iapp

Privacy Governance Report 2024

Table of contents

What's inside?

Foreword

The hallmarks of privacy professionalism inspire and instill confidence.

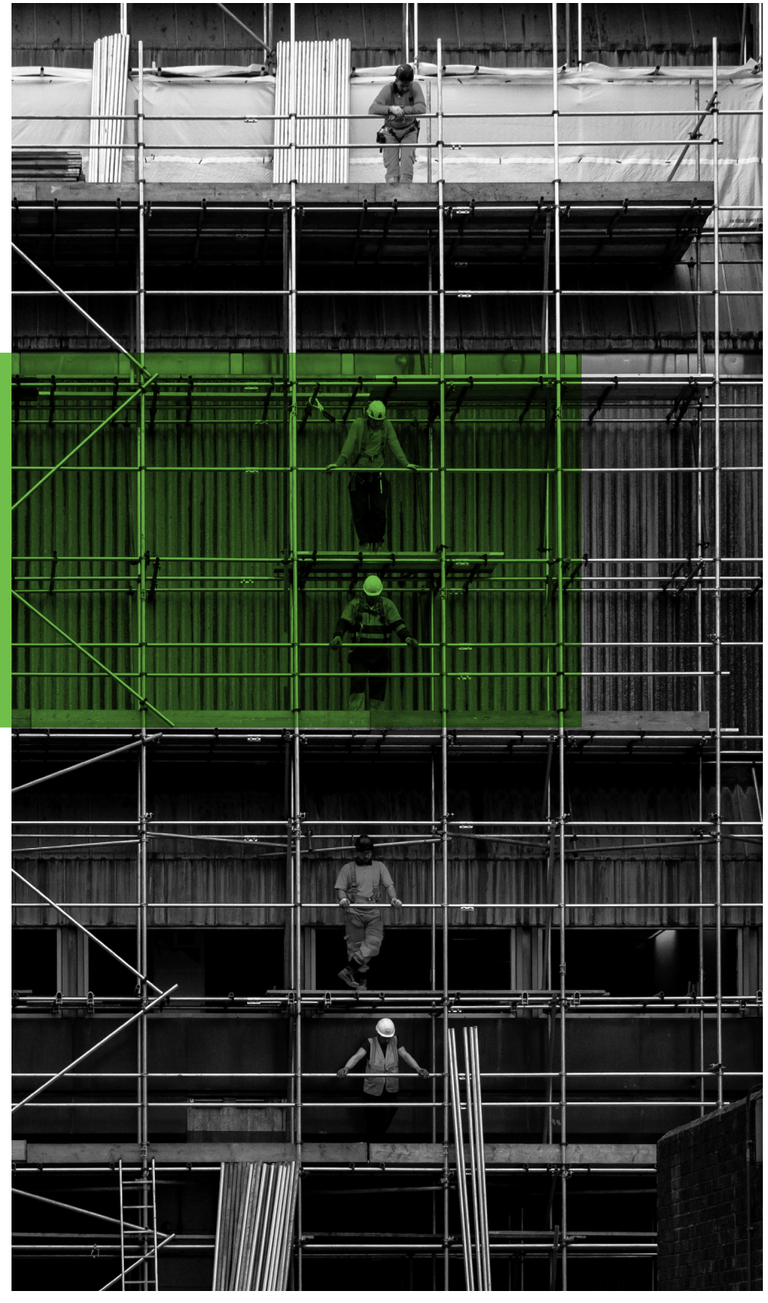
In the poignant and romantic poem "Scaffolding" by the late Nobel laureate Seamus Heaney, it is the astute, diligent and preparatory work of masons in securing scaffolding that enables "walls of sure and solid stone" to be built. It is the professionalism of masonry that inspires confidence. Confidence that the walls built within the frame of secure and tested scaffolding can not only withstand the buffeting of pressure, the creaks and the cracks that come with time and change but also that those walls can grow.

For decades, the profession of privacy has sought to scaffold the sure and solid walls of today's data-driven technologies, economies and societies. History has shown early investment in a professionalized workforce pays dividends later. Against a global backdrop of fiscal pressure and geopolitical instability, the advent and proliferation of new data-driven technologies, increasing privacy regulation, consequential privacy enforcement and litigation have all underscored the importance of effective and professional privacy governance as an enabler and a point of differentiation.

Despite these challenges, the profession has continued to demonstrate an extraordinary capacity for adaptation and resilience, ensuring organizations not only remain compliant with stringent regulations but also uphold the trust and best interests of their customers. In fact, nine out of 10 respondents to this year's survey reported being at least somewhat confident with their organizations' privacy governance program. For them, the privacy governance "wall" has been built.

The IAPP Privacy Governance Report 2024 charts how the efficacy of, and corresponding confidence in, an organization's approach to privacy governance stems from the investment in the hallmarks of privacy as a professional discipline. Those hallmarks — the people, techniques and tools — have scaled, matured and evolved in ways that are resilient and responsive to change. They place the privacy profession and privacy governance in a prominent position to take on broader and heightening responsibilities, spanning artificial intelligence governance, cybersecurity and content moderation to name a few.

The storied history of the privacy profession can inform our expectations about the future growth of digital governance and its professionalization within organizations. 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 in law and policy, technology, business management, and design. The resulting professionalization of the field has generated an accepted body of knowledge, training programs and credentials, as well as a vibrant and convivial global community of practitioners and leaders.



A recurring theme in this year's report is how sustained investment and elevated prominence for privacy governance and the professionals commanding its work results in more robust and more confident practices. Within organizations, privacy champions, practitioners and leaders drive privacy decision-making and awareness across business lines and teams. Strong visionaries and leaders have set the tone for privacy within organizations advocating for data protection as not just a legal obligation, but a core component that should be incorporated into the foundations of business strategy.

What's more, this investment and prominence in privacy governance is being paid forward and leveraged in newer and emerging frontiers spanning the gamut of digital governance.

It's professionalization — and the people, processes and practices that comprise the profession — that increasingly serves as the scaffolding for the emerging structures of digital governance that need "sure and solid" building. We will be more confident because of it.

Joe Jones
Director of Research and Insights, IAPP

Executive summary

Over 80% of privacy professionals have been tasked with an additional responsibility alongside their existing privacy day jobs.

Privacy compliance and how organizations aspire to achieve a better compliance posture remain an ongoing focus for most organizations. Almost all organizations process personal data in some form or another to deliver their business objectives, from small organizations solely processing personal data of a few employees to large multinational organizations processing vast quantities of sensitive personal data every minute to deliver tailored services to consumers.

Has your privacy function acquired additional responsibility*?

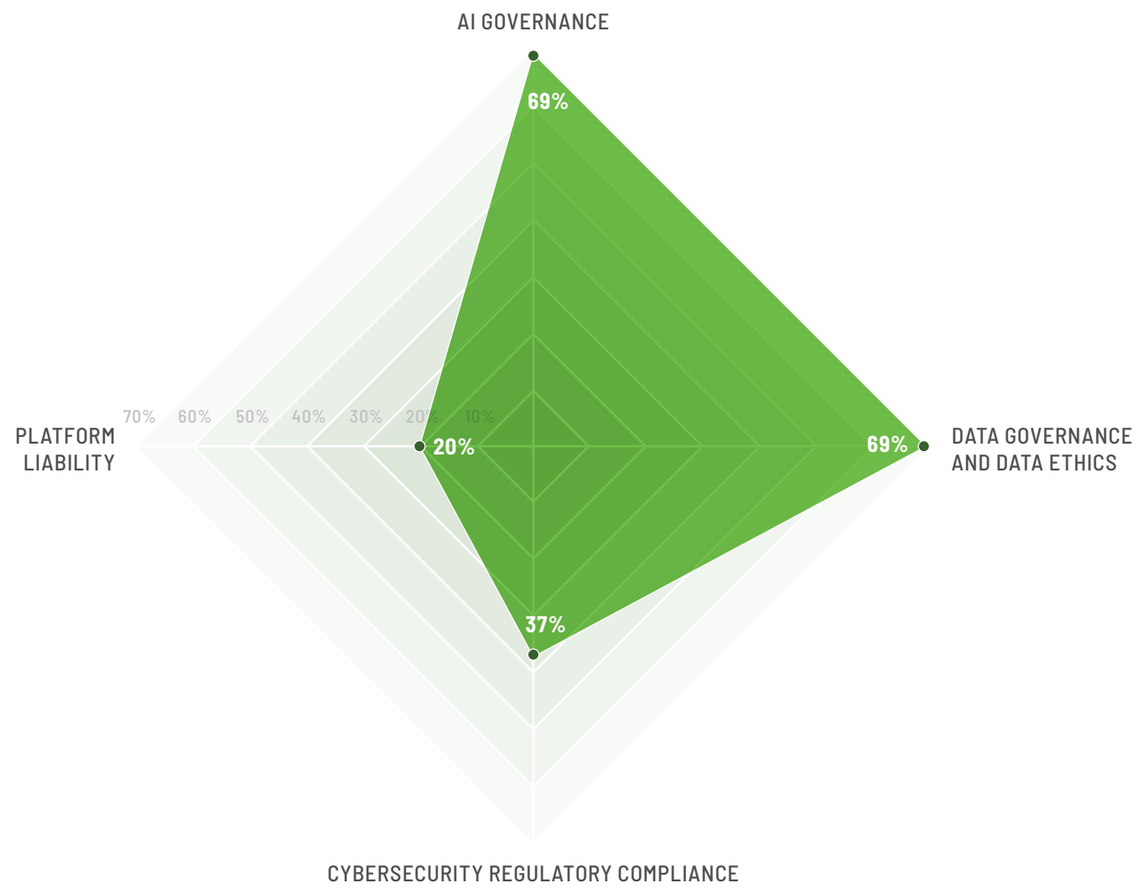
** Domains that make up additional responsibility: AI governance, consumer protection, human rights, content moderation and online safety, platform liability, data governance/data use/data as an asset, data ethics, competition/antitrust, cybersecurity as a regulatory compliance matter, product liability, intellectual property, and digital architecture and infrastructure.*

Developments in recent years have only highlighted the importance of the privacy profession due to the need for better compliance practices to protect individual rights when personal data is being processed effectively and for appropriate responses in the aftermath of various data breaches or ongoing technological developments. Privacy pros increasingly play an important role in enabling their respective organizations to deliver on core business objectives and remain competitive going forward.

However, privacy pros are no longer solely focused on a narrow remit. Increasingly, organizations are looking at these professionals to address the complex environment both internally and externally. As a result, privacy pros are increasingly tasked with additional responsibilities. This year's survey found the vast majority have been asked to take on further responsibilities on top of their day-to-day jobs. Existing C-suite leaders of specific domains are seeing their personal obligations expanded and elevated. For example, among surveyed chief privacy officers, 69% have acquired additional responsibility for AI governance, 69% for data governance and ethics, 37% for cybersecurity regulatory compliance, and 20% for platform liability.

This trend continues at the team level, with more than 80% of privacy teams gaining responsibilities beyond privacy. At 55%, more than one in two privacy pros work in functions with AI governance responsibilities, at 58%, more than one in two have picked up data governance and data ethics, at 32%, almost one in three cover cybersecurity regulatory compliance, and, at 19%, nearly one in five have platform liability responsibilities.

The expanding remit for CPOs



Increasingly, boards are looking for privacy pros to help deliver broader organizational compliance activities.

Privacy pros globally and across organizations of various sizes and industries have more on their plates. This is driven by several factors that introduce increasing complexities in the broader environment. Factors include growing complexity in law, policy and the regulatory environment; more consequential enforcement; growing use of more complex technologies; increased workload due to privacy requests; the need to address ongoing and new challenges; managing and responding to data breaches; and increasingly, boards looking for privacy pros to help deliver broader organizational compliance activities.

Organizations have responded to this growing complexity with increased privacy budgets and more senior privacy leaders in charge of growing privacy teams. Additionally, they prioritize limited resources on the right strategic compliance priorities, focusing on privacy training, establishing mature privacy risk management approaches and utilizing technology to enable and support compliance when possible. The remainder of this report seeks to explore these complexities, the impact on compliance and resulting organizational responses in greater detail.

Saz Kanthasamy
Principal Researcher, Privacy Management, IAPP

Cheryl Saniuk-Heinig
Research and Insights Analyst, IAPP

Luke Fischer
Former Westin Fellow, IAPP

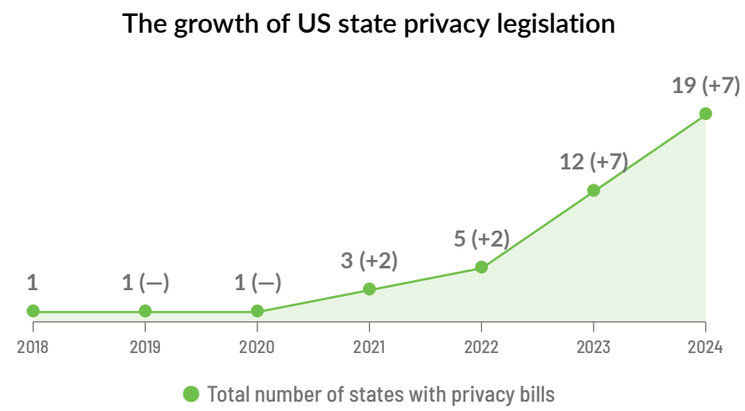
Part I. Increasing complexity

A growing list of interconnected challenges continues to be heaped onto the plates of privacy pros.

Growing complexity in law, policy and the regulatory environment

The existing legal environment in the privacy domain is complex, with a patchwork of global, national and sometimes local laws that impact data collection and processing. The growing number of privacy laws and regulations around the globe have resulted in ever-increasing compliance obligations and challenges for organizations.

This landscape is only growing more complex. Numerous jurisdictions have actively introduced, passed or amended privacy laws this year. The EU AI Act went into effect, marking the continent's first AI regulation. The state law privacy landscape in the U.S. has skyrocketed recently, with seven comprehensive state privacy bills signed in 2023 and seven more signed in 2024.



The U.S. also saw the most movement on comprehensive privacy legislation at the federal level in years with the American Privacy Rights Act, though it stalled in the House of Representatives. With new legislation and regulations, professionals must remain mindful of localization norms across jurisdictions, from India's blacklist approach to cross-border data transfers to Kenya's security exemptions allowing access to personal data from any device. Each of these legislative developments adds to the intricacy of the privacy landscape that organizations are continuously adapting to. With 70% of nations and 79% of the world's population now covered by some form of national data privacy law, the burden on privacy teams continues to grow.

Beyond the sheer number of privacy laws enacted this year, the increasing connectedness of privacy laws with nonprivacy laws furthers the challenges organizations face with compliance. For instance, an overlap between competition and privacy laws in the EU impacts online advertising technology, exacerbating compliance challenges for organizations in the adtech space. In response to the interconnectedness of laws like these, groups like the U.K. Digital Regulation Cooperation Forum are working to coordinate their regulatory disciplines and authorities in charting a straightforward approach for applying digital legislation and to provide organizations with more consistency.

Furthermore, the evolving policy and regulatory environment is impacting organizations. Companies facing or at risk of regulatory action must grapple with operational decisions such as dedicating resources to implement more robust data governance frameworks, creating or leveraging advanced technologies internally, and ensuring organizational resilience in the rapidly changing landscape. Though not entirely unexpected, evolving policies force organizations to pivot their practices.

Finally, consumers' expectations for privacy continue to grow. Now more than ever, consumers are aware of their rights, and privacy issues are at the forefront of their minds. They understand the implications of AI models processing personal data, are aware of privacy risks and data breaches, and are increasingly aware of the consequences of getting privacy wrong.

Against all this, and in large part due to the professionalization of privacy, most survey respondents are confident in their ability to stay informed about new privacy laws and policy initiatives, with 43% overall reporting they are totally confident. However, one in five reported the difficulty in keeping up with continually evolving privacy laws creates challenges in delivering privacy compliance. Organizations are developing ways to iterate, scale and further professionalize their privacy governance programs and processes in the face of new, scaling and compounding challenges.

More consequential regulatory actions

Once confined to discussions within the inner circles of privacy pros, analysis of the scrutiny and enforcement actions of privacy regulators now dominates even mainstream news cycles due to the consequential and downstream nature of the actions' impacts. Recent examples include the European Data Protection Board's opinion on the pay-or-consent model, the EU AI Act officially entering into force, as well as global regulatory scrutiny and lawmaking on issues related to children's privacy and online safety.

This heightened regulatory activity impacts not just the privacy practices of organizations but, more broadly and significantly, the foundations and models of how businesses operate. Organizations that are directly subject to regulatory action may have no choice but to change their privacy compliance practices. But what of organizations that are not directly subject to regulatory action? Data from this year's survey shows one in five respondents changed their privacy approach because of enforcement or litigation actions against other organizations.

Respondents working at organizations with privacy budgets of more than USD2 million were most likely to have changed their privacy approaches, split almost equally between changing as a direct response to an action and as an indirect response. This suggests the scale of the privacy program may be a factor in whether an organization is able to conduct the activities necessary to respond to broader regulatory changes. For organizations that have changed their approaches, this may include enhancing horizon-scanning activities, engaging external and/or internal legal counsel to assess legal requirements, understanding the impact of changes, and taking a risk-based approach to implementing required changes. Organizations that fail to react to consequential market-impacting privacy regulatory requirements may find themselves noncompliant when compared with competitor organizations. Privacy pros are, therefore, contending with more complexity introduced by the need to maintain a macro view of actions by regulators.

