The Privacy Pulse

2026 Global Privacy Benchmarks Report

TrustArc

GOLFDALE CONSULTING

Table of Contents

Top 5 Insights from 2026

The TrustArc Global Privacy Benchmarks is an annual study examining how organizations operationalize privacy governance in an increasingly complex data environment. Based on responses from privacy leaders and business professionals worldwide, the research evaluates privacy maturity, governance practices, technology adoption, and emerging challenges, such as artificial intelligence. The findings include how respondents score on the TrustArc Global Privacy Index,[1] a proprietary composite metric measuring organizational privacy performance.

Overall, these findings provide a global view into how privacy programs are evolving and which organizational practices most strongly correlate with stronger privacy competence. Several clear patterns emerge from this year's results. The five insights below summarize the most important findings from the 2026 Global Privacy Benchmarks.

1 Overall privacy capability declines, and the gap between high performers and mid-tier programs widens.

The Global Privacy Index fell to 53% in 2026 from 61% in 2025. While results held steady at the high end of competence, with one third continuing to achieve exceptional grades (>75%), a noticeable share of organizations shifted from mid-tier scores into the failing range, pulling the overall index downward. This erosion among mid-performing organizations suggests many are struggling to keep pace with rising regulatory, technological, and governance demands, even as privacy remains a headline enterprise priority.

2 Organizations with interoperable technology and key privacy initiatives lead by 4x.

As organizations operationalize initiatives such as data inventory, consent management, Data Subject Request (DSR) management, and Trust Centers, the Global Privacy Index rises from 18% to 85%, from those not fully implemented to those implementing all eleven initiatives measured in the study. With the global average at 53%, most organizations need about five fully implemented initiatives to reach baseline maturity. Performance improves further when these initiatives are supported by integrated privacy tools that share data seamlessly across systems. The findings also show that organizations using purpose-built privacy management software are significantly more likely to operate integrated technology environments than those relying primarily on GRC software. Overall, organizations with interoperable technology and six or more initiatives average 75% on the Global Privacy Index, nearly four times the competence level of smaller, fragmented programs.

[1] *TrustArc's Global Privacy Index is a proprietary composite metric measuring organizational privacy performance across seven privacy competencies and five stakeholder outcomes. Developed through statistical modeling in 2020 and revalidated in 2021, the index aggregates survey responses into a single score ranging from –100 to +100, providing a standardized measure of overall privacy competence.*

3 Privacy ROI compounds as programs move beyond compliance into true business value.

Organizations that deliver value only at the compliance level show almost no privacy competence, but predicted Global Privacy Index scores rise to 29% when programs also improve operational efficiency, 61% when they further strengthen customer trust and sales acceleration, and 90% when value extends across all four ROI layers, including innovation and future-ready operations. Realizing these gains requires treating privacy as a strategic priority, a view that 49% strongly agree reflects their company's approach.

4 AI is now a daily workplace reality, and governance is finally catching up.

Over two-thirds of respondents (69%) report using AI tools often or very often at work, and the frequency of use strongly correlates with governance. Organizations are also beginning to experience AI-related consequences alongside traditional risks such as breaches and regulatory actions, with 24% reporting problems from AI-driven decisions in the past three years, up seven points from 2025. At the same time, preparedness is rising: 76% say they are very confident or confident in their ability to adapt privacy practices to emerging AI regulations. Among organizations that believe the laws apply to their operations, 72% say they are very or prepared for enforcement of the EU AI Act (up from 61% in 2025) and 66% for the Colorado AI Act (up from 57%).

5 Accountability frameworks and certifications act as governance north stars that accelerate privacy maturity and technology integration.

Organizations aligning their programs with governance and accountability architecture frameworks achieve average Global Privacy Index scores in the 70% to 76% range, roughly 20 points above the global average. By contrast, organizations operating without certifications and with siloed privacy systems score as low as –12%. Framework-based governance models help organizations operationalize privacy through integrated controls, coordinated initiatives, and more disciplined technology environments rather than relying solely on point-by-point regulatory compliance.

Survey Scope and Reach, at a Glance

Participants in the 2026 Global Privacy Benchmarks represent 1,844 privacy leaders, executives, and business professionals across a broad cross-section of industries, company sizes, and roles — from privacy executives and dedicated team members to senior leaders and frontline employees. Respondents span major global markets, with Europe and the United States representing the largest shares and Asia Pacific accounting for 15% of the sample. More than half represent organizations with over $1 billion in annual revenue, and more than four in ten have worked at their company for more than ten years, grounding the findings in deep institutional knowledge.

To ensure balanced representation, responses were weighted by organizational revenue and professional role, giving the results an enterprise-wide perspective rather than one skewed toward privacy specialists alone.

WHO

1,844 privacy professionals across 6 global regions

WHAT

7th annual global 360° survey measuring how organizations operationalize privacy governance

KEY TOOL

Proprietary Global Privacy Index (GPI), scored –100 to +100

Analysis and Insights

Drawing on survey results from across industries and regions, the analysis explores how privacy programs are structured, how organizations manage emerging risks such as AI and regulatory complexity, and which operational practices most strongly correlate with higher privacy competence.

We begin by examining how organizations structure their privacy teams, as dedicated leadership, staffing, and organizational placement often form the foundation of effective privacy programs.

Note that key privacy terms, including maturity levels, program metrics, and operational concepts such as DPIAs and DSRs, are used throughout this report. For clarity, concise definitions of these terms are provided in the Glossary at the end of the report.

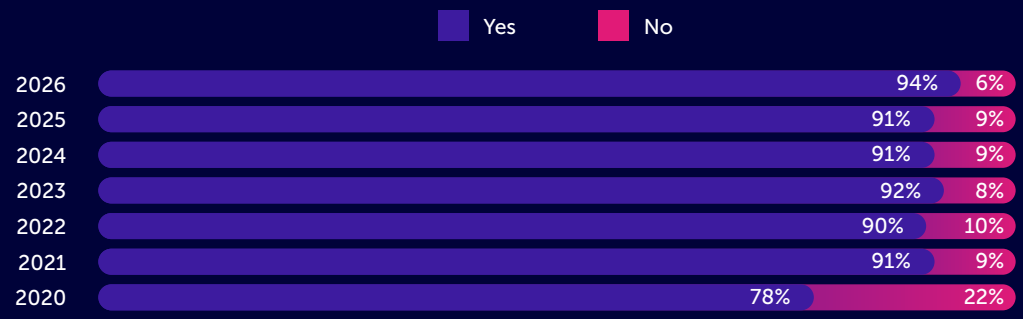
How Privacy Teams Are Built

Strong hiring, dedicated teams signal privacy's importance

Dedicated privacy teams continue to expand and stabilize as a core organizational function. In 2026, 94% of companies with more than $50M in revenue report having a dedicated Privacy Office or team responsible for overseeing privacy issues. This represents a continued increase from prior years and reinforces the growing institutionalization of privacy governance across organizations of all sizes.

Does your company have a dedicated Privacy Office?

Results shown in each year for companies USD $50M+



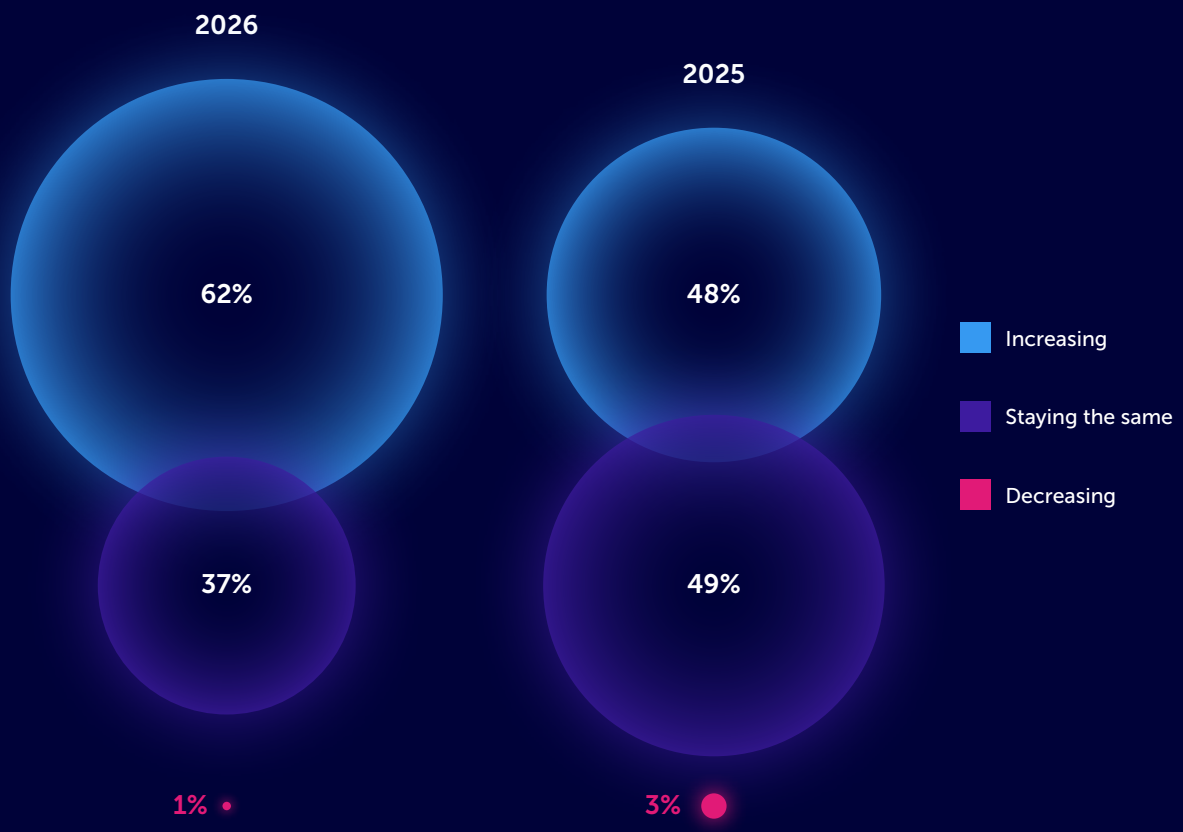
While large enterprises have long maintained formal privacy leadership structures, the adoption of dedicated privacy teams is now broadly consistent across mid-sized organizations as well. **The presence of a Privacy Office is increasingly viewed as foundational infrastructure** for managing regulatory obligations, operational risk, and customer trust in a data-driven environment.

Privacy Office by Revenue

At the same time, demand for privacy expertise remains structurally strong. Privacy hiring expectations strengthened further in 2026. Fully 62% of respondents report that demand for privacy roles is expected to increase over the next year, up significantly from 48% in 2025 and the highest level recorded in the survey. Only 1% anticipate declining demand, reinforcing that privacy expertise is becoming a durable and expanding enterprise capability.

