

TOPICS	Overall	SECTOR									
		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 program	26%	23%	30%	18%	4% ↓	26%	26%	26%	22%	38%	29%
Notice and consent	21%	22%	29%	20%	28%	30%	6% ↓	20%	33%	13%	22%
Privacy and customer (customer trust/ privacy in customer journey, etc.)	10%	9%	22% ↑	8%	8%	7%	4%	0% ↓	11%	8%	14%
Privacy-enabling tech performance (data scanning, process automation, etc.)	7%	4%	13% ↑	0% ↓	0%	15%	0% ↓	4%	11%	13%	10%
PIA, PbD	42%	39%	49%	28% ↓	48%	52%	48%	39%	22%	42%	42%
Privacy in cloud	7%	6%	9%	2%	8%	0%	7%	7%	11%	4%	8%
Privacy in internet of things/ personal devices	3%	2%	5%	0%	0%	0%	2%	3%	11%	4%	3%
Privacy in mergers and acquisitions	5%	4%	8%	0%	8%	4%	0%	3%	11%	13%	6%
Privacy policy management (e.g., update/revision)	22%	23%	24%	22%	8%	15%	24%	13% ↓	33%	25%	28%
Privacy risk and controls management	23%	29%	34% ↑	10% ↓	12%	26%	17%	11% ↓	11%	25%	29%
Risk identification and quantification	19%	17%	25%	10%	28%	19%	17%	16%	0%	13%	25% ↑
Security for privacy	18%	13%	28% ↑	12%	24%	22%	24%	10%	44% ↑	17%	16%
Third-party management	28%	31%	39% ↑	16% ↓	40%	37%	4% ↓	26%	11%	29%	33%
Privacy metrics are not gathered	12%	7%	9%	18%	4%	4%	19%	17%	0%	4%	13%
Other	6%	5%	5%	4%	4%	4%	6%	7%	11%	17% ↑	6%

Technology and telecommunications companies seem to focus significantly more on third-party management compared to the average organization.