Almost half of respondents working in organizations with privacy budgets totaling USD250,000 or more have changed their privacy approaches in the last year.

Growing use of more complex technology

The rapid proliferation of technology further adds to the complex and varied workload faced by privacy pros. The dizzying list of developments spans from AI technologies to increased automation, augmented and virtual reality, personalized medical services, and neurotechnology or quantum computing, to name a few. Often, collecting and processing personal data is at the heart of these technologies, and privacy pros need to balance their organizations' strategic desire to gather more valuable insights from data with privacy and broader digital governance requirements.

Many organizations have responded to the utilization of AI by deploying AI governance functions tasked with managing this risk. Notably, 77% of this year's survey respondents identified their organizations are currently working on AI governance. Looking ahead, it is unlikely organizations will respond to each new development by forming a stand-alone governance function, such as quantum computing or neurotechnology governance. Instead they may seek to evolve existing structures into a streamlined digital governance approach. This is further outlined in the Organizational Digital Governance Report 2024.

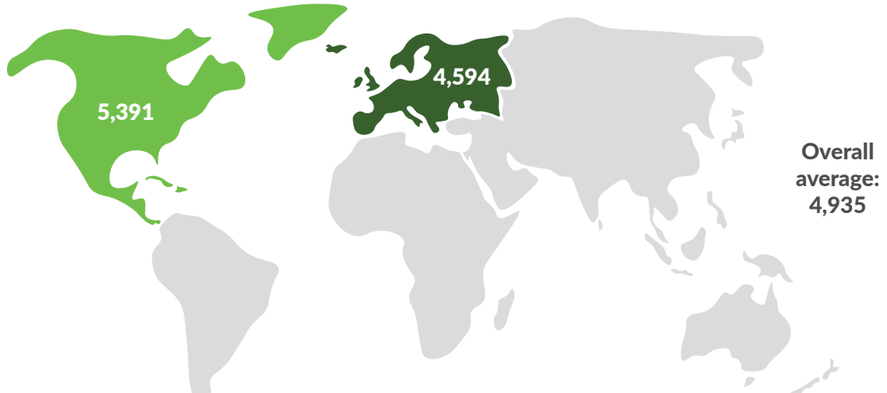
Increased workload due to privacy requests

Privacy functions are meeting the moment and responding in commensurate terms to the trends and developments shaping their new and increased workloads. Privacy functions face many varied priorities, from responding to data subject right requests from increasingly privacy-conscious and statutorily empowered individuals to providing subject matter expertise on privacy impact assessments. This year, we sought to understand the number of these requests fielded by organizations.

On average, organizations are processing nearly 5,000 privacy compliance-related requests, which this report calls "metrics," per year. Respondents working for organizations headquartered in Europe reported around 4,500 metrics, while North American organizations averaged around 5,400.

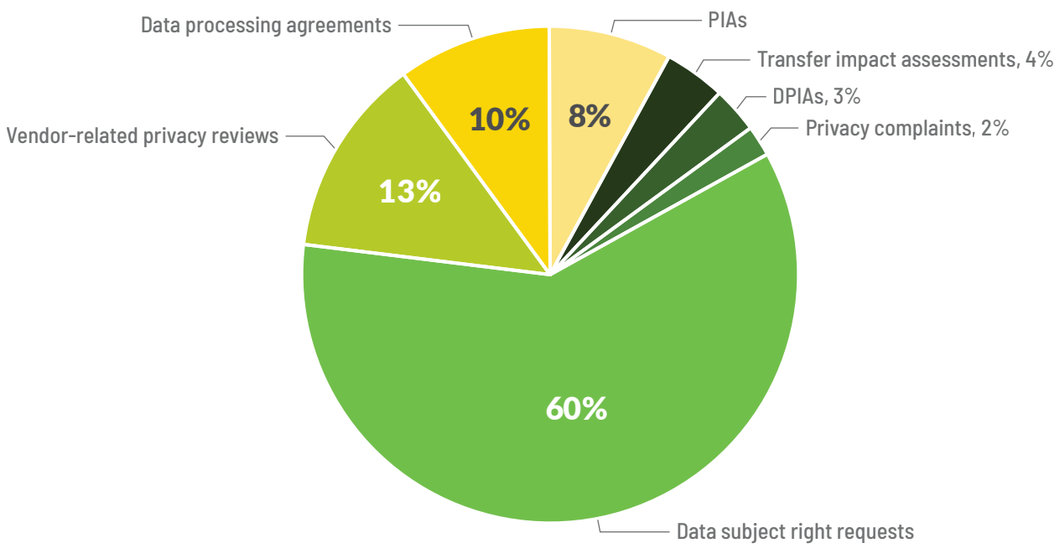
This report refers to privacy function responsibilities, such as impact assessments, requests and processing, as "metrics" to capture the activities completed by privacy teams that may vary drastically across jurisdiction and industry.

Average number of privacy metrics processed and completed per organization in 2023 by headquartered region



	Overall	North America	Europe
Privacy impact assessments	393	250	707
Data protection impact assessments	153	81	357
Data subject right requests	2,972	3,519	2,138
Transfer impact assessments	174	78	498
Vendor-related privacy reviews	638	819	364
Privacy complaints	108	115	124
Data processing agreements	498	529	406
Total	4,935	5,391	4,594

Proportion of privacy metrics completed on average in 2023



What is the impact of this? A rudimentary but likely common set of assumptions applies, including:

- The average full-time employee works a 40-hour week with five weeks of annual leave, 10 days of public holiday and three days of sick leave.
- Between one and two full-time employees would need to work full time on privacy requests when each request takes 30 minutes to completely process.
- Seven full-time employees would need to work full time on privacy requests when each request takes 2.5 hours to completely process.

Organizations in the consumer goods and services sector processed and completed an average of 15,000 privacy requests per year, compared to the government and manufacturing sectors' average between 500 and 700 per year. Respondents working in retail organizations with closer relationships with end consumers reported responding to the highest number of privacy complaints, which was 143 times higher than the lowest reported number in the primarily business-to-business manufacturing industry.

Number of privacy metrics processed and completed by organization in 2023

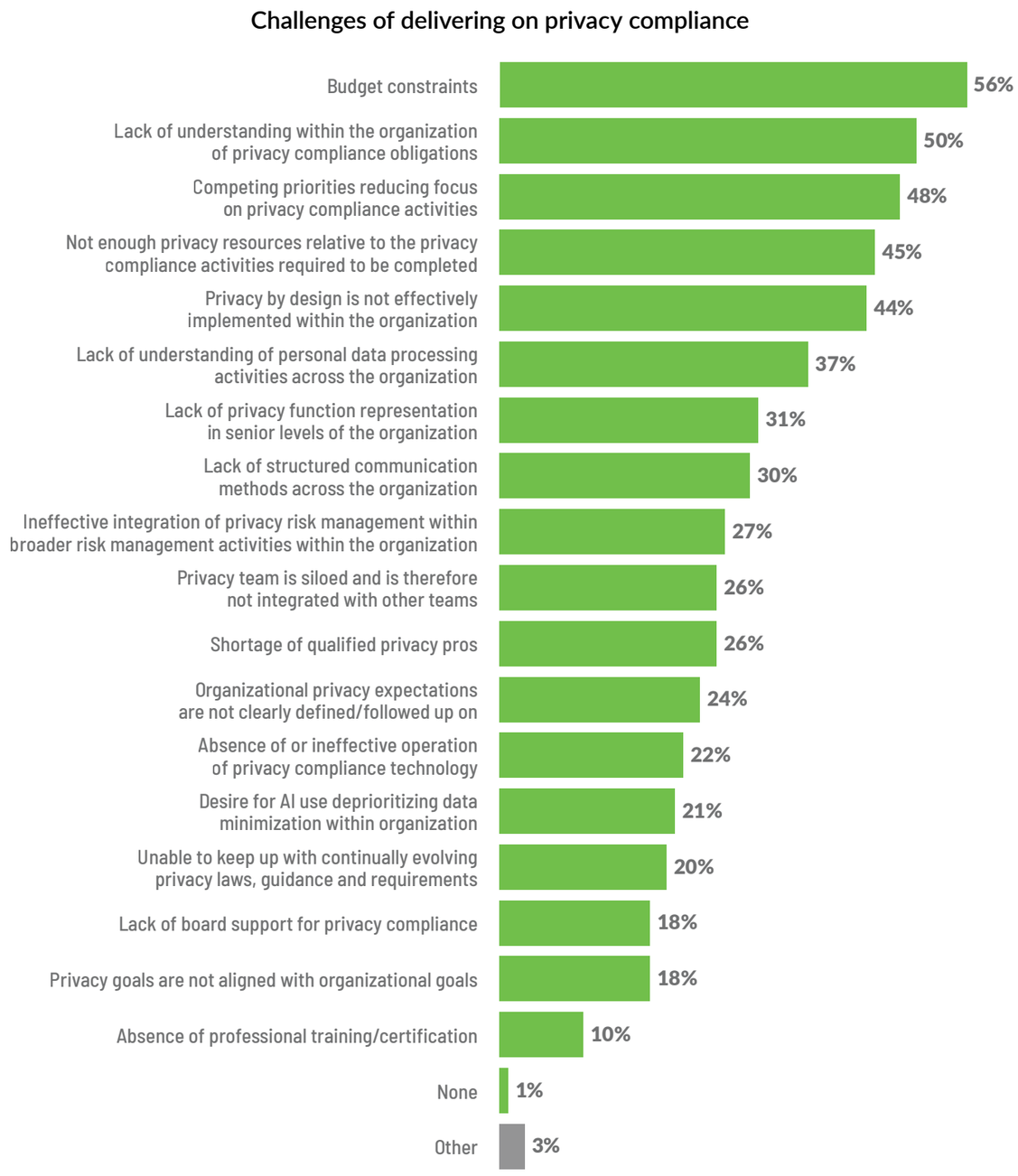
	BY INDUSTRY										BY NUMBER OF EMPLOYEES					
	Banking and insurance	Technology and telecommunications	Education and nonprofit	Business services	Consumer goods, services and retail	Government	Life sciences and health care	Legal	Manufacturing	Other	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	More than 80,000
PIAs	1,086	603	51	396	239	131	112	417	84	191	7	14	127	224	557	2,275
DPIAs	459	147	49	362	94	83	38	61	43	59	5	11	41	90	210	892
Data subject right requests	1,568	6,285	966	542	12,870	229	1,861	41	46	2,531	132	760	2,091	2,781	6,772	8,176
Transfer impact assessments	71	111	18	2,297	100	25	45	12	9	70	4	7	20	84	139	1,234
Vendor-related privacy reviews	2,170	320	87	333	1,628	46	270	233	255	246	34	62	213	276	989	3,685
Privacy complaints	159	131	33	53	286	46	165	32	2	52	3	4	65	61	325	378
Data processing agreements	235	917	89	1,550	387	138	344	621	97	565	30	329	447	403	1,065	953
Total	5,749	8,513	1,293	5,531	15,604	697	2,836	1,417	536	3,715	216	1,188	3,004	3,919	10,056	17,593

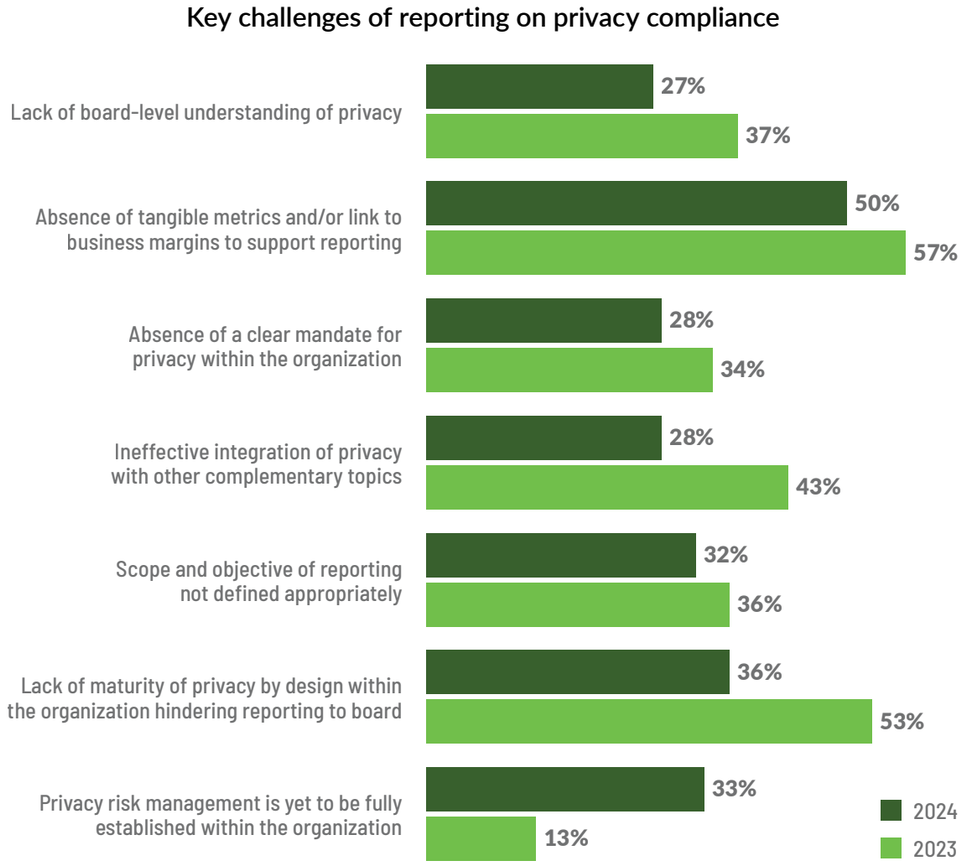
Need to address ongoing and new challenges

Whether respondents reported having additional responsibilities or not, fundamentally, the entire industry still faces the challenge of delivering similar privacy compliance requirements to their organization.

Of respondents, 99% reported facing challenges delivering privacy compliance. Respondents who reported any challenge delivering privacy compliance, including "other," were most likely to also report either budget constraints or that lack of understanding of privacy compliance challenges within the organization was a challenge.

Of respondents, 55% reported experiencing five or more challenges delivering compliance, with 15% of all respondents reporting they experienced 10 or more challenges. Yet nearly one in 10 respondents identified zero or only one challenge in delivering privacy compliance for their organizations. Nevertheless, these challenges are neither stagnant nor permanent. Organizations facing no challenges today could face new ones tomorrow. Evolving threats will continue to emerge and impact organizations, and privacy pros must continue to innovate to confront these challenges to ensure ongoing compliance.





Compliance requires tools, budget, time and innovation. In addition to striving for compliance, organizations have reporting lines for compliance to inform those at the top of its status, challenges and needs.

Despite being tasked with several new responsibilities, privacy pros continue to report recurring challenges with compliance reporting. This year, one in two respondents identified the absence of tangible metrics and/or a link between metrics and business margins that support internal reporting as a key challenge in reporting on privacy compliance. This number is similar to the one in the 2023 report, identifying this as a trending challenge, regardless of organization size.

Respondents who continue to face challenges in reporting compliance may find it more difficult to report on progress, triage compliance issues and ultimately improve compliance efforts, including securing budget increases if required.