A majority of organizations expect demand for privacy roles to increase over the next year, up substantially from 2025. This change undoubtedly reflects continued regulatory expansion, the operational complexity of global privacy compliance, and the growing importance of responsible AI governance. Privacy talent is increasingly viewed not as a compliance cost center but as a strategic capability supporting long-term digital trust and risk management.

In the next year, do you see the demand for privacy roles decreasing, staying the same, or increasing at your company?



As privacy responsibilities expand to address regulatory complexity, data governance, and emerging technologies, organizations increasingly recognize that sustained expertise and organizational support are required to manage privacy risk effectively.

With these structural foundations in place, the next question is what challenges privacy programs are responding to and what value organizations expect them to deliver.

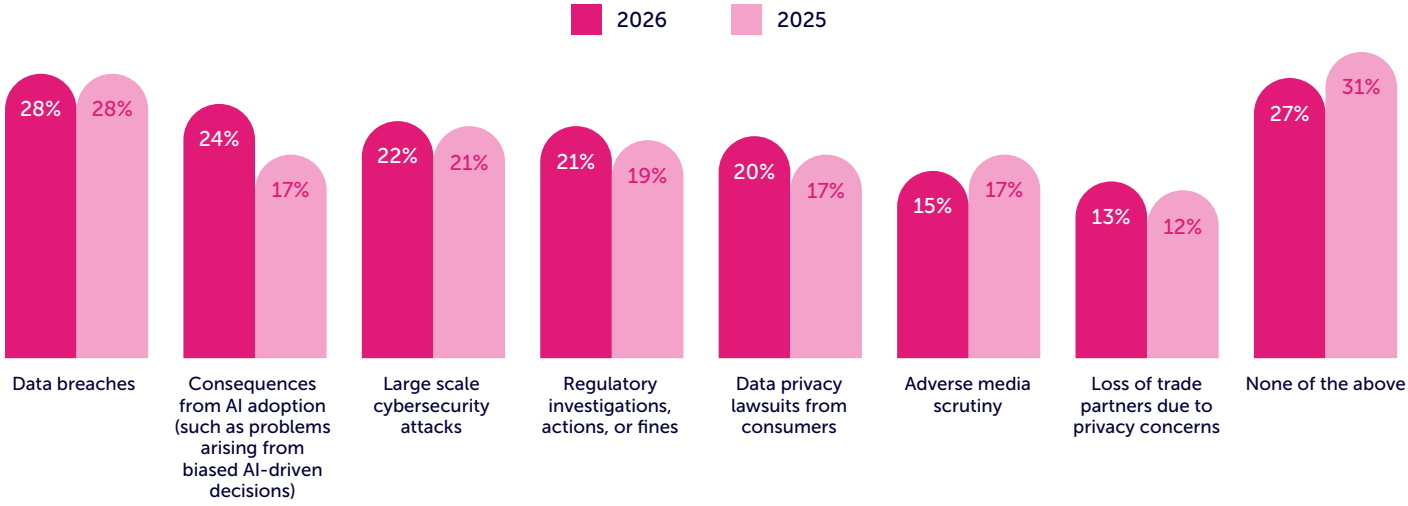
Mature programs realize ROI beyond mere risk management

Privacy programs often begin as a response to risk. Breaches, regulatory investigations, and reputational harm remain powerful drivers of investment. But privacy is no longer defined only by what it prevents. As programs mature, organizations increasingly recognize the broader value they create.

Organizations continue to face a range of privacy risks, with both traditional threats and emerging technology risks shaping the privacy landscape. Data breaches, cybersecurity incidents, regulatory investigations, and reputational exposure remain widely reported across organizations. At the same time, the survey shows a notable rise in reported consequences of AI adoption, with **24% of organizations reporting that AI-driven decisions have caused problems in the past three years**. This increase highlights how AI-related risk is beginning to emerge alongside more familiar privacy vulnerabilities.

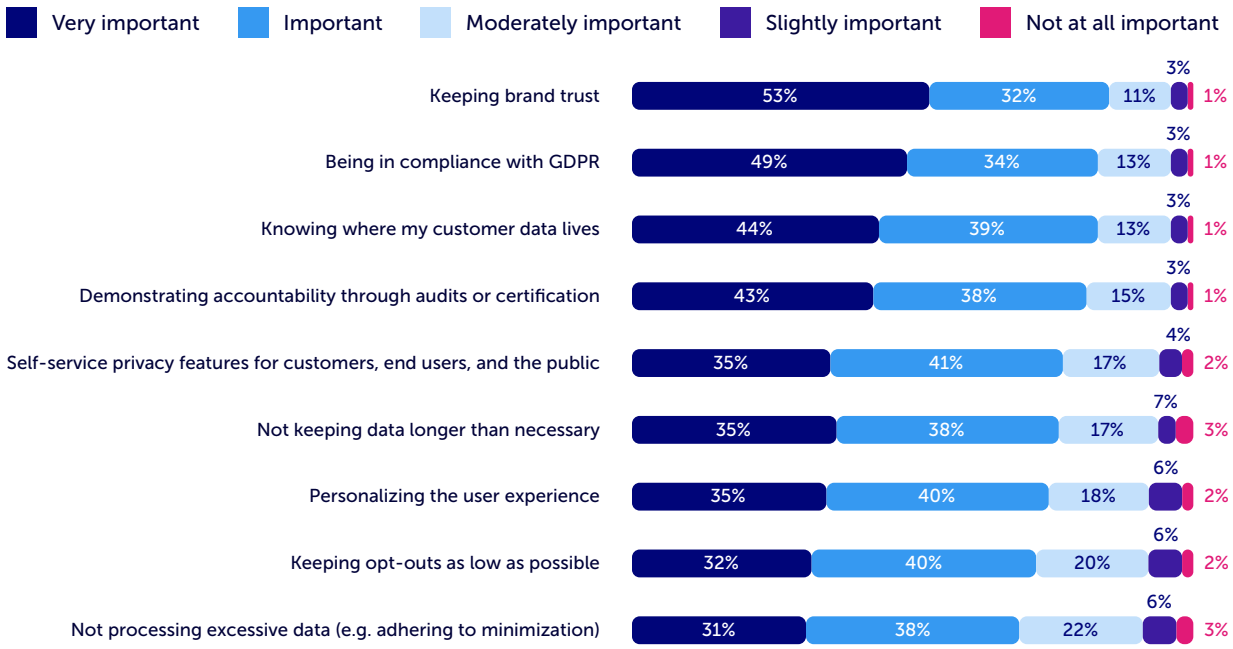
Has your company suffered from any of the following in the past 3 years?

Choose all that apply



Organizations continue to recognize substantial benefits from strong privacy programs, with maintaining brand trust as the top benefit. Operational outcomes such as accountability, user empowerment, and data minimization follow closely, suggesting that privacy programs are increasingly viewed as foundational governance mechanisms that support responsible data use rather than merely as compliance obligations.

On a scale of one to five, how important are the following with respect to your company's privacy efforts?



Organizations report continued upward movement in privacy maturity, with a larger share now concentrated in the strategic and transformative tiers. **In 2026, 61% describe their organizations as strategic or transformative, up from 35% in 2025, while the share in reactive or merely compliant stages fell sharply**, suggesting that privacy management is increasingly a business enabler and competitive capability.

How would you characterize your organization's maturity in Privacy Management?

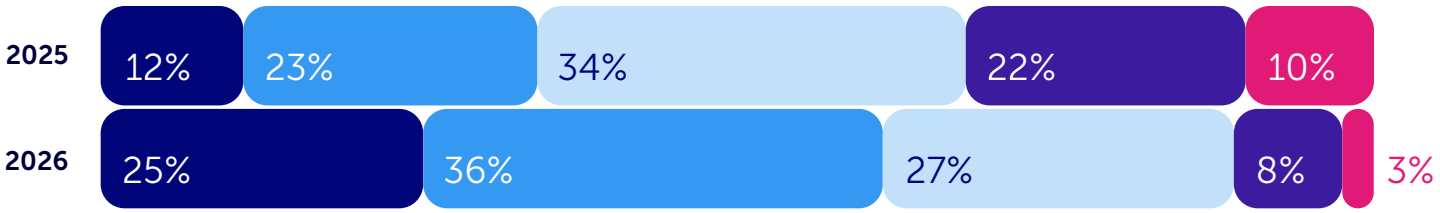
Transformative
Setting industry standards and using innovative practices

Strategic
Using risk-based approach to drive business value and competitive differentiation

Proactive
Anticipating and preventing issues through established processes

Compliant
Meeting minimum regulatory requirements

Reactive
Addressing issues only after they occur



The 2026 ROI report shows that privacy programs generate value across four distinct but connected outcomes. As a baseline, privacy reduces downside risk. However, organizations increasingly see privacy as also supporting operational efficiency, protecting and growing revenue through trust, and enabling scalable innovation, international expansion, and AI-ready operations.

Organizations report meaningful value from their privacy programs across all four ROI drivers, with the strongest concentration still on reducing regulatory exposure. **Strong or significant value is reported for compliance and risk avoidance (73%), productivity and cost savings (68%), revenue and trust uplift (71%), and future-proofing and agility (69%).**

Most organizations report meaningful privacy ROI from their efforts, but the quality and breadth of that value matter. Programs that demonstrate value only through compliance and risk avoidance are associated with essentially flat privacy competence, whereas layered value creation corresponds to materially stronger outcomes. To demonstrate this, we undertook statistical modeling to understand how each value layer contributes to overall privacy performance. Each level was first evaluated independently to estimate its impact, and then combined to assess cumulative effects.

Programs that deliver only compliance and risk avoidance (Level 1) perform weakly on their own. As the additional value layers are added, including operational efficiency (Level 2), revenue and trust impact (Level 3), and enablement capabilities (Level 4), outcomes improve progressively.

Predicted Privacy Index scores increase from -0.4 when only Level 1 is present, to 29 when Levels 1 and 2 are in place, to 61 when the first three levels are strong together, and to 90 when all four levels are fully realized.

The takeaway is clear: performance increases as privacy programs expand beyond compliance into operational, commercial, and strategic value.