Key challenges in leveraging metrics for compliance reporting

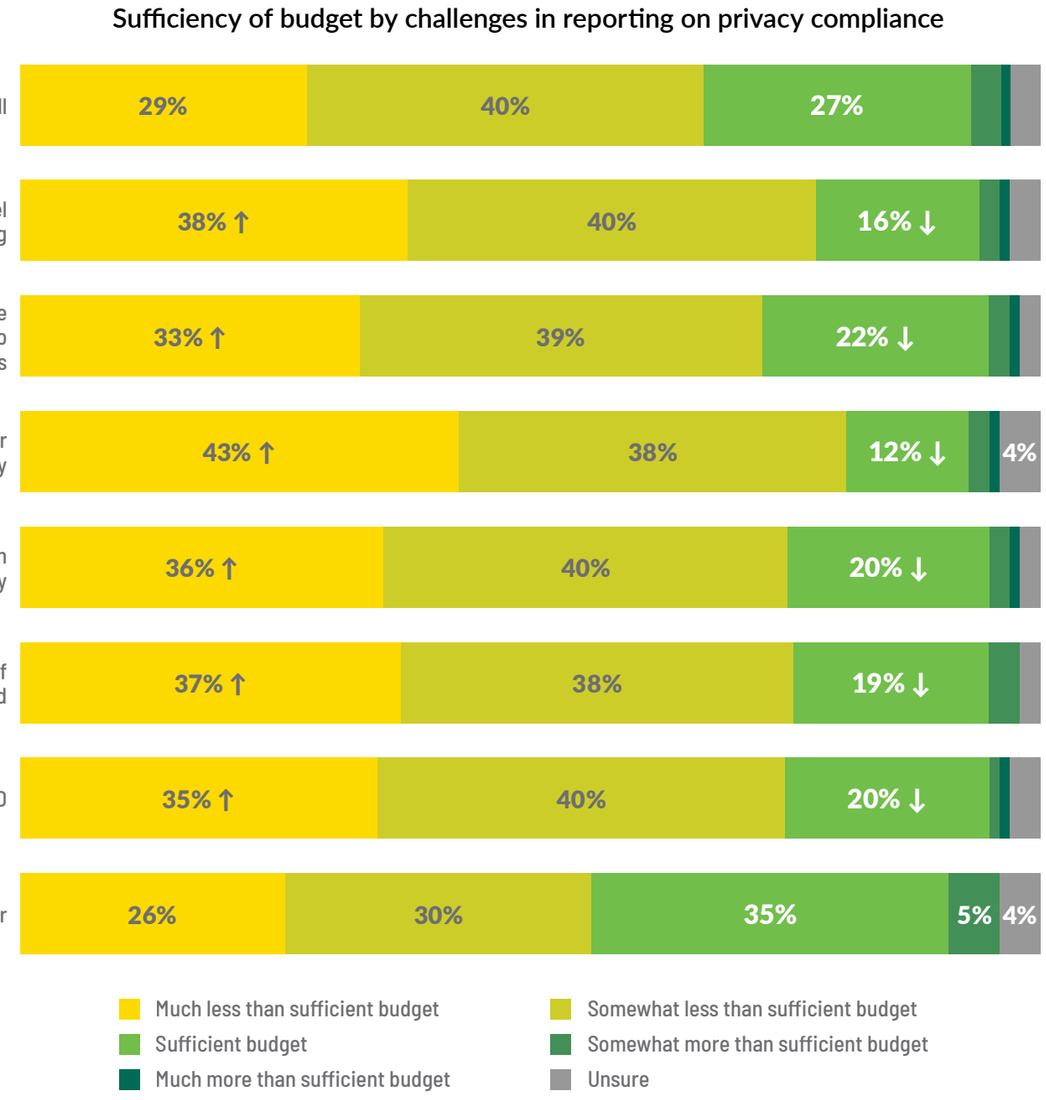
Collecting metrics and performing analysis is usually only the first — albeit important — step. Organizations typically use metrics to empower decision-making and reporting on privacy compliance, particularly to the board. This year's survey asked respondents what kind of challenges they face in doing this. Indicated by 57% of respondents, the biggest challenge is the absence of tangible metrics and/or link to business margins to support reporting. This was followed closely, at 53%, by lack of maturity of PbD within the organization.

These challenges are less prevalent in Asia, where only 43% of organizations lack tangible metrics, compared to 60% of North American organizations.

This may seem puzzling at first. The majority of organizations collect some metrics, so why do so many also identify the lack of metrics as a challenge? One reason, as mentioned above, is some privacy topics lend themselves to metrics more easily than others. Considering the most common topics for metrics represent only a small fraction of the compliance efforts privacy functions undertake, and that it may be difficult to gather metrics on other compliance efforts, privacy teams can be put in a tough position.

Key challenges in reporting on privacy compliance overall and by continent

	Overall	North America	Europe	Asia	Other
Absence of tangible metrics and/or link to business margins to support reporting	57%	60% ↑	52%	43%	56%
Lack of maturity of PbD within the organization hindering reporting to board	53%	52%	48%	49%	71% ↑
Ineffective integration of privacy with other complementary topics	43%	42%	47%	34%	50%
Lack of board-level understanding of privacy	37%	37%	40%	31%	38%
Scope and objective of reporting not defined appropriately	36%	37%	33%	37%	35%
Absence of clear mandate for privacy within the organization	34%	38% ↑	23% ↑	31%	35%
Other	13%	12%	9%	23%	21%