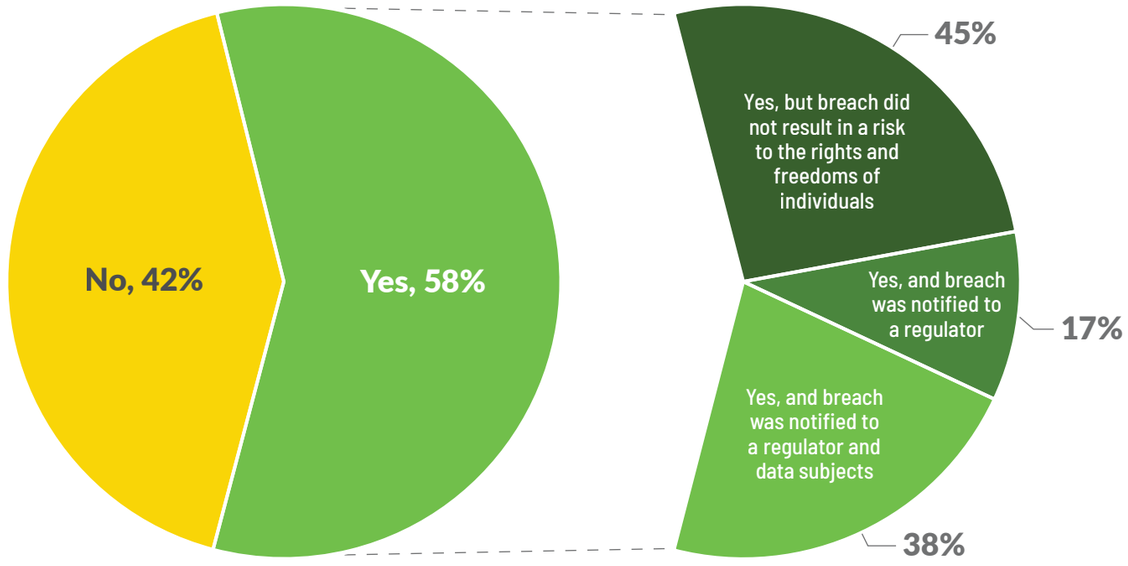
Managing and responding to data breaches

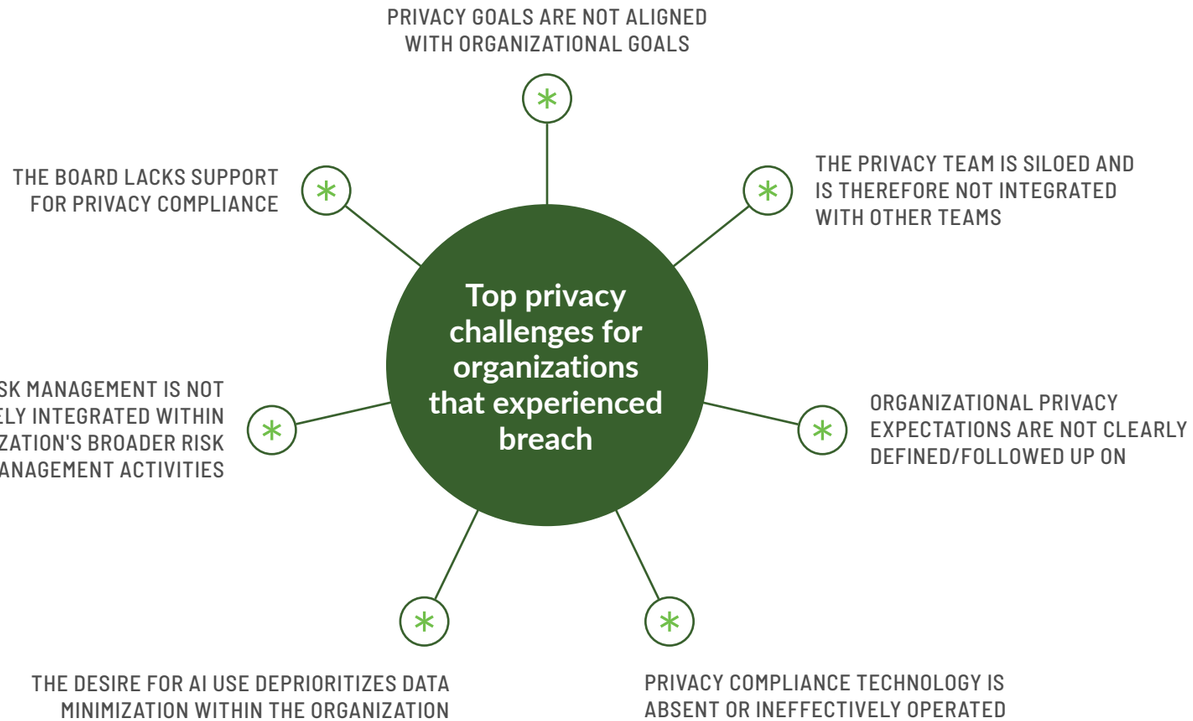
Most organizations will experience data breaches, but standardized response plans help privacy pros remain confident in compliance.

Breaches in security are considered an occupational hazard in the face of modern data processing activities. The need to respond to the impact of a breach requires privacy pros to be on top of their game, as it will also impact work in progress and potentially divert resources from existing projects. Half of this year's respondents identified their organizations experienced a breach within the last year. Of those respondents, 55% stated the breach warranted reporting to a regulator, while 38% identified it was reported to both a regulator and to affected data subjects.

When considering confidence in compliance, the trend is clear. Respondents who were less confident in their organizations' compliance with privacy laws and policies were more likely to work at organizations that had experienced a data breach. Of those not at all confident in compliance, 76% of respondents worked for organizations that had experienced a data breach. Over half of these respondents' organizations had experienced a higher severity breach and notified data subjects and/or a regulator. On the other hand, seven in 10 respondents who were more confident in their organizations' privacy compliance were more likely to work for organizations that either did not experience a breach or experienced a breach that did not result in risks to the rights and freedoms of individuals.

Proportion of respondents who identified their organizations experienced a data breach in the last year and the subsequent action taken





Respondents working at organizations that experienced breaches were more likely to identify their organizations faced a variety of privacy compliance challenges.

Standardized data breach response plans can aid organizations in the aftermath of a breach. These plans are a predefined set of protocols and procedures the organization can immediately follow to identify, contain, mitigate and recover from a breach. At 86%, the majority of respondents work at organizations with standardized response plans for data breaches.

Privacy pros who work at organizations with standardized response plans are more confident in privacy compliance than those who do not. Respondents who have confidence in their organizations are less likely to report privacy compliance challenges, such as a lack of structured communication methods, absence of privacy function representation at senior levels, siloed privacy teams, ineffectually implemented privacy by design, absence of effective privacy compliance technology operation, and reduced understanding of personal data processing activities across the organization.

Additional responsibilities for the privacy team

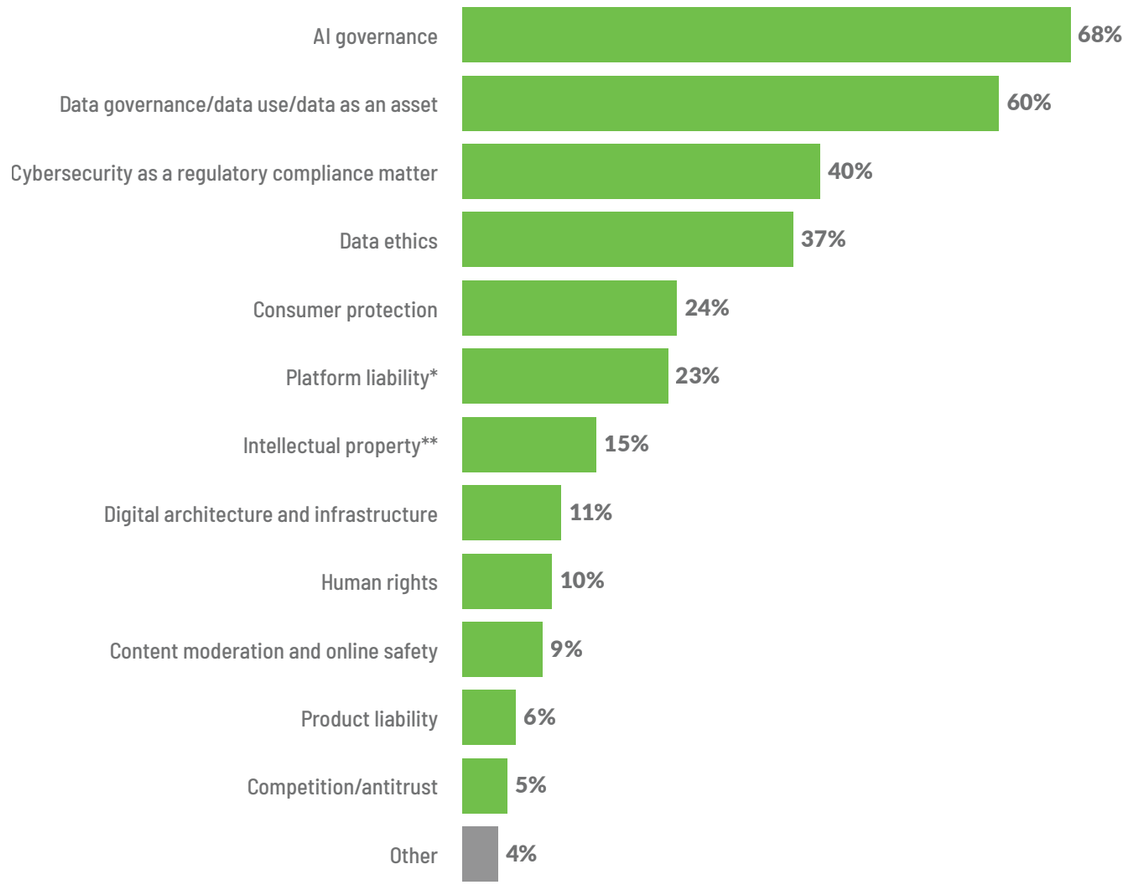
The growing complexity of law, policy and regulatory environments reflects the interconnectedness of privacy laws with nonprivacy laws. This year's survey identified over 80% of respondents have been tasked with an additional responsibility alongside their existing privacy job. Therefore, most privacy functions surveyed are evolving to help their organizations manage additional risks.

It is clear the job of the average privacy pro is changing. AI governance is likely to form a top priority for those who have acquired additional responsibilities. Of those with new responsibilities, 68% of respondents have acquired additional responsibilities for AI governance. Alongside this, data governance, cybersecurity as a regulatory compliance matter and data ethics are common additions to the workload of privacy pros. Two in five have been tasked with the complimentary topics of AI governance and data governance on top of existing busy workloads.

These responsibilities do not exist in a vacuum. Approximately 60% of respondents with new AI governance responsibilities also have new responsibilities in data governance, data use or data as an asset. One in five of those with new responsibilities have added AI governance, data governance and data ethics to their existing privacy portfolios.

Without sufficient skills or resources, this added workload could lead to burnout, missed targets and a steep learning curve for professionals to master. It may impact work quality. With sufficient support and staffing, however, organizations could benefit from potential efficiency gains, innovation, and economic and competitive impacts — if the employee can be retained.

Domains of respondents who acquired additional responsibilities



* Platforms include websites, internal platforms and other digital applications.
** This is limited to digital and regulatory compliance.

Part II. Compliance confidence

Despite growing complexities, privacy pros are tentatively confident in compliance with privacy requirements.

There is no metric to measure compliance perfectly, nor does it operate in isolation. However, one possible proxy measure is the extent to which privacy pros are confident in their organizations' privacy compliance.

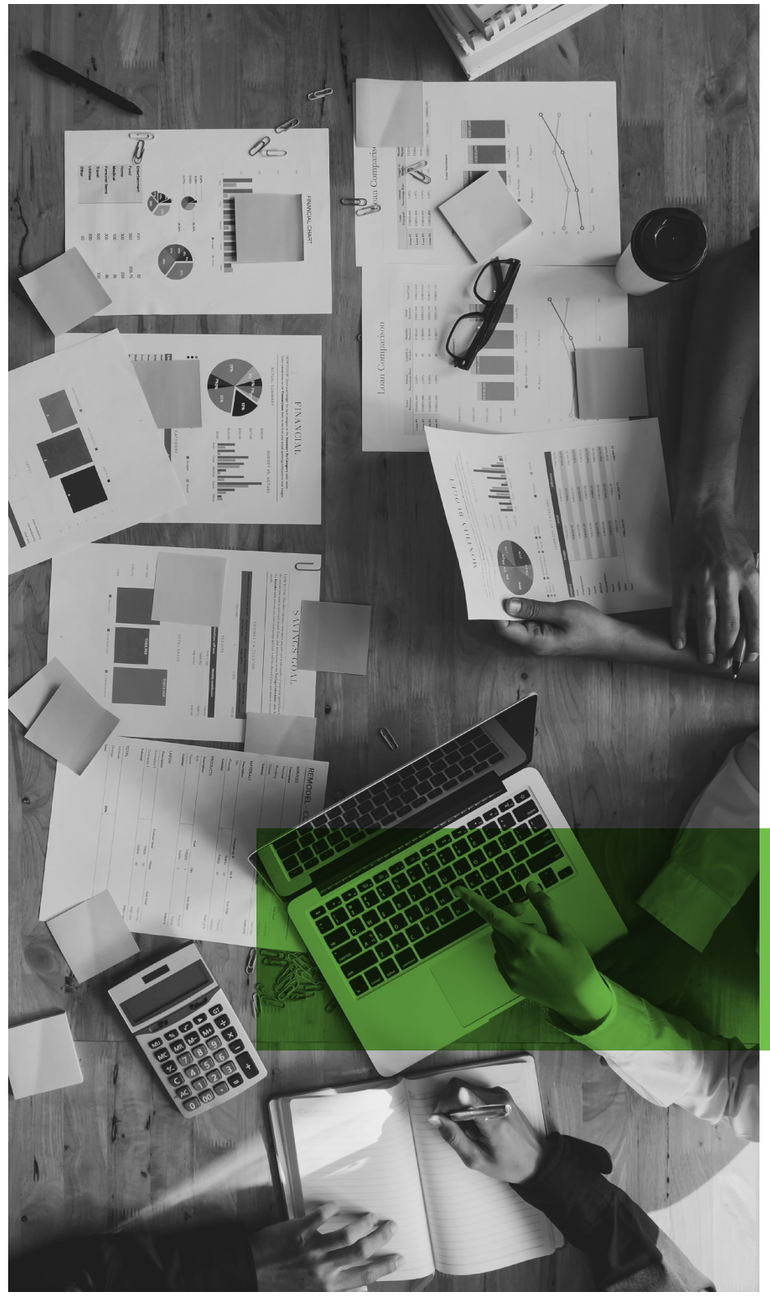
In 2024, two in 10 respondents were totally confident in their organizations' ability to comply with privacy regulatory requirements, and one in 10 were not at all confident.

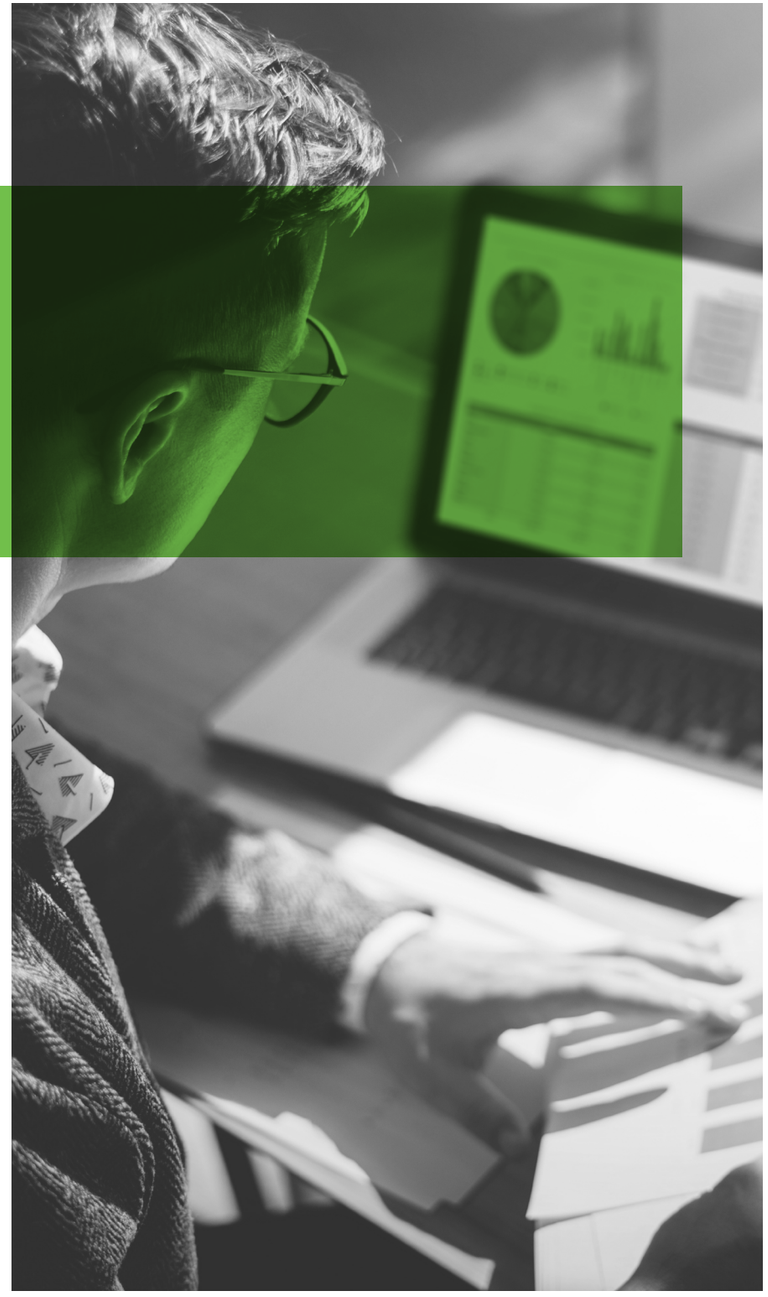
Those respondents were more likely to identify the following compliance challenges:

- → Lack of understanding of privacy compliance obligations within the organization.
- → Lack of understanding of personal data processing activities across the organization.
- → Lack of privacy function representation at senior levels of the organization.
- → Privacy by design not being effectively implemented within the organization.
- → Budget constraints.
- → Lack of board support for privacy compliance.
- → Not enough privacy resources relative to the required privacy compliance activities.
- → Competing priorities reducing the focus on privacy compliance activities.
- → Lack of structured communication methods across the organization.
- → Privacy goals not being aligned with organizational goals.
- → Organizational privacy expectations not clearly being defined or followed up on.
- → Ineffective integration of privacy risk management within broader risk management activities within the organization.
- → Shortage of qualified privacy pros.

Respondents who reported their teams have sufficient resources to complete their objectives were more likely to be totally confident in their organizations' compliance with privacy laws and policies across jurisdictions. Of those who were not confident in compliance, the majority, at 75%, also agreed a lack of the right privacy resources limits the organizations' ability to deliver its objectives.