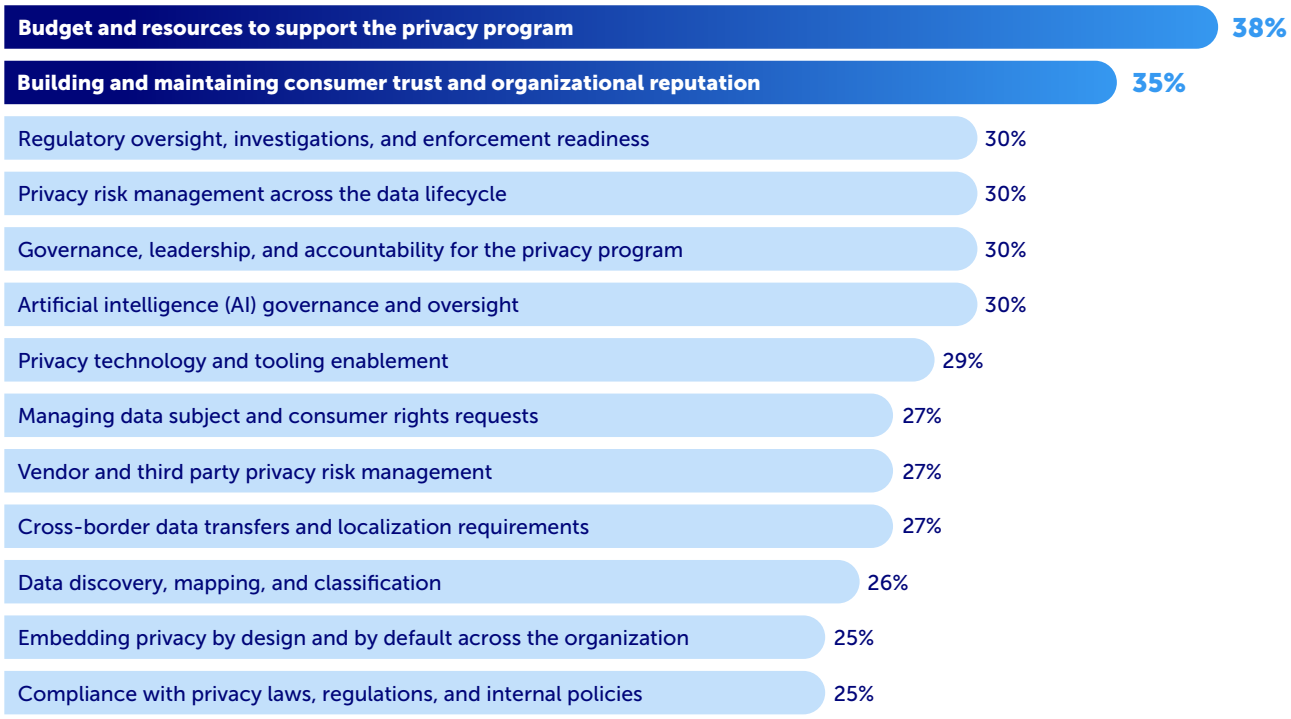
Privacy ROI Compounds as Programs Mature

Each layer added predicts dramatically higher GPI performance — compliance alone barely moves the needle

Organizations' top privacy maturity priorities center on securing budget and resources (38%) and maintaining consumer trust and reputation (35%), with enforcement readiness, AI oversight, and risk management close behind.

To what extent does each of the following areas represent a priority for advancing the maturity of your organization's privacy program in 2026?

Ranked on a 5 pt scale, with "Critical priority" the highest.



In 2026, 29% strongly agree that their company should do much more on privacy, up from 25% the prior year, while overall agreement remains high among respondents. Notably, this gap does not appear to stem from a lack of awareness. Nearly three-quarters report that privacy policies and procedures are well communicated and understood within their organizations, suggesting that the challenge lies less in communication and more in execution and capability.

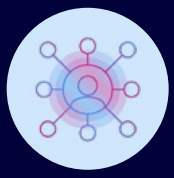
Taken together, these findings show that **privacy programs are shaped by both pressure and opportunity**. Organizations respond to incidents, regulatory risk, and operational complexity. At the same time, they increasingly see privacy as a mechanism for building trust, improving governance, and enabling responsible data use. Understanding this balance between risk mitigation and value creation helps explain why some programs evolve faster and perform more effectively than others.

To understand what distinguishes stronger programs from weaker ones, we examine the organizational behaviors that most consistently correlate with privacy competence. These seven foundational practices, first identified in earlier research, continue to provide a useful lens for evaluating how deeply privacy is embedded within organizations.

A proven formula for winners in privacy

In 2026, as in prior years, we assessed the seven foundational "Keys to Privacy" first identified in our 2020 research. These organizational behaviors reflect how deeply privacy is embedded in governance, culture, and day-to-day decision making. Organizations that demonstrate strength across multiple keys consistently achieve higher levels of stronger Global Privacy Index performance.

For the first six keys, we had respondents rate their level of agreement on a five-point scale, from "strongly agree" to "strongly disagree", on the following: "Please indicate whether you agree or disagree with each of the following statements."



Strategic Integration

"Privacy is a core part of our business strategy."

Privacy remains strongly embedded in business strategy, with 41% of respondents strongly agreeing that privacy is a core part of their business strategy.

Privacy Mindfulness

"Overall, we are mindful of privacy as a business."

Privacy awareness remains broadly embedded across organizations, with 39% strongly agreeing that overall, they are mindful of privacy as a business.

Employee Empowerment

"Every employee can formally raise a privacy issue with confidence that there will be no reprisal."

Employee empowerment regarding privacy is globally evident, with 36% strongly agreeing that employees can formally raise a privacy concern without fear of reprisal.

Privacy as a Differentiator

"We view our privacy practices as a key differentiator."

Privacy continues to be viewed as a source of business distinction, with 32% strongly agreeing that their organization views its privacy practices as a key differentiator.

Board-Level Engagement

"Our Board of Directors regularly reviews and discusses privacy matters."

Board involvement in privacy continues to strengthen, though it remains less developed than other dimensions: 32% strongly agree that their Board of Directors regularly reviews and discusses privacy matters.

Training and Awareness

"Our employees have been sufficiently trained in privacy matters."

Employee training remains an important but comparatively weaker area, with 29% strongly agreeing that employees have been sufficiently trained in privacy matters.

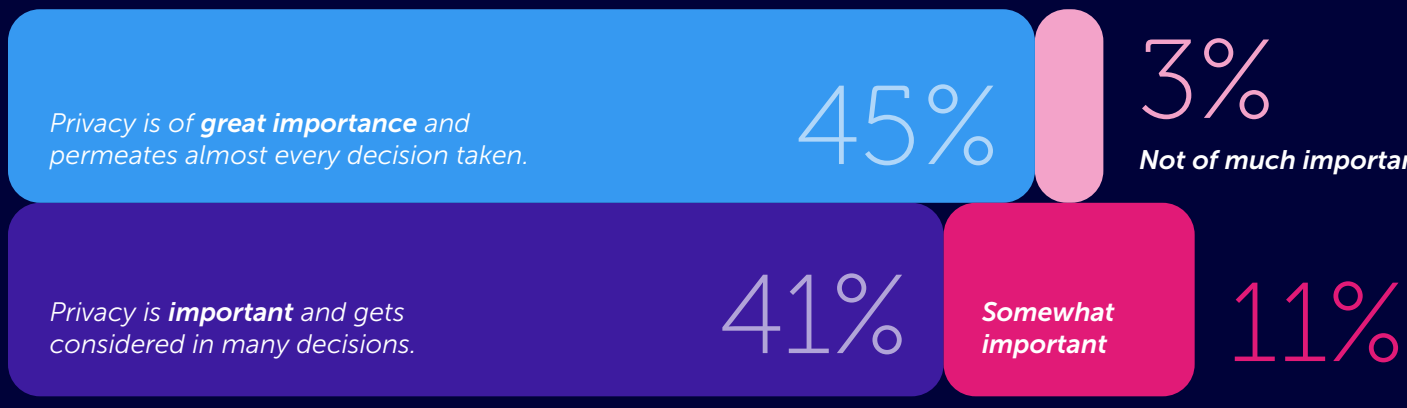
For the seventh key to privacy, we asked more broadly about how privacy considerations were woven into day-to-day decisions within organizations.

Level of Importance in Decision Making

"Which of the following statements best represents how your organization approaches privacy, in terms of levels of importance in how it affects day-to-day business decisions?"

While most organizations report that privacy meaningfully influences business decisions, fewer than half (45%) say it permeates almost every decision, suggesting many programs remain influential but not yet fully embedded in operational decision-making. On the downside, roughly one in ten companies still report that privacy is not very important when making many decisions.

Which of the following statements best represents how your organization approaches privacy, in terms of levels of importance in how it affects day-to-day business decisions?

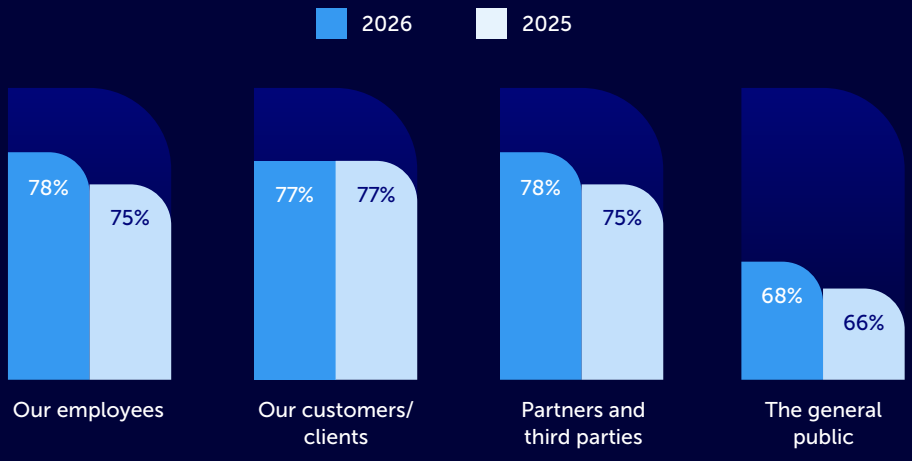


Organizations report strong overall confidence in their ability to protect sensitive employee and customer data, with 82% expressing either complete confidence (36%) or a great deal of confidence (46%). While this indicates that most companies believe their data protection capabilities are robust, a meaningful minority still reports only partial confidence, suggesting continued gaps between perceived capability and consistently secure outcomes.

How confident are you that your company is able to keep all of your employees' and your customers' relevant data secure and protected?

Organizations also perceive strong stakeholder confidence in their privacy practices, though this confidence declines as stakeholders move farther from internal operations. Employees (78%), customers (77%), and partners (78%) are viewed as having similarly high levels of confidence, while the general public trails at 68%. Year-over-year changes are modest but positive for most groups, with the largest gains among employees and partners, while customer confidence remains stable.

How much confidence do you think these key stakeholders have in your company's management of data privacy?



Together, these results suggest organizations believe internal and business-facing stakeholders maintain strong trust in their privacy practices, while broader public confidence remains more fragile.

Programs that excel across the seven keys tend to integrate privacy into strategy, culture, and daily decision-making, transforming privacy from a set of isolated controls into a core operational discipline.