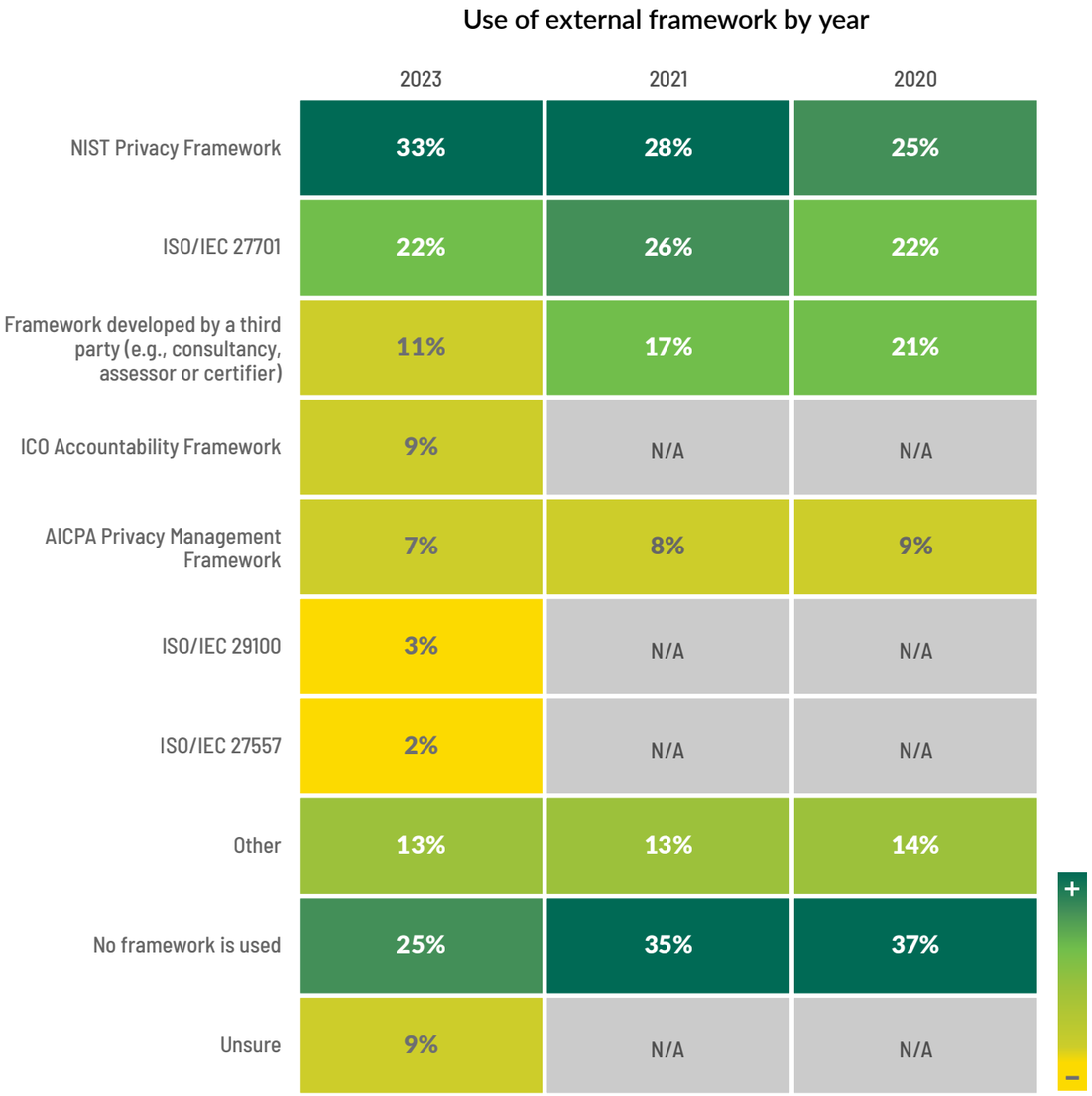
Another factor is budget. Respondents were significantly more likely to indicate challenges in using metrics to report on privacy compliance if their privacy budget was described as less than sufficient. The biggest challenge reported by those with less-than-sufficient budgets was the absence of a clear mandate for privacy, at 43%. This seems to indicate privacy teams with insufficient budgets may be employed by organizations that do not see them as essential.

Standards and frameworks

To alleviate these issues, many standards and frameworks exist to help privacy pros implement, among other things, a metrics-based approach to privacy. In the 2020 and 2021 surveys, respondents identified which external frameworks they use for their privacy programs. This question was asked again this year, considering the release of new materials like the International Organization for Standardization/International Electrotechnical Commission standard 27557 and U.K. Information Commissioner's Office Accountability Framework.