Two out of three respondents who were not confident in their organizations' ability to stay informed about new privacy laws and policy initiatives were also not confident in their organizations' compliance with privacy laws. Effectively scanning the horizon, analyzing new requirements and translating this into prioritized actions remains an essential part of continued compliance.





In a similar trend, privacy pros who were not confident in their organizations' compliance were more likely to identify challenges in reporting on privacy compliance. Respondents who were not confident identified their organizations:

- Lack a clear mandate for privacy within the organization, at approximately 75%.
- Have not yet fully established privacy risk management, at approximately 72%. In the absence of privacy risk management, organizations are more likely to find it challenging to report on whether privacy compliance controls have been designed appropriately and are working effectively.
- Lack a board-level understanding of privacy, at 64%.
- Lack a mature implementation of privacy by design within their organization that hinders reporting to the board, at 64%.
- Face challenges integrating privacy with other topics and lack tangible metrics or a link to business margins that support reporting, at around 50%.

Almost nine in 10 of those who said they were not confident in their organizations' compliance were also likely to say their organizations have insufficient budgets. These results suggest privacy pros who are not confident in their organizations' compliance could face an uphill battle in improving compliance and thus in improving their confidence, considering all current compliance, reporting and budgetary challenges.

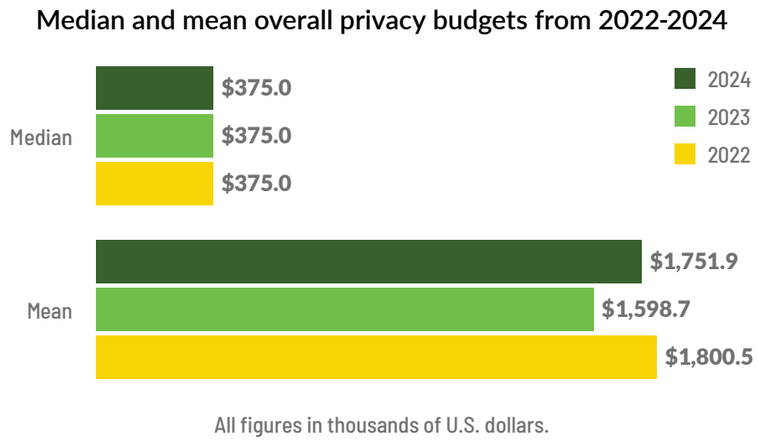
In 2024, 91% of respondents reported they were at least somewhat confident in their organizations' ability to comply with privacy regulatory requirements, with 21% reporting total confidence. Respondents who reported at least some confidence in compliance on average reported fewer challenges delivering on compliance and more confidence in their organizations' ability to stay informed about new privacy laws or policy initiatives. They were less likely to report a lack or limited availability of skills or resources restricted their ability to deliver on their objectives.

Part III. Addressing complexity

While the 2024 median privacy budget of USD375,000 remained identical for the third year in a row, the average privacy budget rose to USD1.75 million this year.

Budgeting

This year saw moderate economic growth with inflation and interest rates gradually retreating and recruitment increasing after years of hiring freezes. This year's relative increase in the average mean privacy budget may reflect healthier macroeconomic conditions as well as new, emerging and acquired additional privacy-adjacent and broader digital governance responsibilities. Both mean and median budget figures are included in this report to illustrate how the economic factors of 2024 impacted organizations differently.



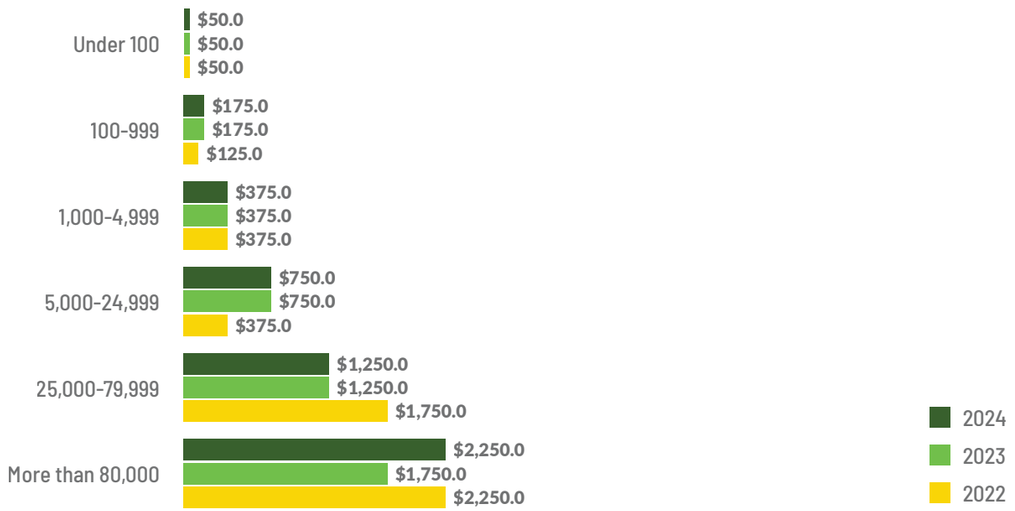
The trend unsurprisingly shows budget steadily increases based on organization size, either by revenue or by number of total employees.

What does the privacy budget look like?

The average privacy budget for 2024 is USD1.752 million, up from USD1.599 million in 2023. The median privacy budget for 2024 remains unchanged from 2022 and 2023. Viewed together, the privacy budgets for organizations may represent a moderate uptick in economic conditions over the past year as well as the growing obligations the privacy role continues to acquire.

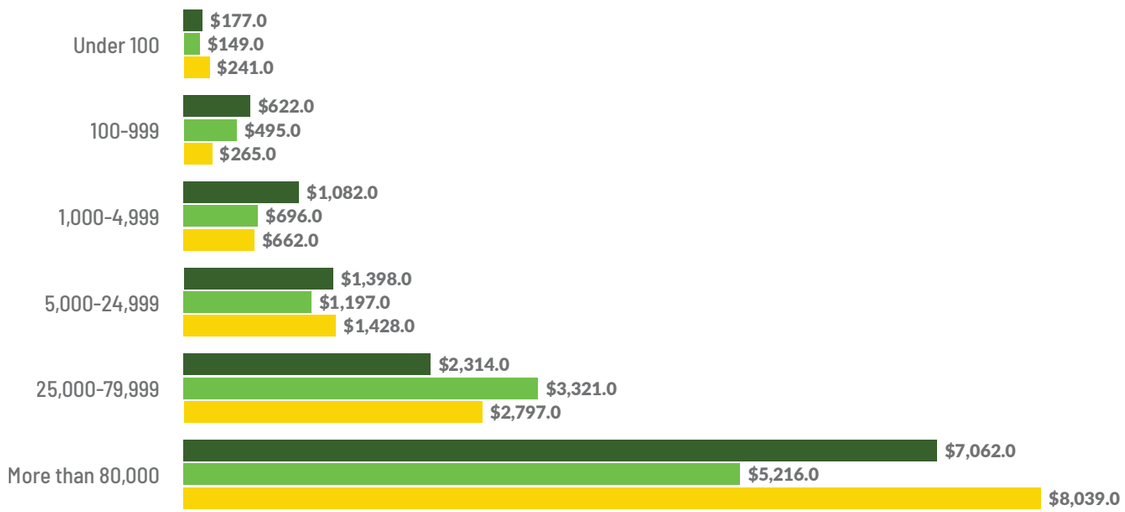
The trend unsurprisingly shows budget steadily increases based on organization size, either by revenue or by number of total employees. The average privacy budget for organizations that reported annual revenues of USD101-999 million is USD485,593, while the average for organizations with annual revenues of USD9-19.9 billion is USD2,447,015.

Median budget by total number of employees within an organization from 2022-2024

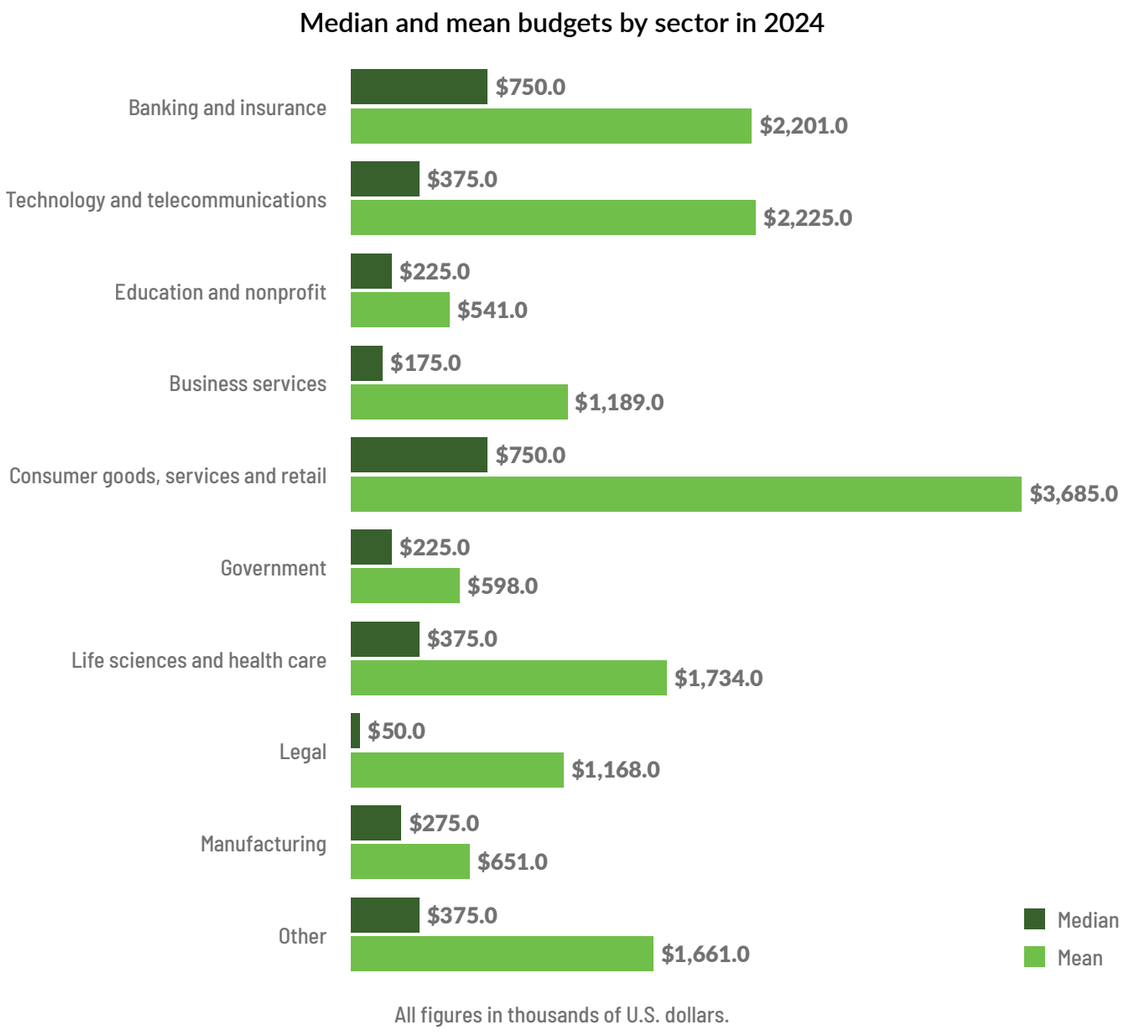


All figures in thousands of U.S. dollars.

Mean budget by total number of employees within an organization from 2022-2024



All figures in thousands of U.S. dollars.



Additionally, of organizations that indicated annual revenues of USD1-8.9 billion, 55% are above the median global privacy budget, significantly higher than the rest of the sample. This trend increases with organization revenue: 67% of organizations with a revenue of USD9-19.9 billion, 77% of those with revenue of USD20-59.9 billion and 90% of those with revenue of USD60 billion or more are above the median privacy budget. These results demonstrate that organizations with greater revenue have more resources to allocate to privacy duties, and organizations with more employees, and likely more privacy employees, have higher budgets to fulfill their privacy obligations.

Budget comparison by continent shows North America leads with a significantly higher median budget than other regions. The median budget of USD562,500 in North America is more than double Europe's USD225,000 and more than three times greater than Asia's USD175,000.

Despite some large Asian organizations reporting high allocations of resources for privacy, organizations in North America generally maintain higher median budgets. More robust U.S. budgets could be explained by healthier market conditions and the complexity of navigating the U.S. state privacy landscape, which has seen a proliferation of comprehensive state privacy laws passed and enacted in the last few years. Additionally, the stakes are high for noncompliance in the U.S. and Europe regarding enforcement actions against organizations that violate privacy laws.

Is it enough?

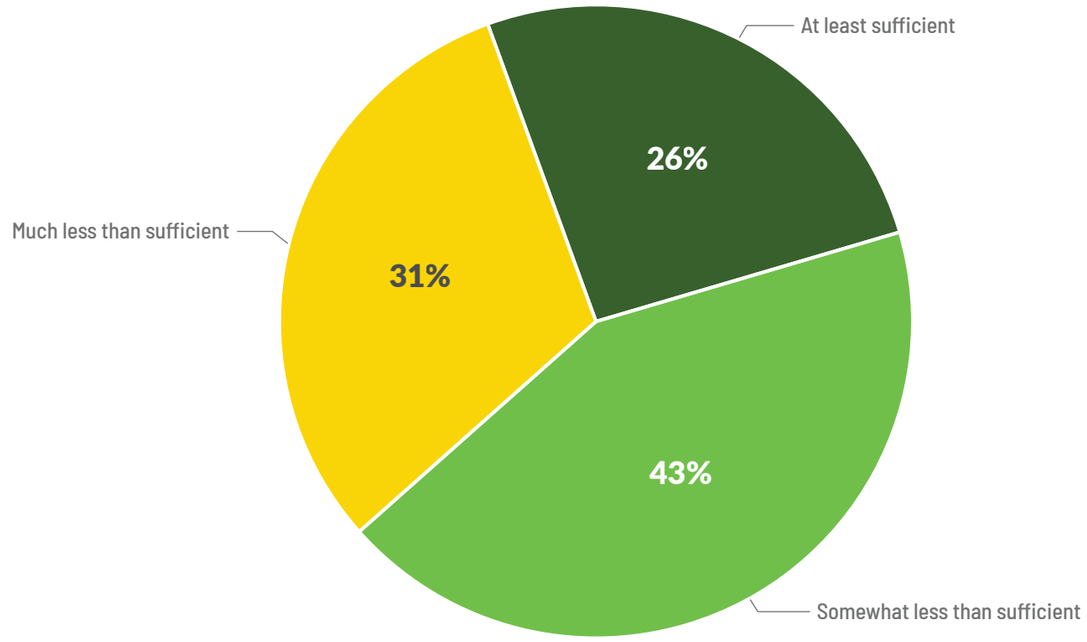
Lastly, respondents described how satisfactory their organizations' budgets are with respect to privacy obligations. Notably, only four in 10 respondents who said their organizations' budget was less than sufficient had above-median privacy budgets. Meanwhile, more than half of those who said their budget was at least sufficient had above-median privacy budgets.

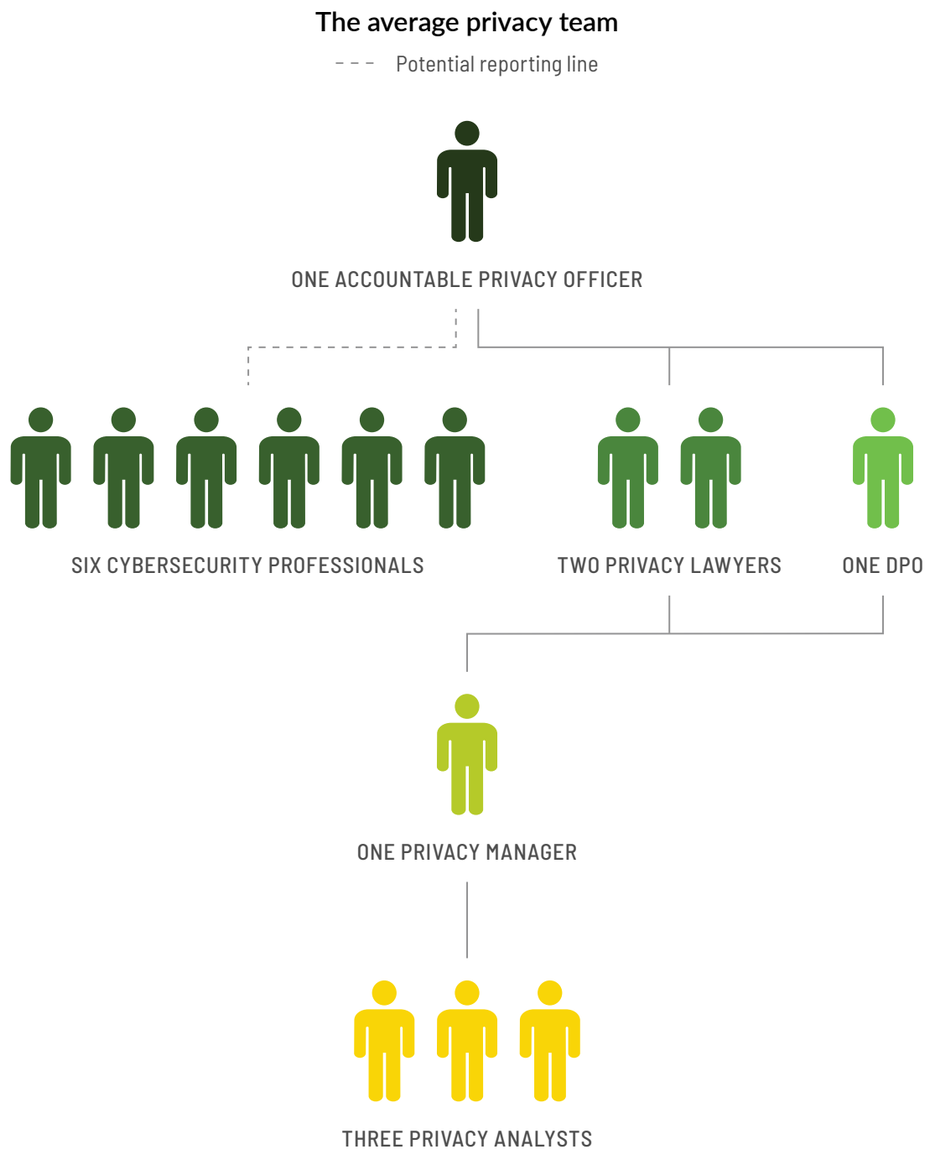
Of the respondents who described not being at all confident in their organizations' compliance with privacy laws and policies, 87% also noted their privacy budgets were less than sufficient. Of respondents who stated their budgets were at least sufficient to meet their privacy obligations, the vast majority, at 98%, were confident in their organizations' ability to remain compliant with privacy laws and policies.