The TrustArc Global Privacy Index

The TrustArc Global Privacy Index is a proprietary composite metric — developed in 2020 and revalidated in 2021 — that scores overall privacy competence on a scale from –100 to +100 across seven core competencies and five stakeholder outcome indicators. Functioning similarly to a Net Promoter Score for privacy, it offers a standardized, weighted benchmark for comparing how effectively organizations embed privacy across governance, culture, and operations.

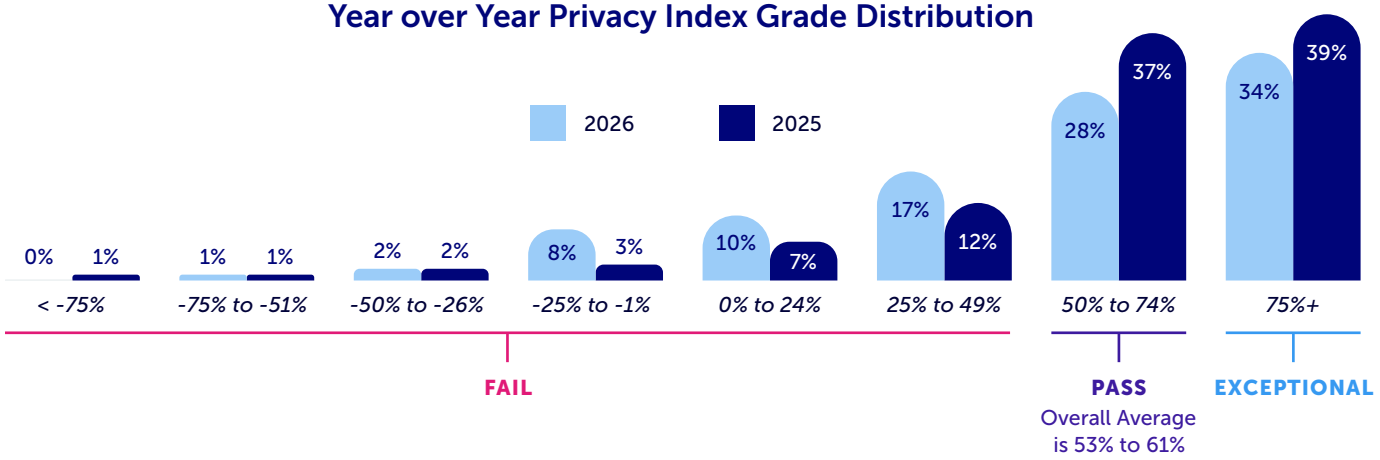
Global Privacy Index drops 8 points

REDUCED CONFIDENCE IN DATA PROTECTION

LIMITED PROGRESS EMBEDDING PRIVACY COMPANY-WIDE

WIDENING GAP BETWEEN LEADERS AND LAGGARDS

Year over Year Privacy Index Grade Distribution



Grade Distribution

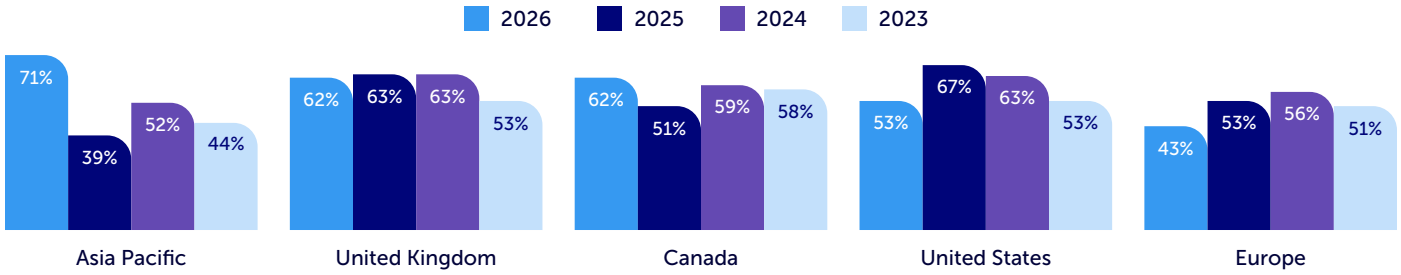
	2026	2025
▼	34% EXCEPTIONAL (75%+)	39%
▼	28% PASSING (50% TO 74%)	37%
▲	38% FAILING (<49%)	24%

Passing grades (50–74%) declined to 28%, while exceptional scores (75%+) remained relatively stable at 34%.

The global average is just 53%. Where do you think you sit?

Asia Pacific improved significantly to 71%, while Canada rose to 62%. Scores declined in the United States (53%) and Europe (43%) and remained stable in the United Kingdom (62%). Because the United States and Europe account for a large share of respondents, these declines weighed on the global average.

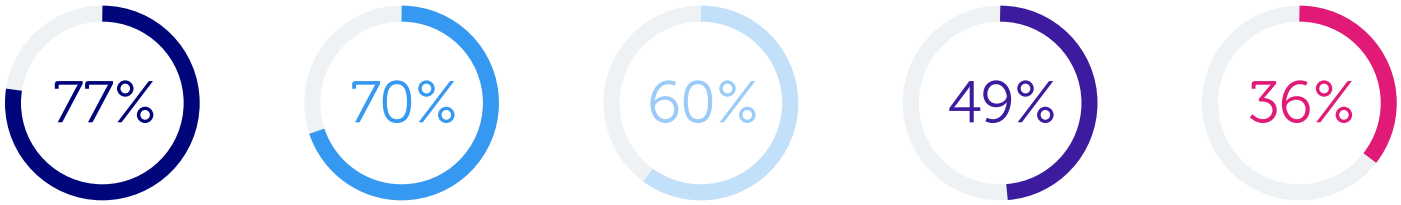
Year over Year Privacy Index Grade Distribution by Region



Organizations that are "transformative" in their privacy maturity level exceed the global average by 24 percentage points. The chart below reflects the distribution behind this result: while higher-maturity programs outperform, a larger share of organizations remain at lower maturity levels, pulling down the overall index.

How would you characterize your organization's maturity in Privacy Management?

Global Privacy Index Averages



Transformative
Setting industry standards and using innovative practices

Strategic
Using a risk-based approach to drive business value and competitive differentiation

Proactive
Anticipating and preventing issues through established processes

Compliant
Meeting minimum regulatory requirements

Reactive
Addressing issues only after they occur

Similarly, organizations with a privacy team score somewhat higher than the global average (59%), yet those without one score failing grades (24%), suggesting that having a privacy team is now simply table stakes.

The Global Privacy Index serves as a useful interpretive lens throughout this report — differences in governance structures, operational practices, technology environments, and strategic priorities translate into measurable differences in privacy performance.

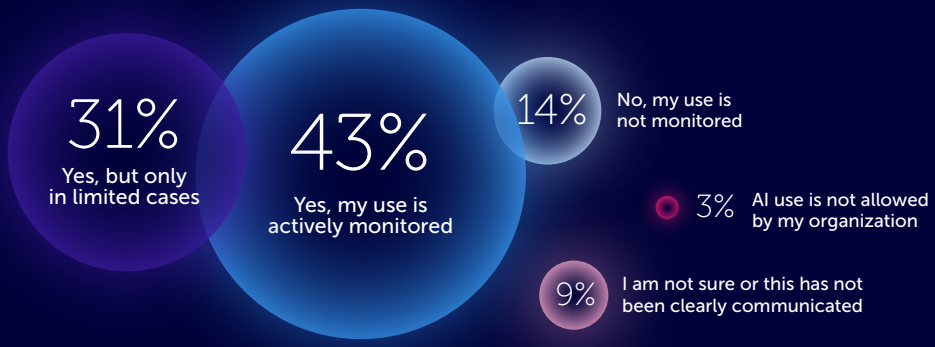
Where relevant, the analysis highlights which organizational choices most strongly distinguish higher performing privacy programs from those still developing their capabilities.

With that benchmark established, the report turns to one of the fastest evolving challenges for privacy programs today: artificial intelligence.

More deployment, stronger governance, continued challenges

As expanding AI use rapidly reshapes data use, privacy programs are being asked to manage new forms of risk while supporting innovation across the business. In 2026, **69% of respondents reported using AI tools very often or often in their day-to-day roles**, indicating that AI has moved well beyond experimentation into routine operational use. Oversight is also becoming more common: 43% say their AI use is actively monitored for compliance with privacy and security policies, and another 31% report limited monitoring. Analysis shows a strong positive correlation (0.51) between frequent AI use and active monitoring, suggesting that organizations expanding AI deployment are also strengthening governance alongside adoption.

To the best of your knowledge, is your own use of AI tools at work monitored to ensure compliance with your organization's privacy and security policies?



Despite widespread use, organizations report several challenges in ensuring AI privacy compliance. Rapidly changing technology (44%) and technical complexity (39%) lead the list of concerns, followed by limited privacy or compliance expertise (32%), unclear regulatory requirements (32%), and lack of AI-related technical expertise (30%).

What is challenging about ensuring that your AI systems comply with privacy requirements?

Choose all that apply

At the same time, most organizations have begun addressing these challenges through workforce preparation: 45% report providing comprehensive training on AI use and privacy considerations, and another 35% have issued basic guidance.

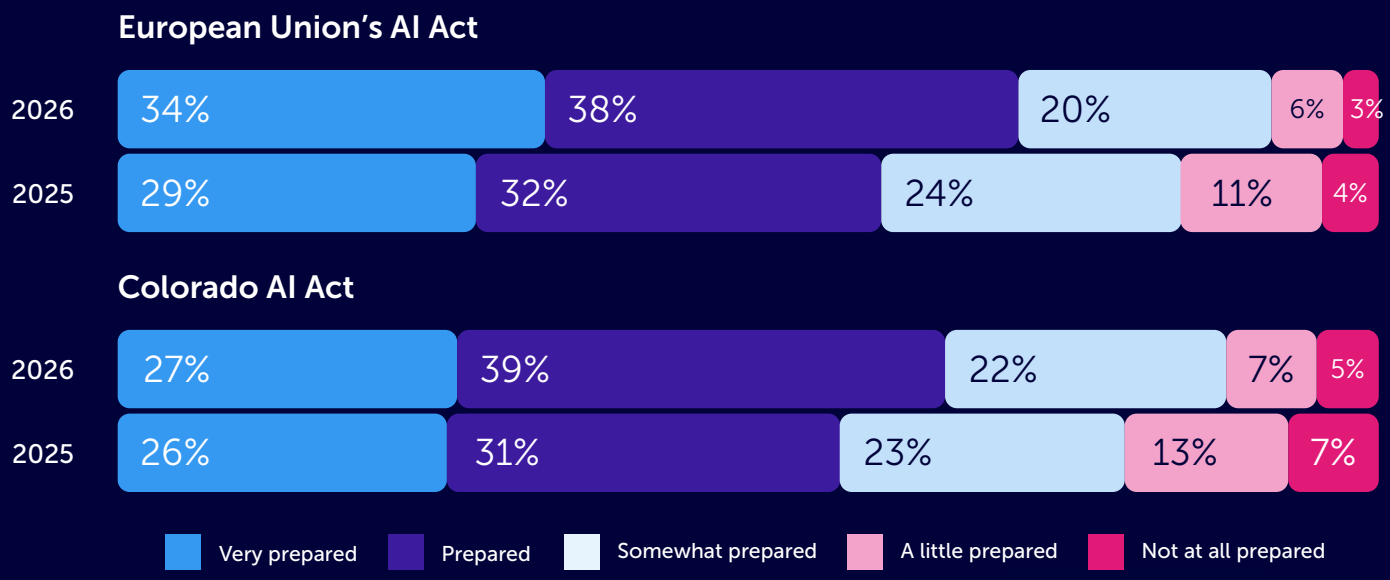
Organizations also report strong confidence in their ability to adapt privacy and data management practices to emerging AI regulations. In 2026, 76% expressed confidence in their ability to meet new global AI and data protection requirements. Preparedness for specific laws has also improved year over year. For the European Union's AI Act, 72% report being very prepared or prepared in 2026, up from 61% the prior year. Similar gains are seen for the Colorado AI Act, with 66% now reporting being very prepared or prepared, up from 57% in 2025.