Primarily, the use of some type of standards or frameworks has increased since 2020, with 25% of respondents claiming not to use a framework this year, down from 37% in 2020. Additionally, use of the U.S. National Institute of Standards and Technology Privacy Framework increased from 25% in 2020 to 33% in 2023.

Use of frameworks can be payed forward in other ways: 31% of organizations that identified a lack of board-level understanding of privacy as a reporting challenge do not use a framework. Similarly, 34% of organizations that identified the absence of a clear mandate for privacy as a reporting challenge do not use a framework. In both cases, these percentages are significantly higher than the overall average of 25%. This illustrates a few of the many ways integrating frameworks can help alleviate reporting challenges.



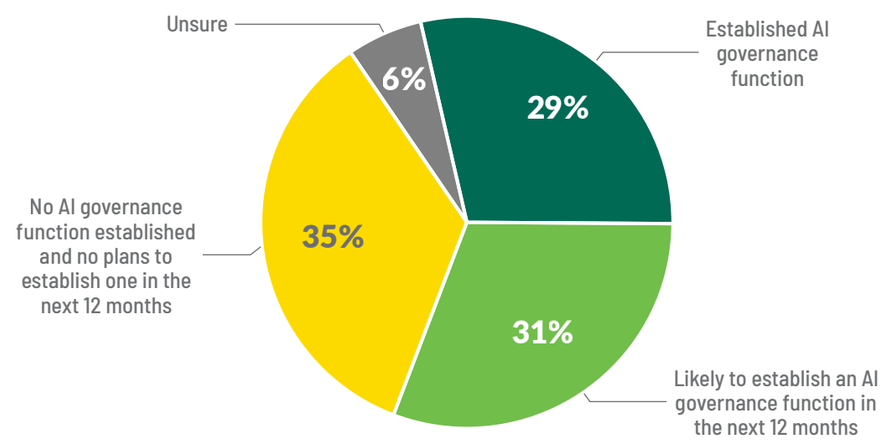
**N/A: Data not applicable as it did not appear in the 2021 or 2020 survey.*

AI governance — so much more to come!

Of respondents, 57% said their company's privacy function has acquired additional responsibility for AI governance.

Anticipation and anxiety levels related to use of AI are at all-time highs. Scientific breakthroughs, technological invention and innovation, real-world harms, and seemingly dystopic futures dominate discussion. A clarion call has been sounded. The safe and responsible development, integration and use of AI requires effective governance. This year's survey asked organizations to share whether they use AI, how they use it and how they govern it. Responses reveal, for the first time, how organizations have geared or are gearing up for AI governance. Responses – broken down by geography, sector and organizational size – included which functions and professionals are taking on the responsibility of AI governance, what tools and frameworks are being leveraged and what challenges organizations are facing.

Existence of an AI governance function



The new IAPP AI Governance Center, in partnetship with EY, will publish the full results in a separate dedicated report, the IAPP-EY Professionalizing Organizational AI Governance Report. While a lack of industry consensus on which department carries primary responsibility for the AI governance function remains, the privacy function leads the way in taking on the additional responsibility.

Of survey respondents, 57% said their organization tasked the privacy team with some responsibility for AI governance, with legal and compliance and security coming in at 55% and 50% respectively. Considering 75% of organizations said they are either already using AI products or plan to within the next twelve months, the need for action in the AI governance space is clear.

IAPP-EY Professionalizing Organizational AI Governance Report coming December 2023.

Our research approach

Our Research and Insights team focuses on bringing our membership accurate, meaningful and actionable privacy research and insights in a digestible way.

We do this by leveraging our team of internal experts and global network of subject matter experts, professionals and volunteer contributors.

Scope

We asked our global membership base to complete the 43-question governance survey. Over the course of 5 weeks, from May to July 2023, more than 500 individuals from over 50 countries and territories responded.

Visit the IAPP Resource Center for more privacy-related resources, including legislation trackers, tools, guidance, surveys and in-depth reports.

Contacts

Connect with the team

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

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

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

Joe Jones
Director of Research
and Insights, IAPP
jjones@iapp.org

Follow the IAPP on social media

Published November 2023.