Furthermore, privacy pros who said they believe their organizations' budgets are insufficient may face more challenges when delivering on privacy compliance. These shortfalls demonstrate that privacy governance and the development of proactive, holistic privacy programs are stunted when too few resources are allocated to the domain. In turn, such organizations may be incapable of meeting the required compliance demands.

With organizations beginning to loosen budgetary constraints, privacy pros should take this time to think strategically about advocating for budgets that will support the work needed to meet the profession's growing obligations.

Sufficiency of privacy budget with respect to privacy obligations





Resourcing and senior leadership

Having senior privacy leaders in charge of growing privacy teams may lead to greater confidence in compliance.

Composition of privacy teams

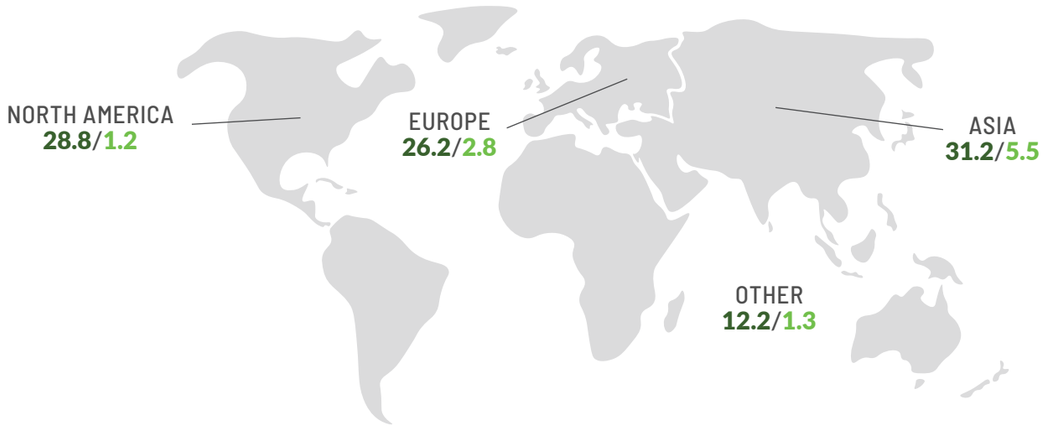
The parameters of the privacy profession continue to change, as do the resources needed for privacy teams to be successful. A privacy team's makeup is as diverse as the tasks they are responsible for. This year's survey sought to understand the varied roles, internal and external, that make up respondents' privacy teams. Internally, approximately half of respondents work on teams with an accountable privacy officer, privacy lawyer, cybersecurity professional, data protection officer, privacy manager and privacy analyst. The organizational chart on the left helps readers visualize the average privacy team and how its makeup changes with organizational demographic factors. This average changes depending on jurisdiction, company size, revenue and sector.

Approximately 70% of respondents in European organizations have at least one DPO, with an average of three to four full-time DPOs each. In comparison, only 40% of organizations headquartered in North America have a DPO, with an average of less than one full time DPO per organization. Privacy teams at organizations with privacy budgets between USD0 and USD499,000 on average are similar in size, with teams tending to double once the budget is over USD500,000. This suggests, regardless of budget, a baseline privacy team is required to deliver on privacy compliance activities.

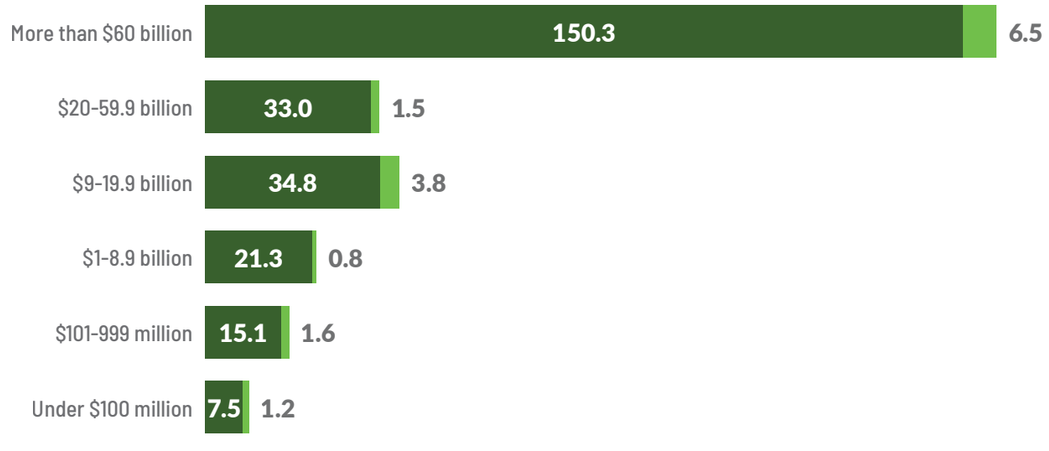
Average number of internal and external team members

Internal External

On average, organizations headquartered in North America and Asia have larger privacy teams than any other continent, though Asia has both the highest average for number of internal and external privacy employees

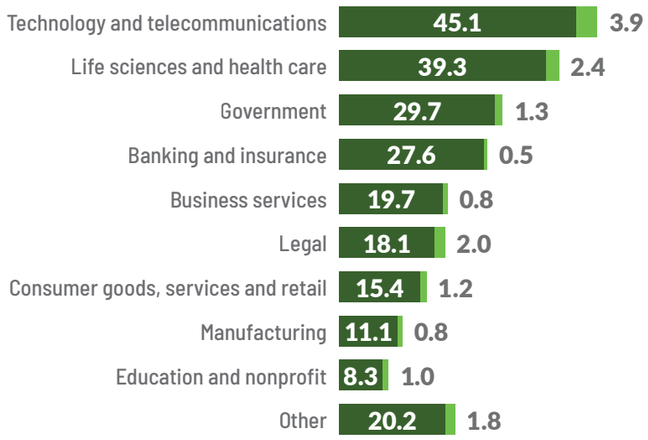


Average team size tends to grow proportionately with revenue

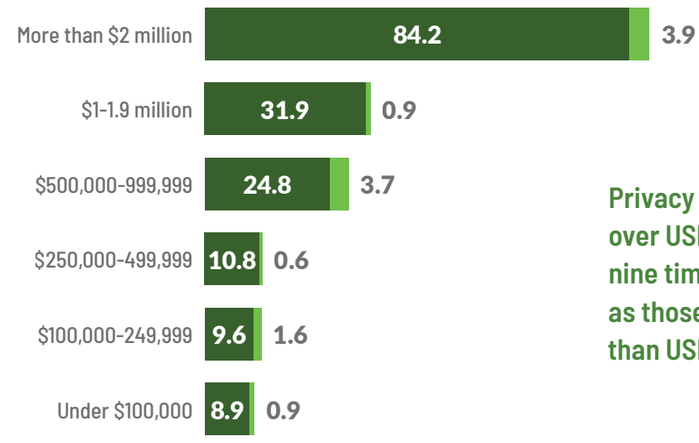


All categories in U.S. dollars.

Technology and telecommunications organizations, followed by life sciences and health care organizations have the largest privacy teams on average



Average team size tends to increase with a growing privacy budget



All categories in U.S. dollars.

Privacy teams with budgets over USD2 million are almost nine times larger on average as those with budgets less than USD100,000.

Having privacy leaders at the top drives confidence.

Clear and effective communication with those in executive positions allows the decision-making process to become more streamlined, optimizes the flow of information, and facilitates timely and informed executive actions. This year's report again looked at the reporting line of the most senior privacy pros in their organizations.

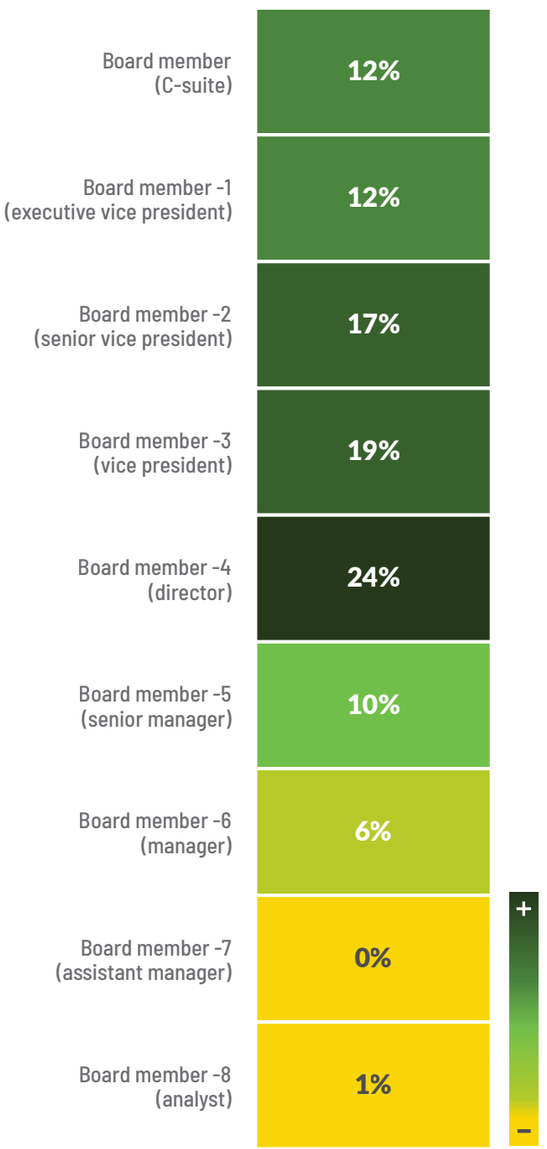
Nearly one in four privacy pros are part of organizations in which the most senior privacy or data protection employee is a C-suite executive or an executive vice president. Of respondents, 84% work at companies in which the most senior privacy or data protection employee is a director or above, a slight increase from 77% in 2023. However, when the most senior privacy employee is four rungs below the board, such as a director, respondents were more likely to report they were not at all confident in their organizations' compliance with privacy laws compared to professionals at organizations with privacy employees in the C-suite or as an executive vice president.

When the most senior privacy employee is not located in the C-suite, organizations take mixed approaches to who is accountable for privacy. More than a third of respondents reported their most senior privacy employee reports to the general counsel or head of legal. This is followed by one in 10 respondents who said their organizations' head privacy employee reports to the chief compliance officer. The remaining third said their organizations' most senior privacy employee reports to one of several roles: chief operating officer, chief information officer or chief risk officer.

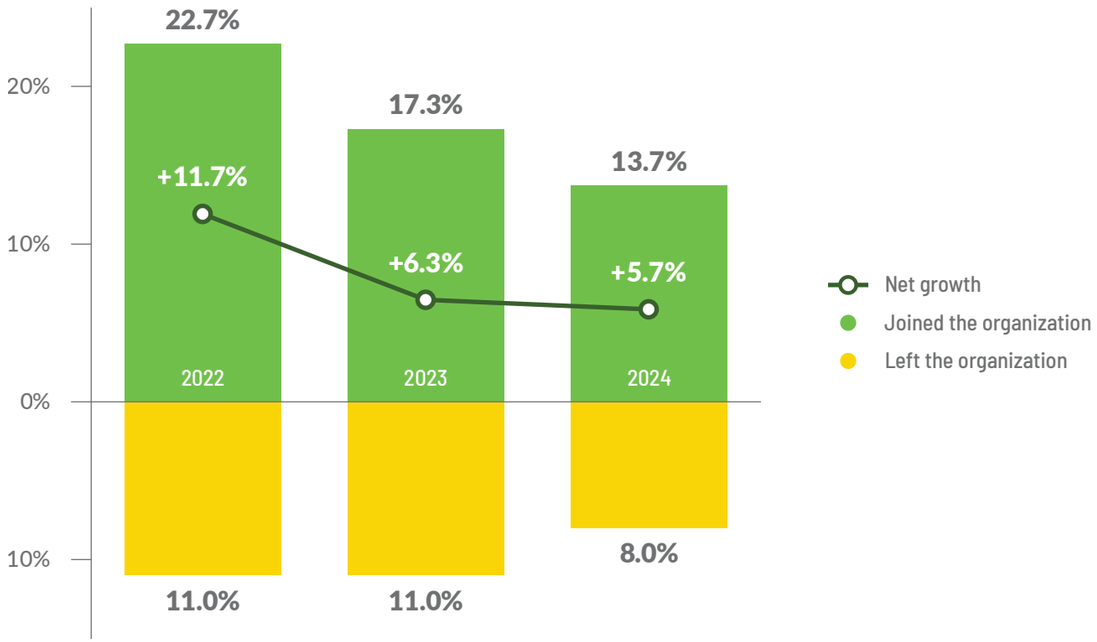
Approximately one in two respondents in the technology and telecommunications, business services, legal, or consumer goods, services and retail industries work at organizations where the most senior privacy employee reported to the chief legal officer or head of legal. Survey results show reporting lines are also impacted by company size. Head privacy employees at companies with 1,000 employees or more are most likely to report to general counsel or head of legal, compared to companies with 100 employees or less. At those companies with 100 employees or less, a third of respondents said the head privacy employees reports directly to the CEO. This trend tracks not only for the number of employees but for gross annual revenue as well.

Of respondents who reported they could deliver their objectives despite a lack of or limited availability of the right skills or resources, 58% have an accountable privacy executive, such as a board member, on their team. Of respondents who identified their companies' budgets were at least sufficient to deliver on their privacy compliance obligations, around 60% had an accountable privacy executive on their team. This highlights the importance of having a senior or executive privacy leader, as they may be able to advocate for and secure additional resources via recruitment.