76%

feel confident in meeting new global AI regulations

How prepared do you feel your company is for enforcement of the following new AI regulations as they pertain to privacy requirements.

Excludes "Does not apply"



Leadership pressure to accelerate AI adoption is also rising. In 2026, 74% of respondents agree or strongly agree that their leadership team is pushing to expand AI deployment across business units, up from 66% in 2025. As AI adoption expands, privacy teams are increasingly responsible for ensuring that governance, training, and regulatory readiness keep pace with technological change. The results suggest that many organizations are beginning to build this capability, but the operational complexity of AI systems continues to challenge traditional privacy controls.

Managing these demands often requires more than policy and oversight alone. Organizations increasingly rely on specialized technology to operationalize privacy governance at scale.

+8%

more pressure from leadership to adopt AI

Integrated, interoperable solutions win…when paired with action

Privacy programs increasingly depend on technology to manage the scale and complexity of modern data governance. Here we explore the tools organizations use to support these activities, the structure of their privacy technology stacks, and how integration across systems influences overall program effectiveness.

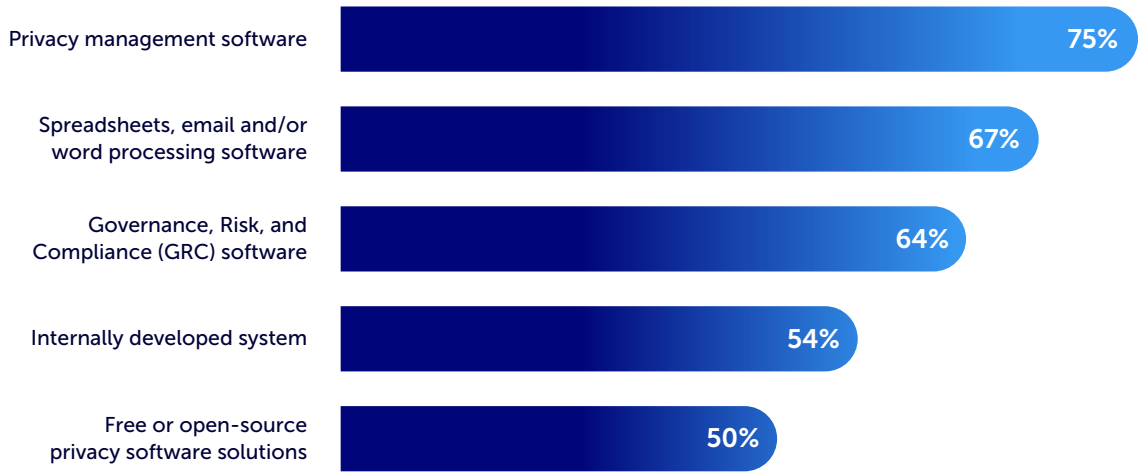
Organizations continue to rely on a mix of technologies to manage privacy programs. Dedicated privacy management software remains the most common primary solution, used by 22% of respondents in 2026. Internally developed systems (25%) and GRC platforms (19%) are also widely used, while others continue to rely on open-source tools (16%) or manual approaches such as spreadsheets and email (18%). The distribution has remained relatively stable over time, indicating that many organizations are still evolving toward more integrated privacy technology environments.

Organizations using dedicated privacy management software report the highest Global Privacy Index scores at **75%**.

Privacy program performance varies significantly depending on the primary technology used. **Organizations using dedicated privacy management software report the highest Global Privacy Index scores at 75%**. Programs relying primarily on spreadsheets or basic office tools average 67%, while GRC systems average 64%. In contrast, organizations using internally developed tools (54%) or open-source solutions (50%) score substantially lower. Purpose-built platforms are more consistently associated with higher levels of operational privacy competence.

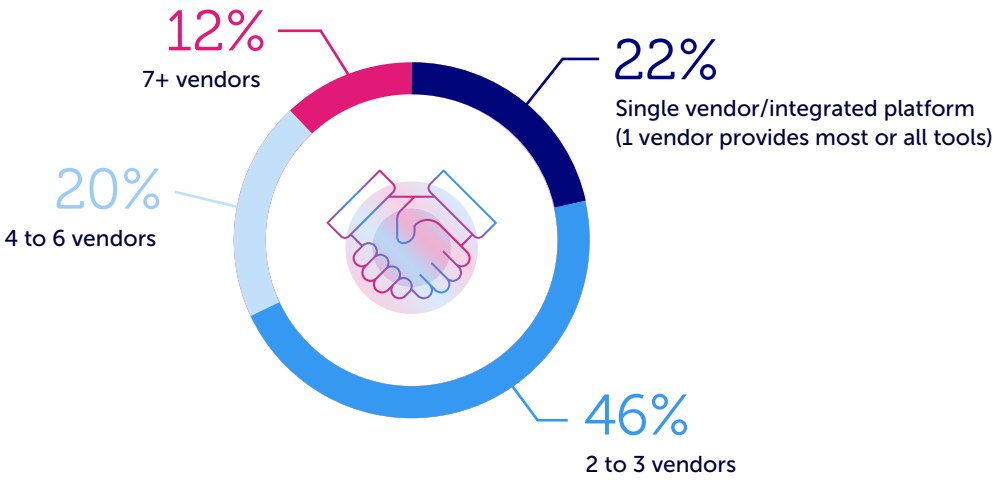
Global Privacy Index Scores shown by "What primary solution do you use to manage your privacy program?

Excludes "Don't know/Not sure"



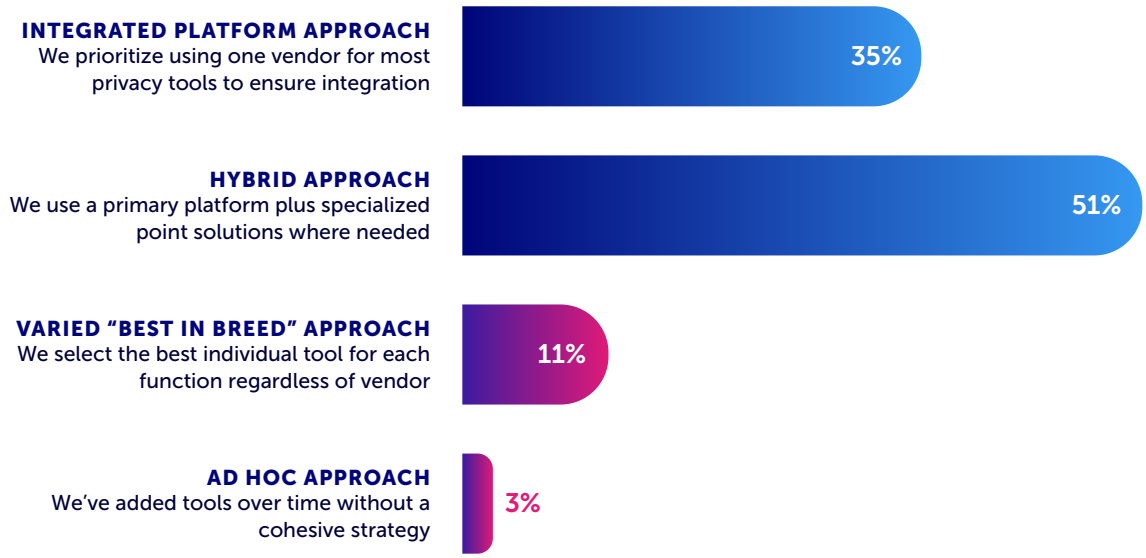
Most organizations do not rely on a single privacy vendor. In 2026, almost half (46%) report using two to three vendors to support their privacy capabilities. At the tails of the distribution, 12% operate complex stacks of seven or more tools while 22% rely primarily on a single integrated platform.

How many different vendors does your organization currently use to manage the privacy tools discussed in this survey?



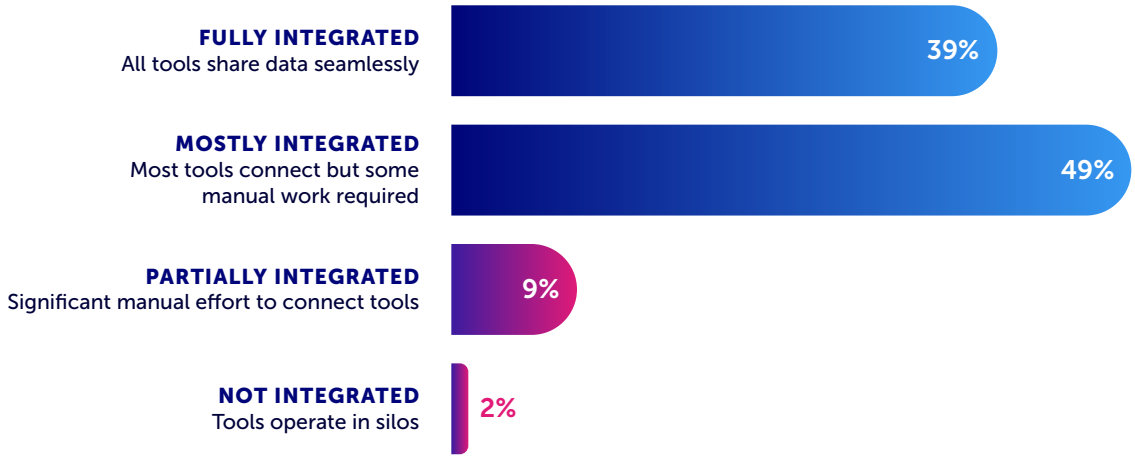
Reflecting this multi-vendor environment, most organizations pursue a hybrid technology strategy: 51% report using a primary privacy platform combined with specialized point solutions. Fully integrated single-vendor approaches account for 35% of programs, while best-in-breed multi-vendor strategies (11%) and ad hoc tool accumulation (3%) are relatively uncommon.