Position of most senior privacy or data professional in organization



While privacy teams have grown on average, the rate of growth appears to have slowed down overall over the past three years

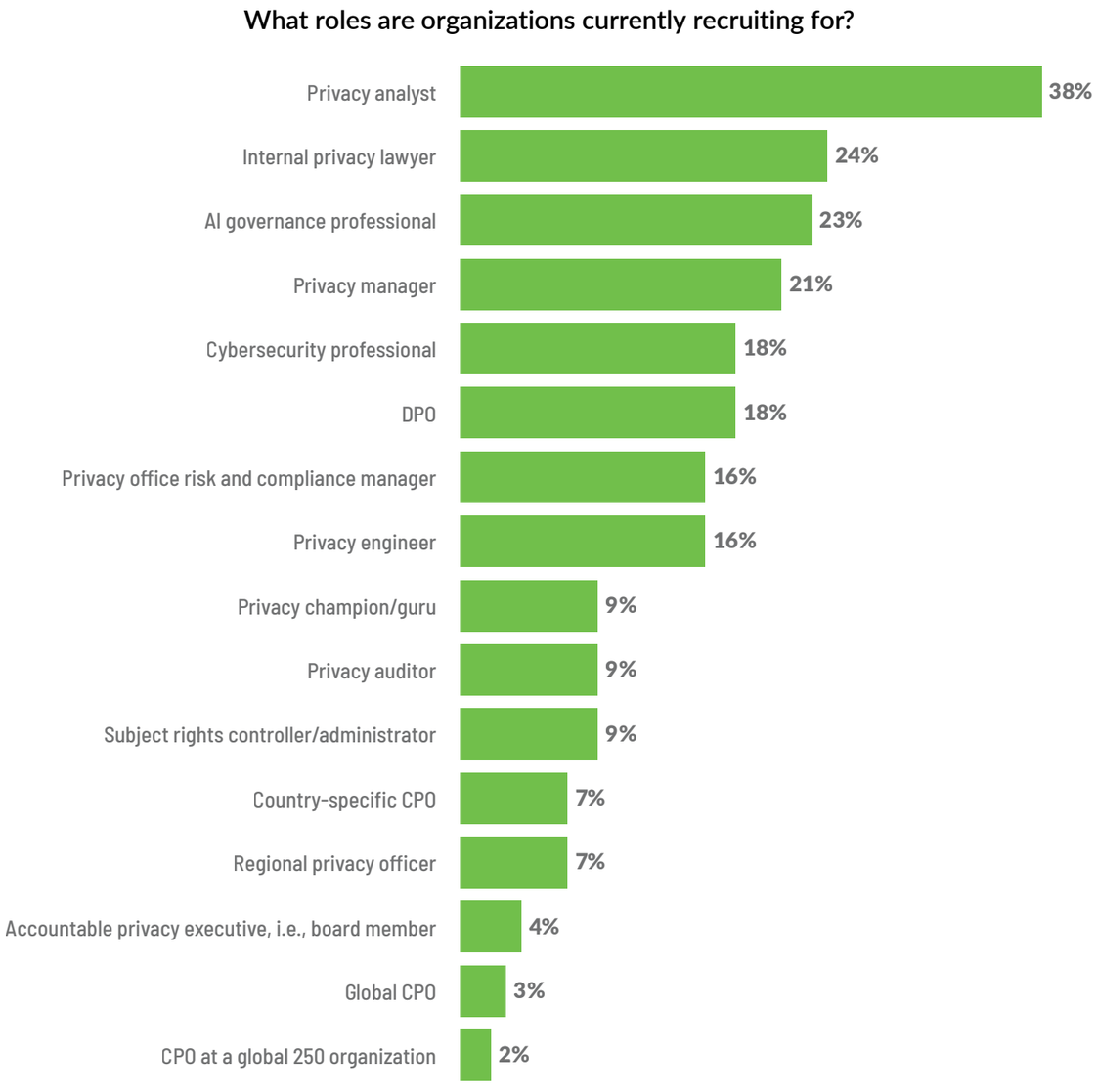


Privacy teams see less change

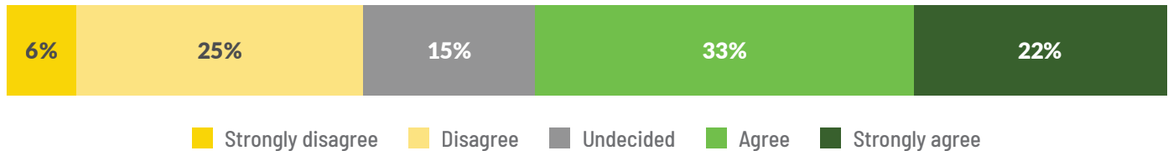
Overall, based on this survey, privacy teams have grown by 5.7% in the last twelve months. However, at approximately 57%, the majority of respondents reported their privacy teams have had a zero net change in size in the last year. Only a third reported positive growth in the number of staff. Interestingly, of those who reported zero net change for the previous 12 months, 73% reported no recruitment was currently underway and a further 67% identified no future recruitment was planned, suggesting these privacy teams are expected to stay stable other than any unplanned job changes.

The three-year trend starting in 2022 shows potential stabilization in privacy teams, with a greater proportion reporting a net zero change this year. This stabilization may be due to recruiting challenges, budget constraints or even having privacy teams that are now the right size. However, at least one in two respondents who reported a net-zero change in privacy team size at their companies also reported challenges delivering compliance, including in categories such as budget constraints. With 53% of respondents reporting a shortage of qualified privacy pros as a challenge to delivering compliance, recruitment challenges may also explain the lack of growth in some privacy teams.

Approximately 62% of overall respondents stated their organizations have no current recruitment plans. This figure drops to 36% for organizations with more than USD60 billion in annual revenue or with more than 80,000 employees, suggesting the largest organizations continue recruiting as needed. When focusing on those with open recruitment, 38% of respondents' companies are recruiting or will be recruiting for privacy analysts in the next 12 months, while 23% are looking for an AI governance professional. While fewer organizations are recruiting for higher positions such as an accountable privacy executive or CPO, they are more likely to recruit for other roles, especially DPOs and privacy managers. The organizations recruiting for CPO roles were also more likely to be headquartered in Europe than not.



To what extent did respondents agree with the following statement: "The lack/limited availability of the right privacy skills/resources limits my ability to deliver on my objectives."



The absence of the right resources currently within the privacy team or an inability to recruit resources with the right skill set can severely impact an organizations' ability to deliver on its compliance obligations. Approximately two-thirds of respondents reported a lack of or limited availability of the right privacy skills or resources on their teams limited their ability to deliver on objectives. Additionally, respondents who reported their organizations have the right resources were substantially more confident in their organizations' ability to stay informed about new policy laws and initiatives.

Confidence in compliance obligations correlated with several other team implementations. For instance, privacy pros at organizations with a structured incident-response process were more confident in their organizations' compliance than those at organizations that deal with breaches on an ad hoc basis. Those who work at organizations where the right privacy skills and resources exist to allow them to deliver on their objectives are more likely to report greater confidence in the organizations' legal compliance.

Activities of the privacy function

The privacy role is progressing to encompass varying functions, with greater focus on AI governance. Privacy teams must prioritize limited time, budget and resources on the right strategic privacy compliance priorities.

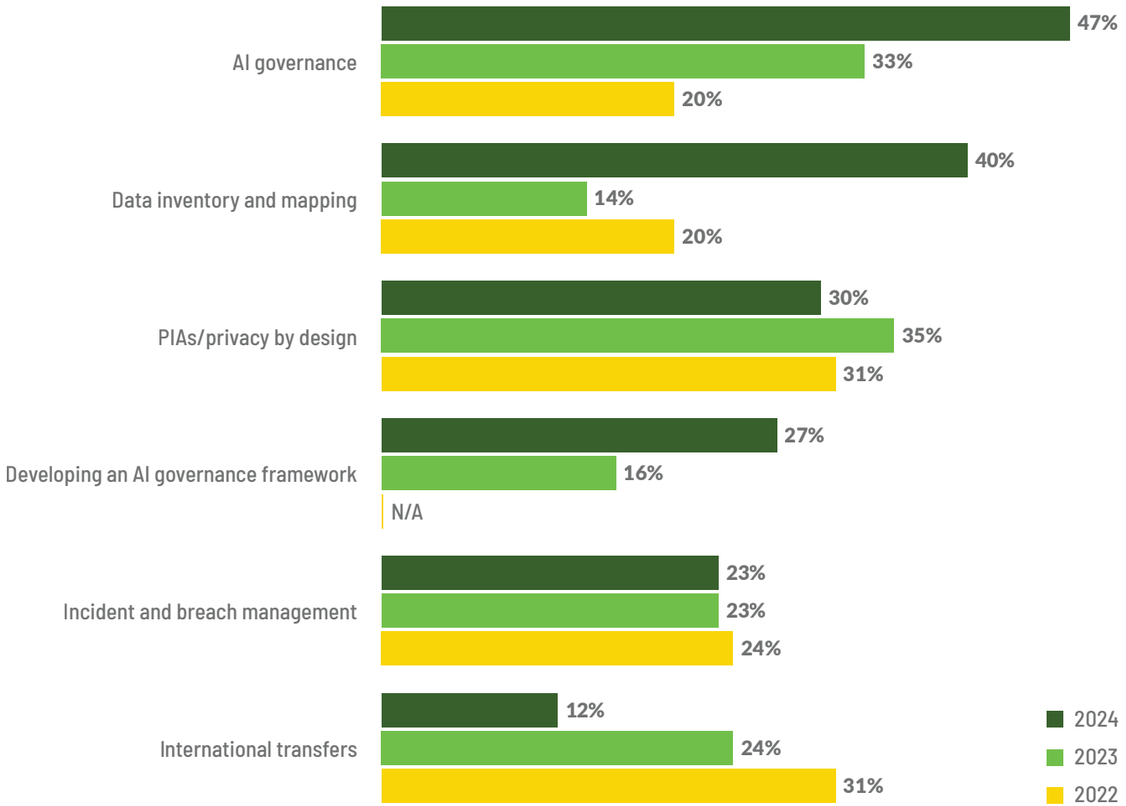
As the privacy domain has continued to evolve in the last few years, privacy pros have been compelled to adapt with the changes and chart a governance path that allows them to keep up with the growing obligations of the profession. Survey responses demonstrate organizations are focusing on both emerging technologies and established privacy practices.

AI governance has seen a sustained sharp annual increase as a top priority for organizations over the past three years.

Viewing the evolution of organizations' top strategic priorities since 2022 by sector, AI governance has seen a sustained sharp annual increase as a top priority for organizations over the past three years, predictably in response to the growing development and implementation of AI technology. Meanwhile, the establishment of dedicated AI governance teams has decreased significantly, suggesting organizations are tasking existing teams with the work of AI governance.

International transfers have seen a steady decrease over three years, while data inventory and mapping have more than doubled since 2023.

Three-year trend of selected strategic priorities chosen within top five



Viewing responses by sector, most industries saw an increase in AI governance as a top strategic priority, except for organizations in the life sciences, education and nonprofit sectors. The consumer goods sector saw the most significant increase of AI governance as a top strategic priority, with a 34% rise from 2023, followed by manufacturing with a 29% rise, and banking and insurance with a 25% rise. This advancement is likely explained by the skyrocketing implementation of AI in each of these industries, with machine learning facilitating product marketing, automated banking, supply chain management and various other routine functions. In turn, the need for AI governance has grown exponentially.

Data inventory and mapping also saw a steady increase as a top strategic priority across all industries, possibly due to a growing need for professionals to understand their data landscape to train or implement AI within their organizations.

Incident and breach management has remained relatively consistent as a strategic priority since 2022, an unsurprising trend as data breaches and cyber incidents are constant concerns for organizations in all sectors and likely make up the foundational backbone of privacy team responsibilities. Privacy by design and privacy risk controls have also seen relatively little change since 2022 across all sectors. However, privacy by design and PIAs sharply declined as a priority in two industries, dropping from 11% in 2023 to 0% in 2024 in the legal sector and from 24% in 2023 to 6% in 2024 in the business services sector. Interestingly, the development of AI governance frameworks increased steadily in all sectors over the past three years, except for in the legal and manufacturing industries. Legal and manufacturing saw respective 18% and 4% decreases in priority since 2023.

When viewed by continent, responses indicate the top-five strategic priorities have trended differently around the world. Unsurprisingly, AI governance has sustained a sharp increase as a top priority in all regions. It jumped to the top in North America, reported by 46% of respondents in the region, as well as in Europe, where it was reported by 50%, and Asia, where it was reported by 55%. Data inventory and mapping also saw a significant increase in priority from 2023 to 2024 in Asia and Oceania, rising from 9% to 21% and 3% to 48%, respectively. Again, this spike is likely explained by the need for organizations to understand is the location of their data in response to the explosion of data needed by AI models, as well as the rise in the number of comprehensive privacy legislations in the regions.

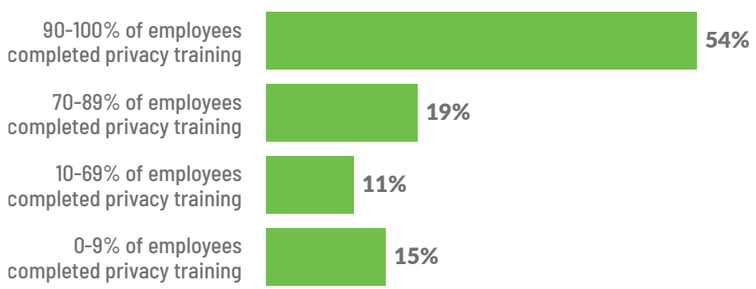
Training

Although more than half of respondents reported 90% of employees in their organizations had completed privacy training, one in five identified less than 50% of employees had completed any privacy training.

The importance of privacy training is clear: Train staff to understand their obligations and they will be better empowered to make privacy-compliant decisions when processing personal data. Those who need it may then be given more role-specific training designed to support them when they collect and process higher volumes and/or riskier personal data.

This year we sought to understand the extent to which privacy functions and employees are completing some form of privacy training.

Privacy training completion rates in respondent organizations in 2023



When examining training data regionally, respondents working at organizations headquartered in North America were more likely to have 90% or greater training completion rates compared to other regions, at 58%. This drops to 36% of organizations with 90% of employees or more completing training in Europe.

This variation in training completion rates might be somewhat surprising as privacy training can form a core part of educating the workforce, while training completion rates can form a demonstrable metric to show privacy knowledge within an organization. Budgetary challenges are one reason privacy training may not be available to all. Most respondents said their organizations spend, on average, between 0% and 10% of their total privacy budget on training. They said their organization spends an average of 5% of the budget on internal training and an additional 5% on professional development, including external training courses and certifications. These allocations remained consistent across different rates of training completion, suggesting those working at organizations with higher training completion rates had not achieved this solely by proportionally allocating more budget to privacy training.

Privacy pros working at organizations with low privacy training completion rates may have a different compliance environment from those working in organizations with higher privacy training completion rates. For example, one in two respondents working at organizations with training rates higher than 70% had regularly performed PIA processes with triggers established in the organization. In contrast, one in two respondents identified PIAs are performed on an ad hoc basis or not at all in organizations with privacy training completion rates between 0% and 9%.

Ultimately, training remains a valuable method to assess whether employees have basic privacy knowledge commensurate with their roles and responsibilities in relation to personal data. Better yet, the ability to track training completion rates, follow up with those that have yet to complete training and monitor training against identified privacy compliance risks is likely a key part of how organizations address employee privacy risk.

Risk

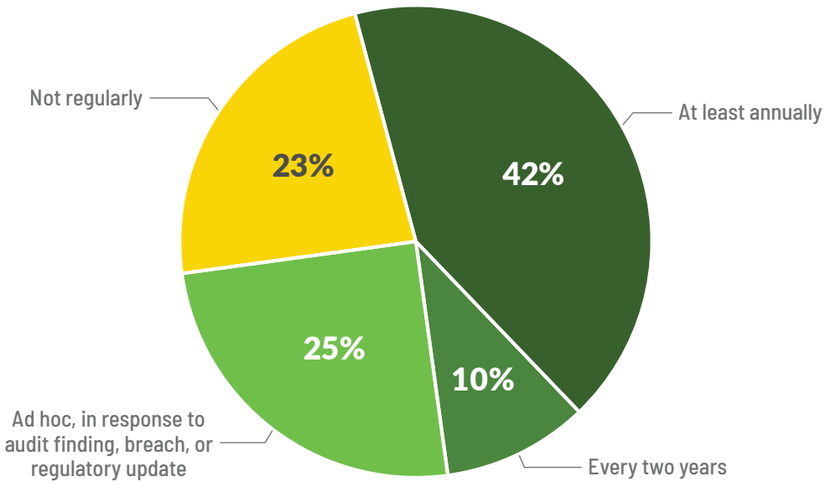
Organizations are subject to different regulations. They process differing sets of personal data for various purposes, so they experience risk differently and, as a result, have varying risk tolerance and mitigation strategies. Organizations conduct risk assessments by analyzing and examining potential risk factors or events that could have adverse impacts and then comparing those with defined tolerance levels.

By implementing effective organizational privacy risk management, companies can take steps toward managing adverse legal and regulatory consequences, protecting business reputations, and maintaining individuals' privacy. Organizations that balance individual privacy rights against the need to use that personal data may further demonstrate trust in their ability to safeguard personal data and advocate for its ethical use.

Regular enterprise-wide or business-unit-wide privacy compliance risk assessments can support an organization's ability to identify, assess and manage privacy risks in a top-down manner. For the second year running, four in 10 respondents reported their organizations undertake enterprise-wide privacy compliance risk assessments once, twice or four times per year. Most respondents indicated their organizations do not undertake regularly scheduled enterprise-wide privacy compliance risk assessments. This year, 23% of respondents said their organizations do not undertake regular enterprise risk assessments, while 25% identified they are triggered in response to key events such as audit findings, data breaches or changes in regulatory requirements. That average increased to over one in two respondents in the banking and insurance sector and the business services sector. However, the education, nonprofit, and life sciences and health care sectors only saw one in four organizations complete risk assessments at least annually.