Which statement best describes your organization's privacy software technology stack?



Interoperability across privacy tools plays an important role in program maturity. Nearly nine in ten organizations report that their privacy tools are at least mostly integrated, with 39% saying their systems share data seamlessly and another 49% indicating that most tools connect but still require some manual work.

How would you rate the integration and interoperability of your privacy tools?



The level of integration also strongly influences the outcomes of privacy programs. **Organizations with highly integrated technology environments and six or more fully implemented privacy initiatives achieve Global Privacy Index scores of 75%, well above the global average.** In contrast, fragmented programs with partially integrated tools and fewer implemented initiatives average only 21%. That is, Integrated leaders achieve nearly 4 times the privacy competence of fragmented programs.

Fragmented vs. Integrated Programs

FRAGMENTED PROGRAM

~21%

AVERAGE GPI SCORE

Siloed, manual processes

GRC tools adapted for privacy

Reactive compliance posture

≤ 5 initiatives fully implemented

INTEGRATED LEADER

~75%

AVERAGE GPI SCORE

Purpose-built privacy platform

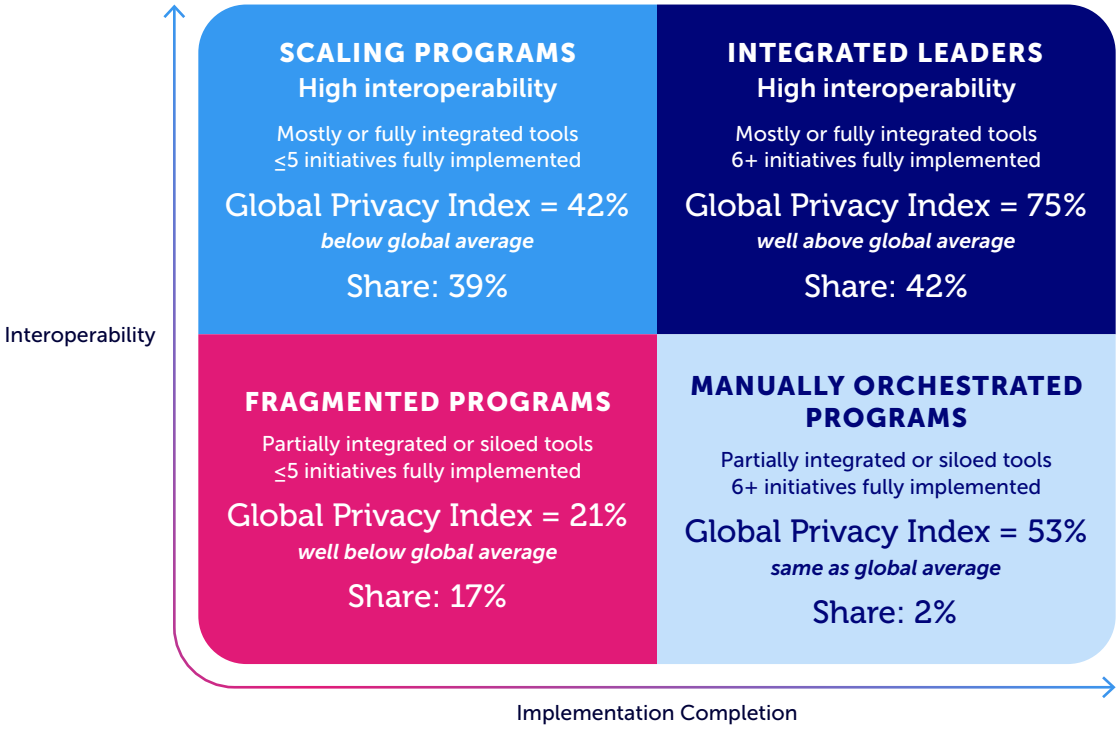
Fully integrated tech stack

Principles-based governance

6+ initiatives fully implemented

4x higher competence

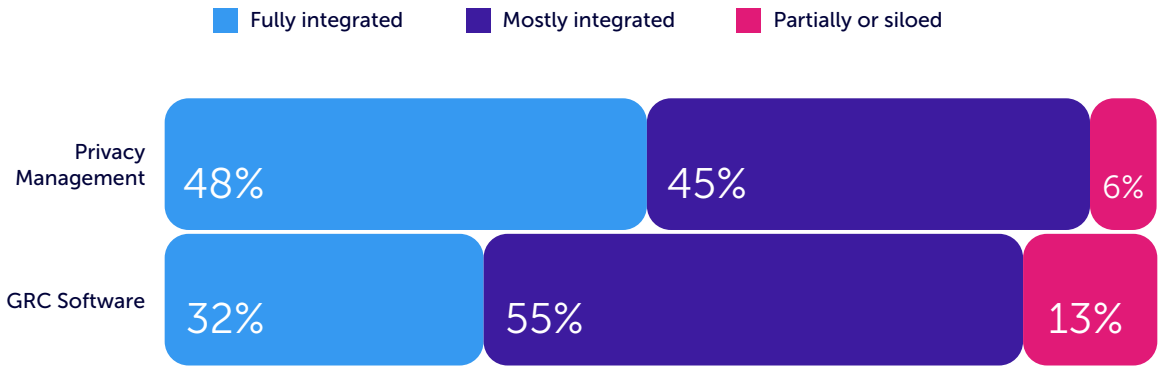
Profiling of Privacy Toolsets



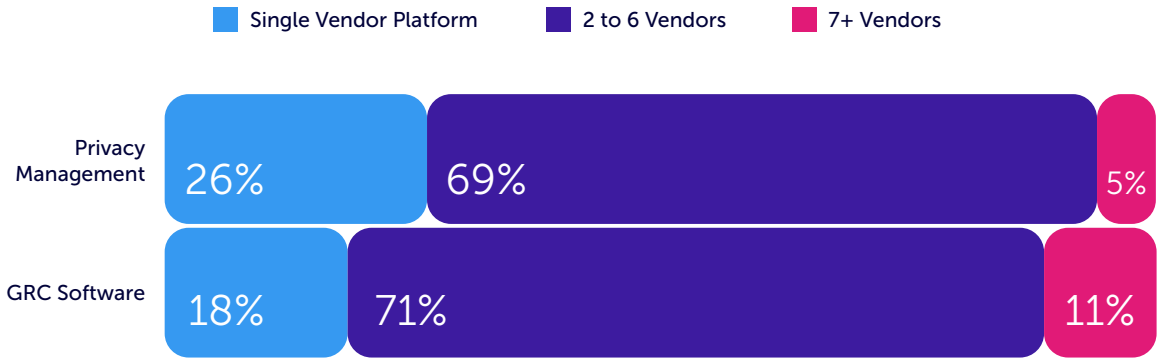
Technology choices also shape the structure of the broader privacy stack. Privacy management platforms are more likely to operate platform-centric architectures, while GRC implementations more often produce fragmented multi-vendor stacks. That is, **organizations that use privacy management software as their primary solution are more likely to have fully integrated technology interoperability, fewer privacy vendors, and an integrated platform than those that use GRC software.** GRC deployments more often evolve into hybrid multi-tool ecosystems.

PROFILING PRIVACY MANAGEMENT VERSUS GRC SOFTWARE

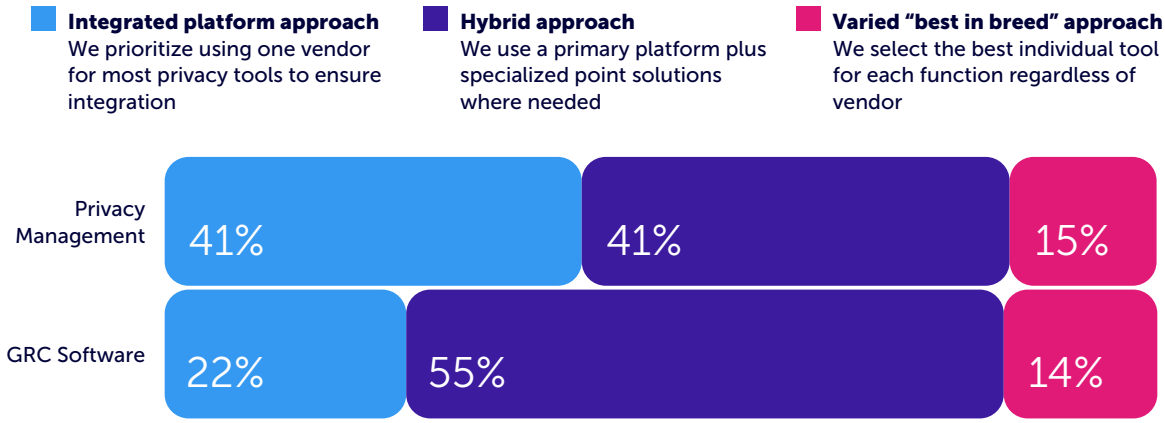
Privacy Platforms Show Higher Integration than GRC Solutions



Privacy Platforms More Likely Single Vendor Than GRC Solutions



Privacy Platforms Favor Integrated Architectures More Than GRC



Organizations that operate integrated privacy technology environments and rely on purpose-built platforms tend to achieve higher levels of privacy competence than those that manage fragmented tools or manual processes. Integration allows privacy teams to coordinate initiatives, share data across systems, and scale governance practices more consistently across the enterprise.

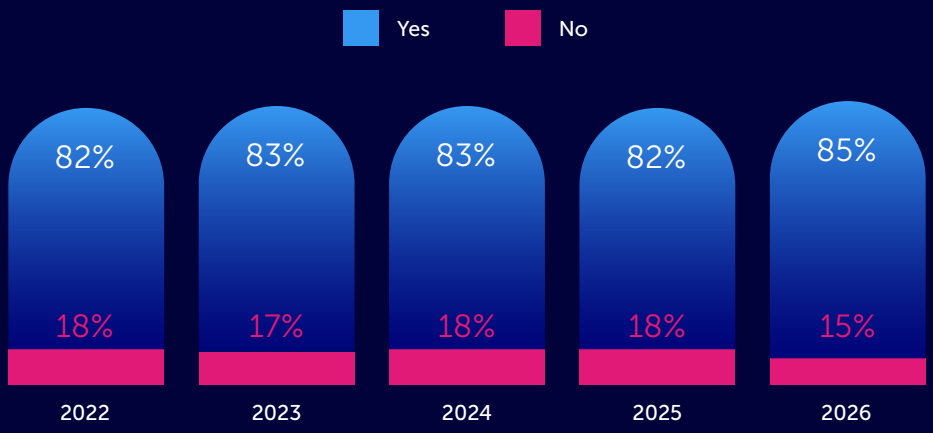
However, technology alone does not determine whether a privacy program is effective. Organizations must also evaluate whether their policies, controls, and operational activities are delivering the intended outcomes.