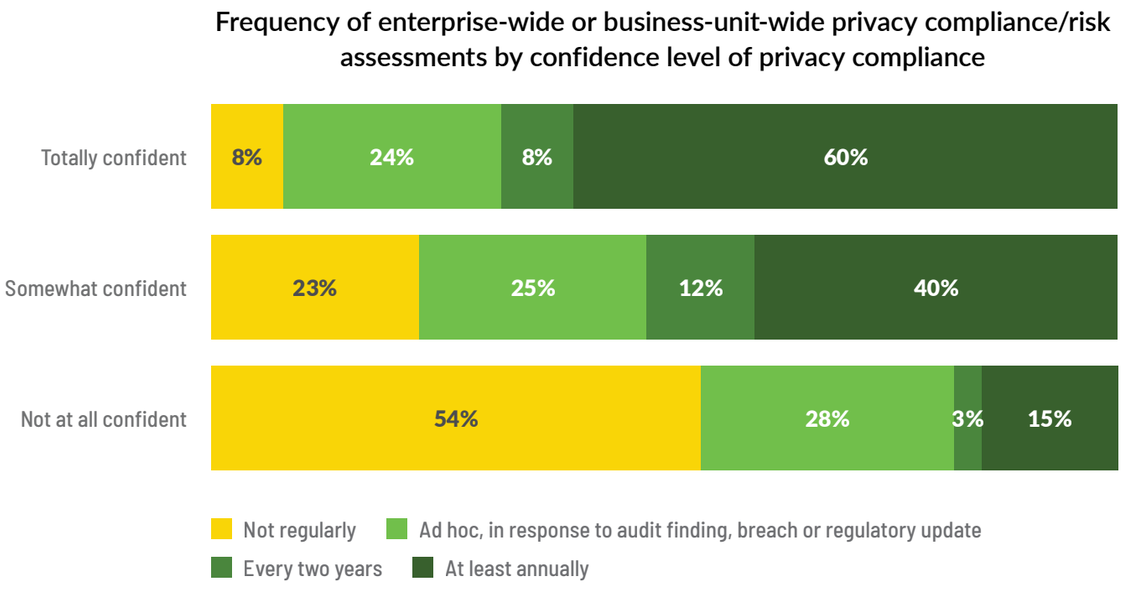
Established and mature privacy risk management may lead to compliance confidence.

Frequency that organizations conduct enterprise-wide or business-unit-wide privacy compliance/risk assessments



Frequency of enterprise-wide or business-unit-wide privacy compliance/risk assessments by 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
Not regularly	18%	21%	35%	24%	12%	26%	31%	19%	42%	18%
Every two years	11%	9%	10%	6%	12%	14%	14%	14%	4%	7%
Less than annually	29%	30%	45%	30%	24%	40%	45%	33%	46%	25%
Annually	40%	33%	18%	39%	37%	20%	30%	38%	21%	38%
Twice a year	5%	4%	3%	6%	2%	2%	1%	5%	4%	5%
Quarterly	8%	9%	5%	6%	5%	2%	3%	0%	8%	2%
At least annually	53%	46%	25%	52%	44%	24%	34%	43%	33%	45%
Ad hoc, in response to audit finding, breach or regulatory update	17%	25%	30%	18%	32%	36%	20%	24%	21%	30%



As an organization's size increases, by either revenue or number of employees, the tendency for more frequent top-down enterprise-wide assessments of privacy compliance also increases. Six in 10 respondents working in organizations with more than USD60 billion in annual revenue identified their organizations conduct these assessments at least annually. In comparison, only a third of those working in organizations with USD100 million or less in annual revenue identified the same.

Similar to 2023, this year we sought to understand the trend when considering confidence in compliance. Respondents who said they are totally confident in their organizations' privacy compliance capabilities were 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 in their organizations' level of privacy compliance.

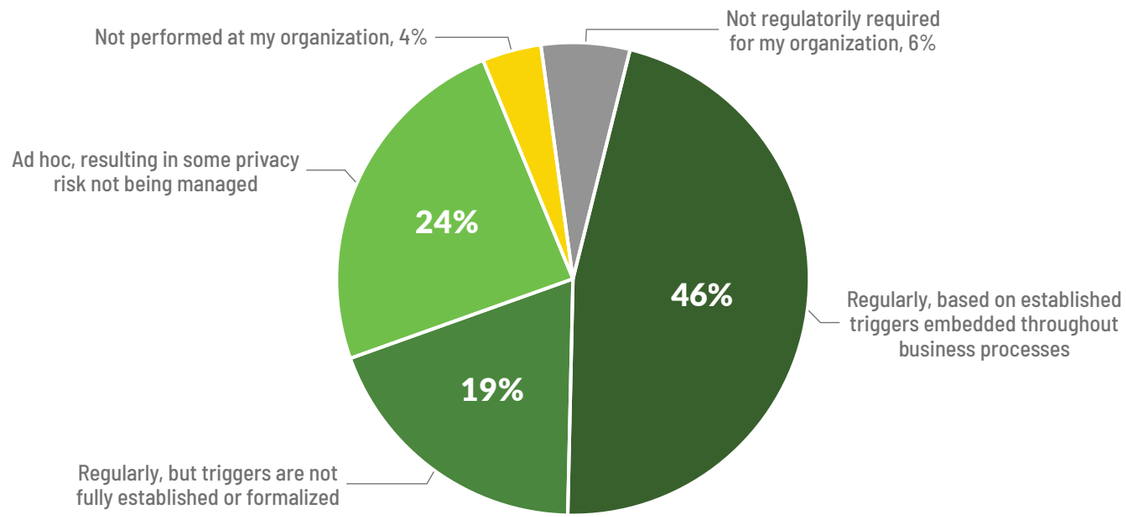
Factors that influence this could include the absence or ineffective implementation of privacy by design within the organization, thus requiring greater resources to conduct project-specific risk management. Another reason is that the cost of enterprise privacy compliance risk assessments may be prohibitive to conducting them on a regular basis. Those who identified their companies' budgets as 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 companies' budgets as less than sufficient were more likely to work for organizations that undertake enterprise privacy risk assessments on a less than annual basis.

PIAs

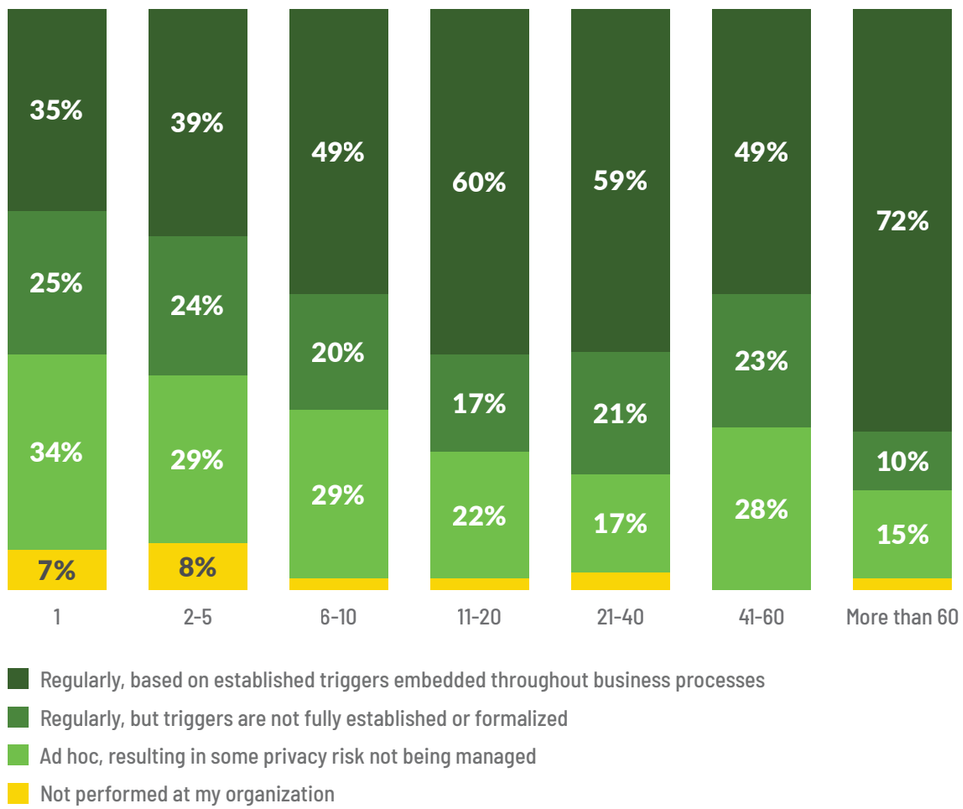
PIAs, whether regulatorily required or not, are often an important tool and process for an organization's privacy risk management. In 2024, the number of organizations that perform PIAs or DPIAs regularly, based on established triggers embedded throughout the business processes, was similar to the number in 2023. Like in 2023, almost one in five organizations still do not have fully established triggers. On average, two out of three respondents identified their organizations complete PIAs regularly. One in four said their organizations complete them ad hoc, likely resulting in some privacy risk not being managed.

Industry also impacted when and how organizations perform PIAs. For example, of the respondents whose organizations are required to perform the assessments by regulation, 3% in the consumer goods, services and retail sector still do not perform PIAs or DPIAs. In contrast, 63% in that industry have established triggers for PIAs embedded throughout business processes — the highest percentage across industries. The education and nonprofit sector was the least likely to perform PIAs regularly, with 47% of respondents in those industries reporting their companies perform ad hoc assessments or do not perform them at all.

Frequency of PIAs or DPIAs performed by an organization



Frequency of PIAs or DPIAs by number of countries in which the organization has officers or business operations



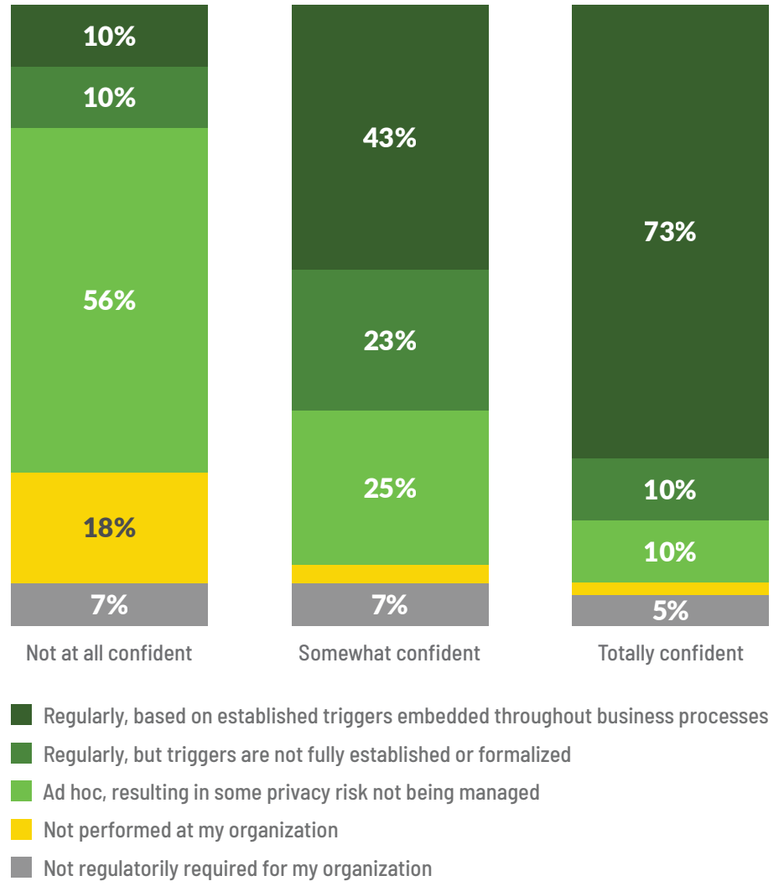
Notably, respondents from larger organizations that conduct PIAs are more likely to have established PIA processes, potentially due to the organization's complexity or because their teams have the resources to perform these activities regularly. The likelihood that an organization did not conduct a regulatory required assessment decreased as an organization's number of employees increased. Although one in four organizations with fewer than 100 employees performed PIAs or DPIAs regularly based on established triggers, that percentage increased as employee numbers increased. The largest organizations were more likely to undertake PIAs regularly and were more likely to have taken steps to establish a formal PIA process.

Organizations operating in multiple jurisdictions are more likely to have established mechanisms that trigger regular impact assessments embedded throughout their business processes.

Privacy pros may feel more confident in compliance if their organizations have taken steps to embed the PIA process within the organization, establish privacy by design and take a risk-based approach to performing PIAs.

Nearly eight in 10 respondents who were not at all confident in their organizations' compliance reported their organizations either do or do not regularly perform PIAs or DPIAs. However, 77% of respondents who were totally confident in compliance said their organizations perform them regularly based on established triggers. An additional one in 10 respondents who noted being confident in their companies' compliance also said their organizations perform them regularly but without established triggers. This suggests privacy pros may feel more confident in compliance if their organizations have taken steps to embed the PIA process within the organization, establish privacy by design and take a risk-based approach to performing PIAs. Around 60% of respondents who said they were not at all confident in their organizations' compliance with privacy requirements work in organizations where the PIA process is ad hoc, whereas this drops to 10% for those who said they were totally confident.

Frequency of PIAs by confidence in an organization's compliance with privacy regulations



There are two main methodologies for risk assessments: qualitative and quantitative.

Qualitative

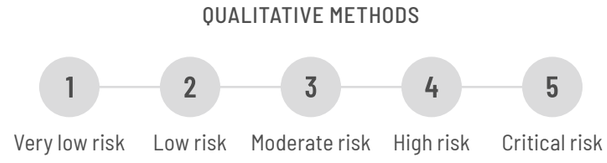
- → Qualitative risk assessments use subjective judgment to identify and prioritize risks based on their potential impact and likelihood.
- → Qualitative assessments offer insight into potential risks.

Quantitative

- → Quantitative risk assessments employ numerical data and statistical models to measure and analyze risk, which provides a more objective forecast compared with the qualitative approach.
- → Quantitative assessments deliver measurable and comparable risk metrics.

Quantitative vs. qualitative privacy risk management

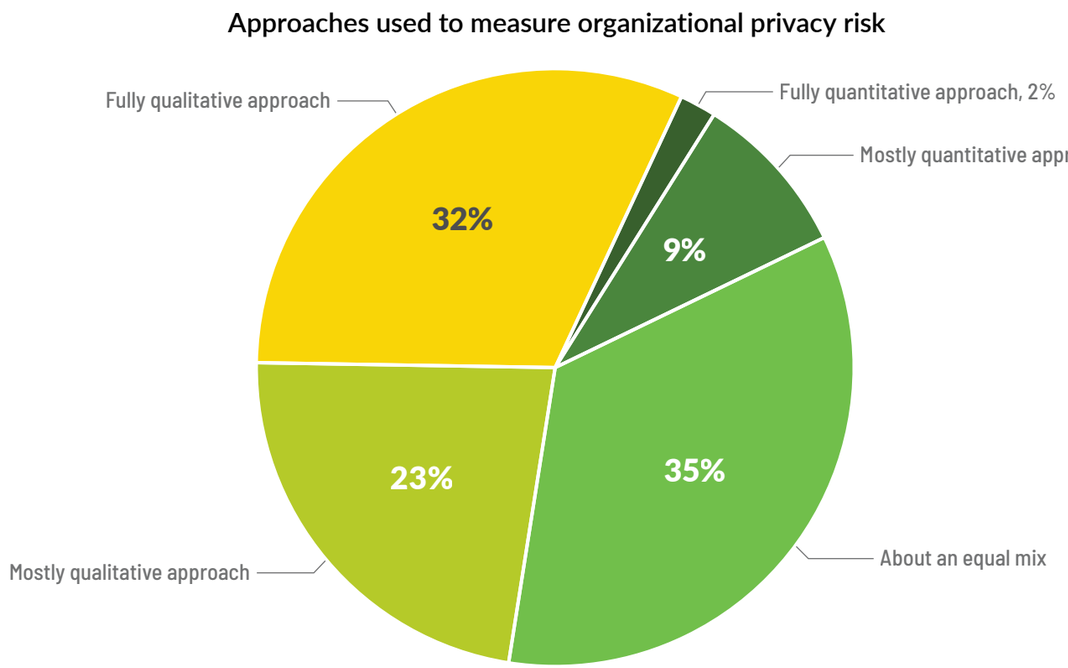
At the organization level, we asked respondents how privacy risk was measured, seeking to establish if organizations utilize qualitative methods, relative ratings or quantitative methods to forecast and model organizational risk.

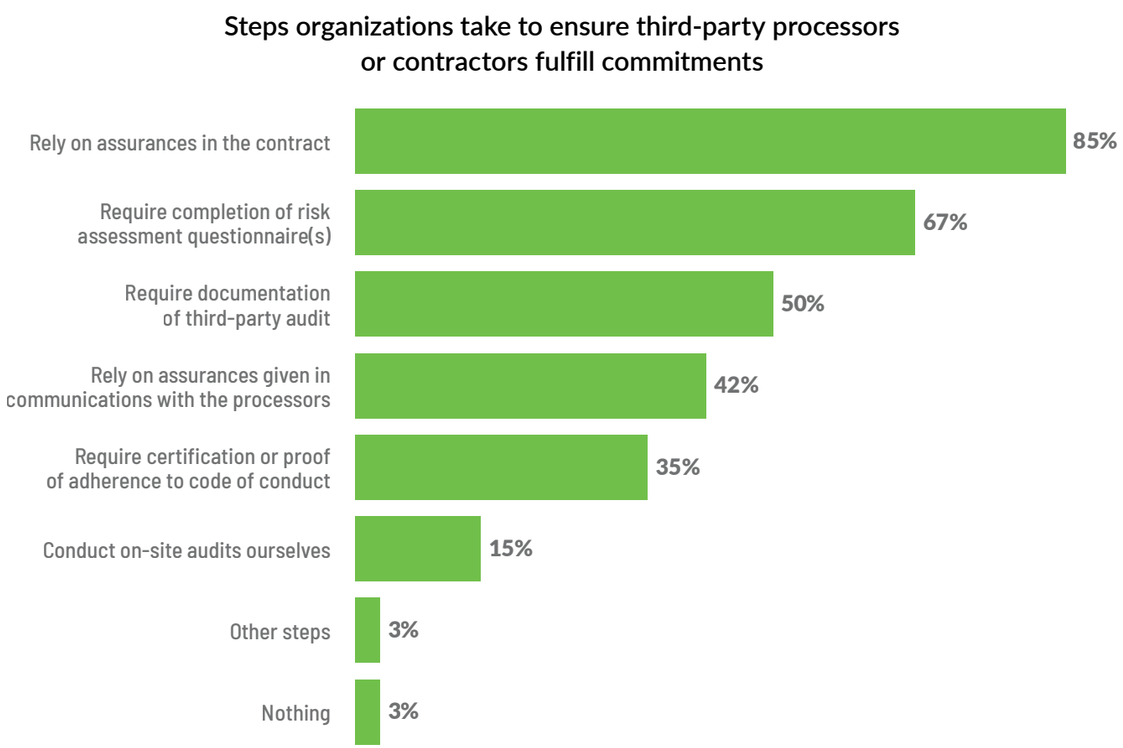


When considering organization size, the largest companies by number of employees or by privacy budget are most likely to have approaches that are at least 50% quantitative. Almost six in 10 respondents who work at organizations with more than 80,000 employees or with privacy budgets greater than USD2 million identified the approach to privacy risk management is at least as quantitative as qualitative. As privacy risk management matures, it will be interesting to see how this balance shifts and if organizations will use more quantitative methods to measure privacy risk.

The survey also asked respondents to what extent individual harms are considered by their organizations' management approach to privacy risk assessment. Nine in 10 articulated that individual harms are included or considered. When individual harms are not considered in an organization's management approach to privacy risk assessments, privacy pros were less confident in compliance compared to their peers. However, how organizations define individual harm undoubtedly varies by company, sector and even department.

Nine in 10 use a qualitative approach at least as much as a quantitative approach to privacy risk management.

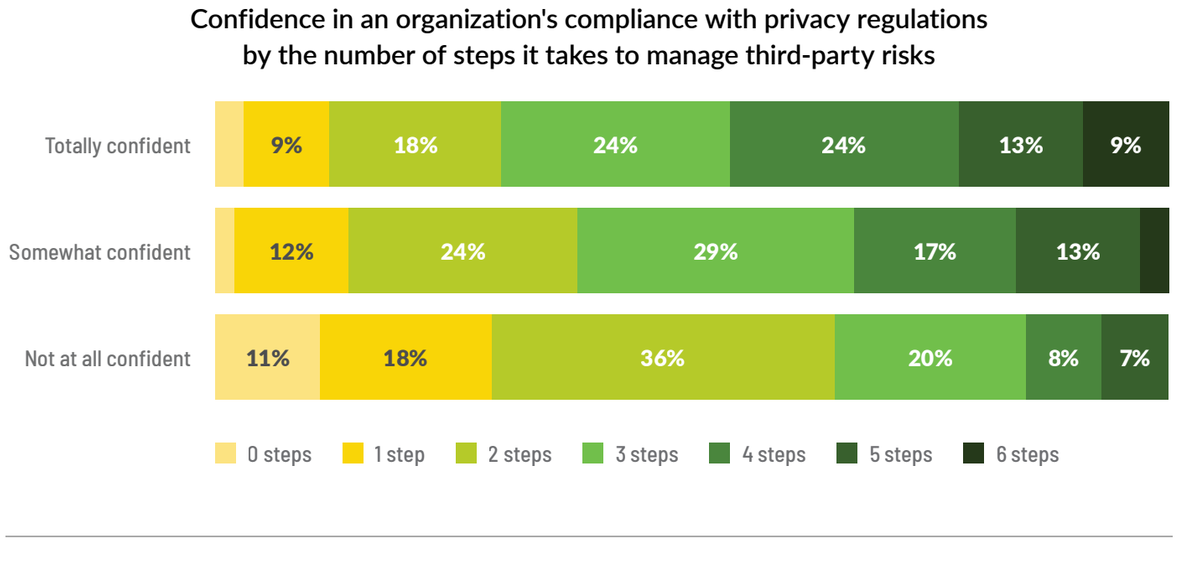




Third parties and contractors

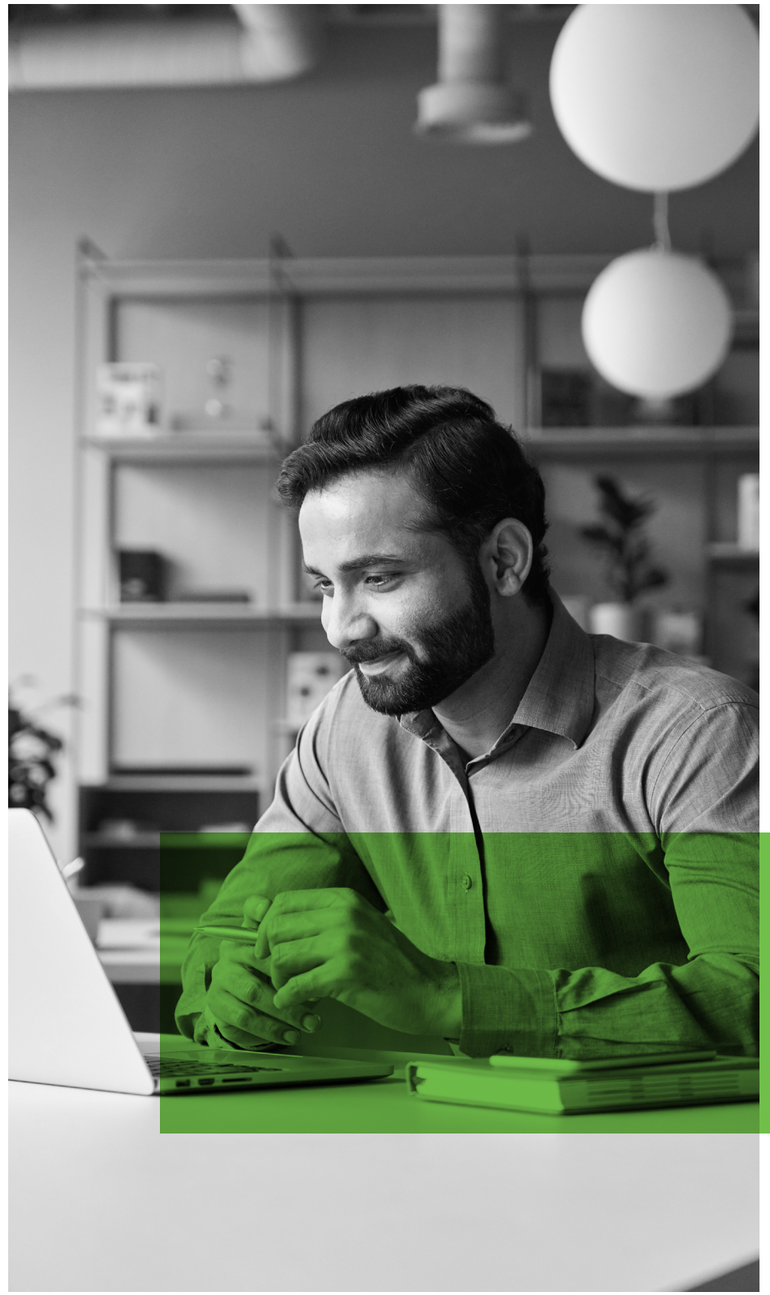
Regarding third-party processors and contractors, privacy pros are doing more than just relying on assurances in contracts to ensure commitments. It remains important for organizations to outsource to third parties and take advantage of specific expertise, obtain cost efficiencies and scale operations as needed to meet core business objectives. However, the absence of a third-party risk management process, particularly when sharing personal and sensitive personal data, may expose the organization to unmitigated third-party privacy risk.

The third party's privacy risk posture, therefore, should be a core part of how an organization manages its 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.



Almost six in 10 respondents selected their organizations rely on assurances in contracts and require completion of risk assessment questionnaires. Just over a third of respondents also noted their companies require documentation of third-party audits in addition to assurances and risk assessment questionnaires.

On average, organizations take three steps to manage third-party risks. Additionally, respondents at organizations that take three or more steps to manage third-party risks are more likely to be confident in the organizations' compliance with privacy laws and policies. This result suggests organizations embracing diversified, risk-based approaches to third parties are better positioned to confidently mitigate and adapt to evolving risk and compliance challenges than those relying on a single measure, which could become the single point of failure during security incidents.



Responses indicating if and how a privacy task is performed

	Not performed	Manual	Semiautomated	Fully automated
Consent management	11%	21%	42%	26%
Cookie consent/website scanning	10%	9%	31%	50%
Data mapping/inventory	12%	49%	33%	6%
Third-party risk management	5%	52%	39%	4%
Privacy/DPIAs	8%	56%	32%	4%
Data subject rights request management	8%	50%	37%	5%
Remediation tracking	24%	51%	22%	3%
Data minimization	17%	54%	25%	4%
Data retention	10%	42%	42%	7%
Data anonymization	24%	31%	34%	11%
Data pseudonymization	24%	30%	34%	11%
Data tagging	36%	23%	34%	7%
Program management (policies, benchmarking, maturity/planning)	6%	72%	20%	1%
Privacy by design	13%	61%	25%	1%
Privacy risk management	7%	62%	29%	3%
Privacy training and awareness	3%	33%	49%	14%
Privacy policies management	3%	72%	23%	3%
International data transfer assessments	28%	52%	18%	2%
Incident management	2%	56%	38%	3%
Regulation tracker	10%	62%	24%	4%

Privacy technology and tooling

The proliferation of autonomous tools and privacy-enhancing technologies is ever-increasing within companies. Organizations that intend to introduce automation must choose whether to dedicate the time and resources to developing technologies tailored to their needs or engage in services or products developed by or with third parties for their privacy functions. This year's report examines the privacy and compliance-oriented tasks respondents complete manually, through semiautomation or full automation, and it examines whether companies are developing automated technology themselves.

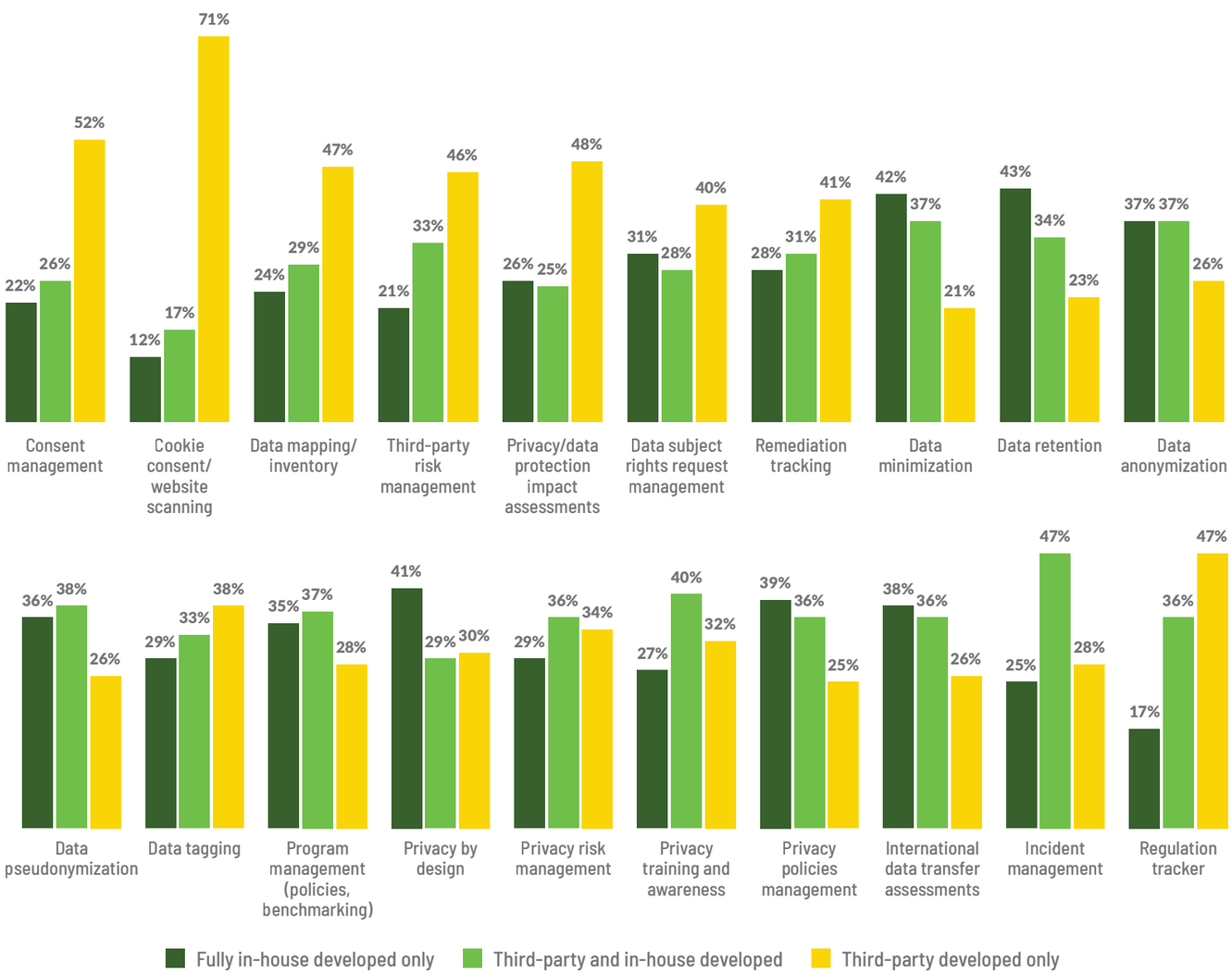
To better understand the level of assistance each organization employs, we asked respondents which of the following common privacy-related and compliance-oriented tasks their organizations completed manually, through semiautomation or full automation.

The emerging utilization of technology to support privacy compliance can boost confidence in compliance.

Privacy tasks differ from entity to entity and are influenced by location and industry, among other factors. For example, in the government sector, organizations are more likely to perform PIAs and DPIAs manually and are less likely to automate program management. The information technology sector is more likely to fully automate data tagging and program management. On the other hand, the finance and banking sector is more likely to manually perform consent management, cookie/consent and website scanning and is also more likely to perform incident management by semiautomation.

Organizations headquartered in the EU are more likely to manage third-party risk manually, while companies in North America are more likely to complete this via semiautomation. Those at companies with fully automated consent management, cookie consent/website scanning, data mapping/inventory and PIA/DPIAs were also more likely to be confident in compliance with the EU AI Act.

Origin of automation technologies at organizations



In-house compared to third-party automation

The development of PETs or any automation requires sufficient thought and resources. Organizations that intend to introduce automation to their tasks must choose whether to dedicate the time and resources to developing technologies tailored to their needs or select services or products developed by or with third parties for their privacy functions.

Organizations at which the privacy team reports to the general counsel or head of legal and uses automation for consent management, cookie consent and website scanning, or data mapping and inventory were more likely to use technologies developed by third parties.

Automation and confidence

On average, 9% of respondents reported they were not confident in their organizations' ability to comply with privacy regulations and policies. The percentage of respondents who were not confident increased when a selected privacy process was not performed or was done manually. For example, over three out of 10 respondents at companies that did not perform data mapping or inventory, third-party risk management, data retention, data tagging, privacy by design, or privacy training and awareness reported they were not at all confident in compliance.

Looking ahead

Many privacy pros are gaining additional responsibilities in AI governance and digital governance.

A prominent result from this year's survey was the acquisition of new responsibilities in AI governance and digital governance. The privacy function rarely sees stagnation due to the vibrancy, diversity and complexity of the field. Although privacy pros are reporting new responsibilities and facing complex challenges, confidence levels in privacy compliance remain relatively stable.

Like last year, the IAPP AI Governance Center will publish a report outlining the results of questions specific to AI and AI governance from this year's survey. The survey reflected what many privacy pros are experiencing: The privacy function is more likely to gain additional responsibility for AI governance when the organization is working on AI. Although the majority of organizations are currently working on AI governance, this number jumps significantly when organizations are using AI for process automation, at 88%, automated decision-making, at 89%, data analysis, at 88%, personalizing experiences, at 89%, or customer interactions, at 90%.

Respondents working in AI governance face significant challenges. For example, one in two respondents reported a lack of understanding of AI, underlying technologies and/or AI compliance obligations within their organizations impacts their ability to deliver for their organizations. One in three respondents stated there are not enough AI resources relative to the activities required to be completed, organizational AI expectations are not clearly defined or followed up on, there are budget constraints, and there is a lack of AI governance representation in senior levels of the organization. Stay tuned for a full report on these challenges and other AI governance industry insights.

Our research approach

We focus on bringing our membership accurate, meaningful and actionable research.

The IAPP Research and Insights team focuses on bringing our membership accurate, meaningful and actionable 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 78-question governance survey. Over the course of eight weeks, from April to May 2024, more than 670 individuals from 45 countries and territories responded.

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

More than 670 individuals from 45 countries and territories responded to this 78-question governance survey.

Contacts

Connect with the team

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

Cheryl Saniuk-Heinig
Research and Insights Analyst, IAPP
csaniuk-heinig@iapp.org

Luke Fischer
Former Westin Fellow, IAPP

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

Follow the IAPP on social media

Published November 2024.