Privacy management platforms are nearly twice as likely to operate fully integrated tech stacks compared to GRC software (48% vs. 32%), giving privacy teams a structural advantage in coordinating data governance at scale.

Measure it, manage it, operationalize it

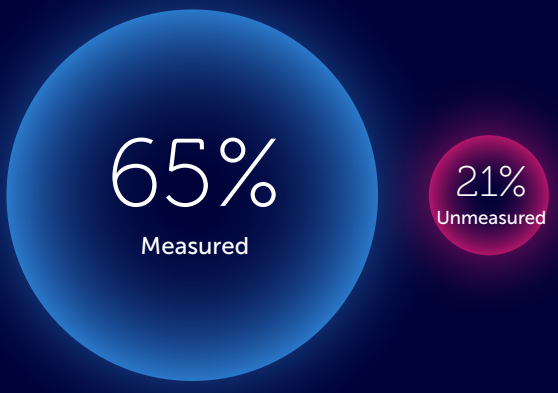
Most organizations now report measuring the effectiveness of their privacy programs, reflecting the growing maturity of privacy governance. In 2026, 68% say they track program effectiveness, and when excluding unsure respondents, this rises to 85%. The consistency of this figure over several years suggests that formal measurement has become a standard component of modern privacy programs, supporting stronger oversight and accountability.

Does your company currently measure the effectiveness of its privacy program?



The impact of measurement on program performance is substantial. Organizations that measure the effectiveness of their privacy programs achieve an average Global Privacy Index score of 65%, compared with just 21% among those that do not, underscoring that measurement is a strong indicator of operational discipline and program maturity.

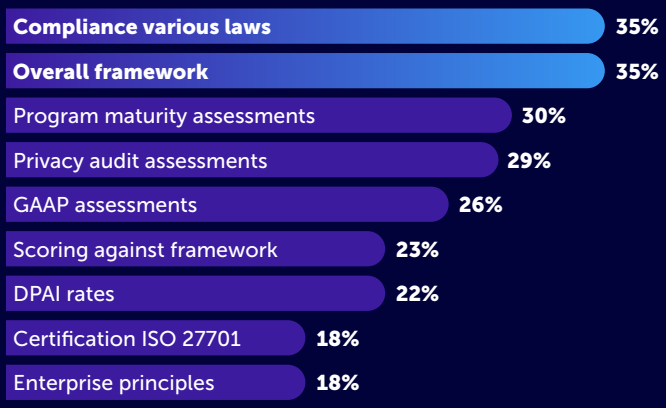
Average GPI Score: Measured vs Unmeasured



When organizations measure privacy performance, they most often do so through structured frameworks and regulatory alignment. Compliance with applicable laws and internal privacy frameworks are the most commonly cited methods, each used by 35% of organizations, followed closely by maturity assessments and internal audit processes. At the operational level, privacy teams most frequently track performance using activity-based KPIs, such as response times and completion rates for privacy impact assessments, reflecting a focus on operational efficiency and program throughput.

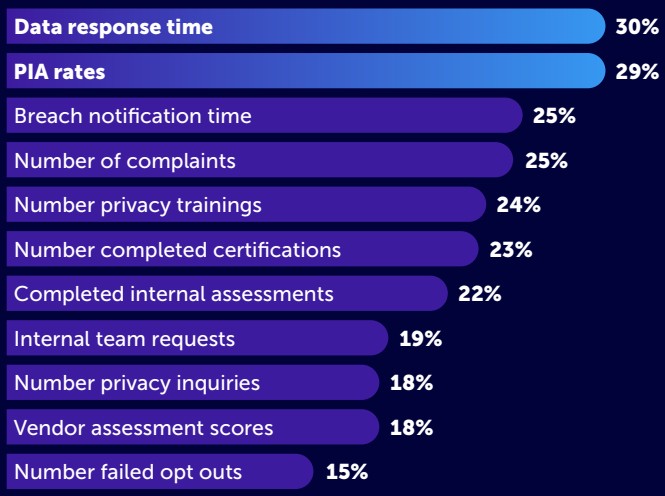
What are your company's primary methods for measuring your privacy program?

Choose all that apply



What are your company's privacy program KPIs?

Choose all that apply

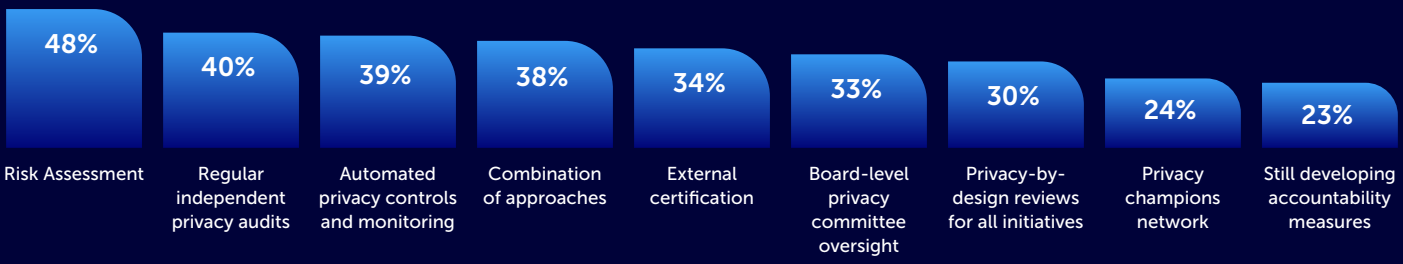


Organizations also rely on a range of governance mechanisms to ensure privacy accountability. Risk assessments are the most widely used approach, reported by 48% of organizations in 2026, followed by regular independent audits and automated privacy controls and monitoring. Compared with the prior year, several governance mechanisms show modest growth, including automated monitoring, external certifications, and privacy-by-design reviews. Together, these practices indicate that organizations are gradually expanding accountability beyond traditional audit processes toward more embedded and technology-enabled privacy governance.

While measurement has become a hallmark of high privacy performance — allowing for better resource allocation, risk management, and continuous improvement — measurement alone does not create maturity. The real test lies in how organizations translate governance, priorities, and oversight into concrete operational practices.

How does your organization ensure privacy accountability?

Choose all that apply

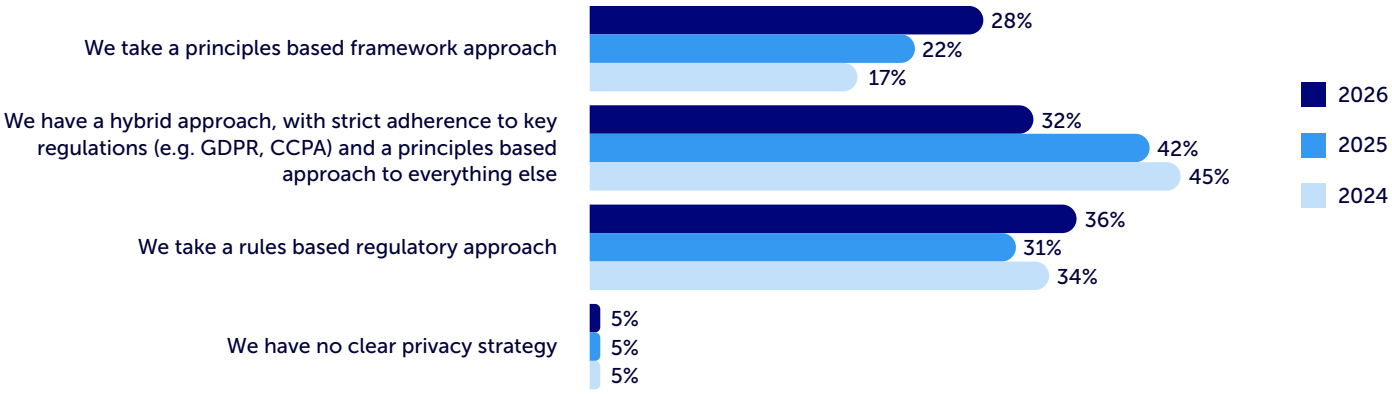


Walking the privacy walk pays off

Privacy maturity ultimately depends on how organizations operationalize privacy programs in practice, including the regulatory approaches they follow, the privacy initiatives they have implemented, and the certifications and governance frameworks that help structure these efforts.

In 2026, 36% report following a rules-based regulatory approach, up from 31% in 2025, while hybrid strategies that combine strict regulatory compliance with broader principles-based governance have declined to 32%. At the same time, 28% now report operating under a primarily principles-based framework.

Which statement best reflects your company's approach to your privacy program?



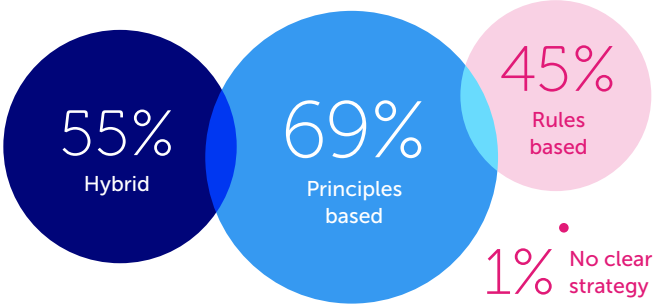
A rules based approach focuses on meeting defined regulatory obligations. A principles based approach applies broader privacy principles to guide decisions across the organization and across jurisdictions. This requires greater privacy competence, including the ability to use judgment to reconcile competing legal requirements and design programs that are defensible, adaptable, and aligned with the intent of the law rather than rigid rule execution.

This distinction plays out clearly in the results, in which, while hybrid approaches are broadly in line with the average at 55%, and rules based approaches fall 8 points below average at 45%. Organizations with no clear strategy perform dramatically worse, with a negligible score, underscoring the importance of having a defined and operationalized approach to privacy management.

Principles-based approach =

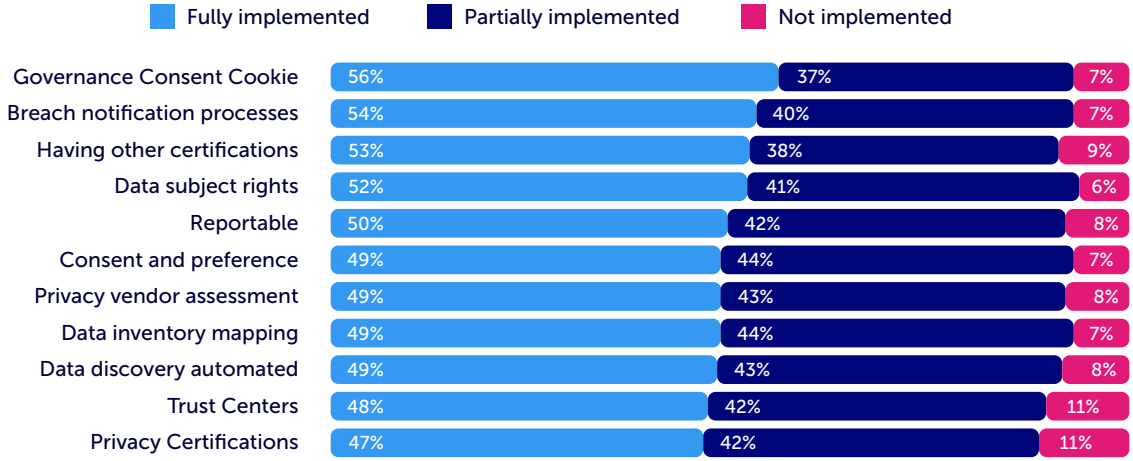
+16% points

better GPI scores



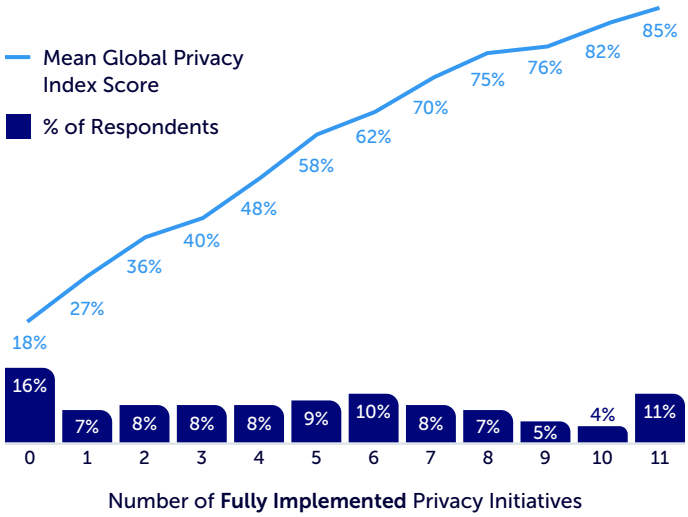
Across organizations, a wide range of operational privacy initiatives are now broadly implemented. Core operational capabilities show the highest levels of adoption, including governance for cookie consent (56% fully implemented) and breach notification processes (54%). Data subject rights management and reportable privacy programs also exceed 50% full implementation. Capabilities such as vendor privacy assessments, data inventory and mapping, and automated data discovery are close behind, indicating that many organizations are building comprehensive operational privacy infrastructures across both internal data governance and external compliance requirements.

For each of the following privacy initiatives, please indicate the state of implementation at your company currently.



The number of initiatives implemented is directly and predictably related to privacy maturity. Organizations with only a few implemented initiatives score significantly below the global average on the Global Privacy Index, while maturity increases steadily as programs expand. By the time organizations have implemented ten or more initiatives, average privacy competence reaches the **mid-80% range, demonstrating that operational breadth and program completeness are closely linked to overall privacy effectiveness**.

Global Privacy Index by Number of Privacy Initiatives



The privacy initiatives measured included the following:

- DSR requests management
- Cookie consent + website tracker
- Consent and preference management (omnichannel)
- Breach notification processes
- PIAs through the supply chain
- Strategic and reportable privacy program
- 3rd party privacy certs
- Having other certifications
- Trust Center
- Data discovery
- Data inventory and mapping

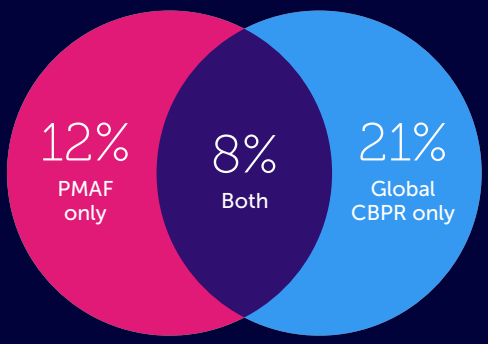
Participation in key frameworks signals higher privacy competence

Formal certifications and governance frameworks also play a central role in program implementation. Globally recognized privacy and security standards such as ISO/IEC 27701 and Europrivacy are cited as the most valuable certifications, each selected by 41% of organizations. Security-adjacent frameworks, including ISO/IEC 27002 and broader privacy governance standards such as ISO/IEC 29100 are also widely valued. These results indicate that organizations frequently adopt privacy certifications within broader information security and governance ecosystems rather than as isolated compliance exercises.

Which certification or compliance standards are most valuable to your company?

Choose all that apply

Adoption of Nymity PMAF and APEC/Global CBPR Framework



Governance frameworks often serve as anchors for broader certification strategies. Among organizations adopting the Nymity Privacy Management Accountability Framework (PMAF), nearly 40% also participate in the Global CBPR program.

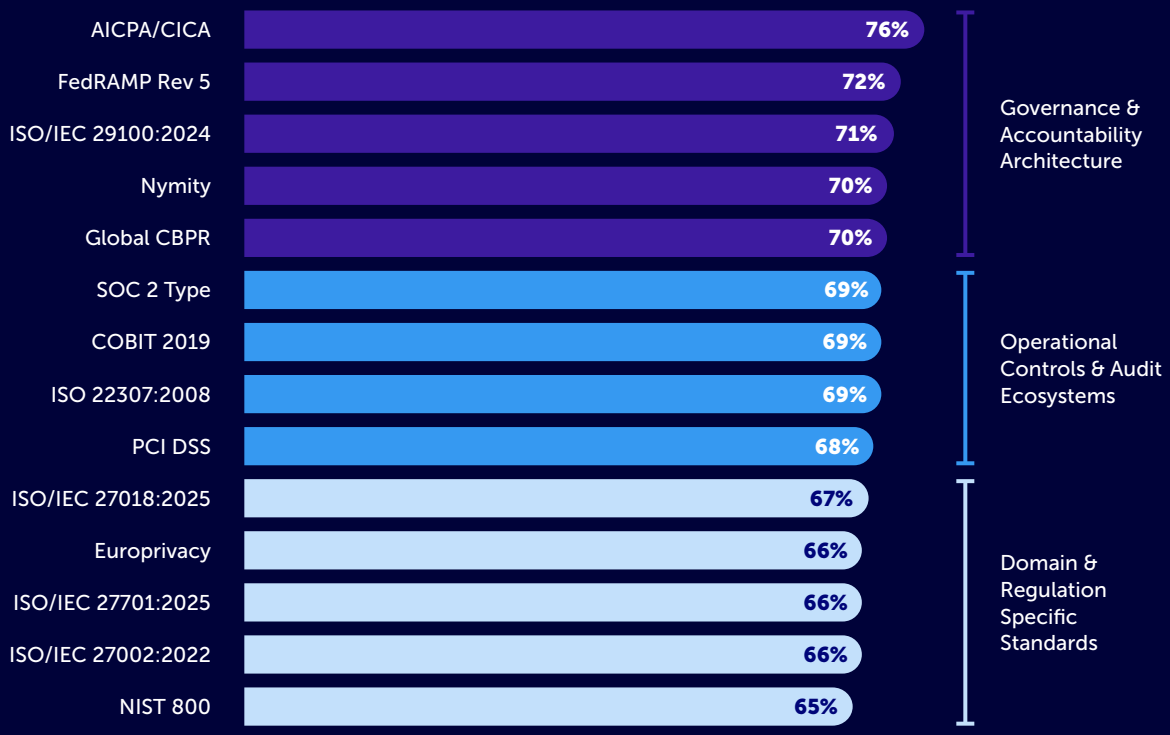
Global/APEC CBPR adopters tend to share a distinct profile: they are predominantly large enterprises, operate across multiple geographic regions, and frequently report active AI usage and monitoring practices. Workforce privacy training is also common within these organizations, reflecting the governance maturity typically associated with cross-border privacy certification programs.

Profile of Global/APEC CBPR Adopters

- Predominantly large enterprises, with 88% from companies exceeding $500M in revenue.
- Higher concentration in the technology sector (35%).
- Operations spanning multiple regions (average is over 3 regions).
- Widespread AI use, with 83% using AI often or very often.
- Active monitoring of AI usage, reported by 88% of organizations.
- Workforce privacy training is common, with 81% reporting that they provide employee guidance or training.
- Europrivacy certification appears in 53% of Global CBPR programs.

Across all certification types, participation correlates with higher levels of privacy competence. Programs anchored in governance and accountability frameworks achieve some of the highest Global Privacy Index scores, often outperforming programs focused primarily on domain-specific standards. These findings suggest that certifications deliver the greatest maturity gains when they reinforce enterprise governance structures rather than serving solely as technical compliance controls.

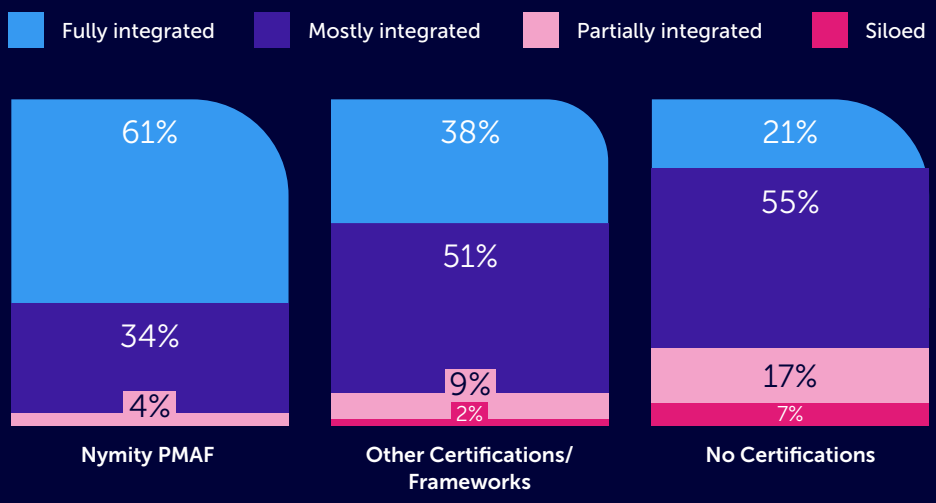
Global Privacy Index Averages by Frameworks/Certifications



The relationship between governance frameworks and operational performance is particularly evident among organizations that adopt the Nymity Privacy Management Accountability Framework. These organizations are significantly more likely to operate fully integrated privacy technology environments and consistently achieve some of the highest Global Privacy Index scores. In combination with integrated technology stacks, Nymity adopters demonstrate especially strong privacy competence, reinforcing the importance of aligning governance frameworks with interoperable privacy technology infrastructure. Organizations adopting the Nymity PMAF are three times as likely to operate with fully integrated privacy technology stacks as organizations without formal certifications.

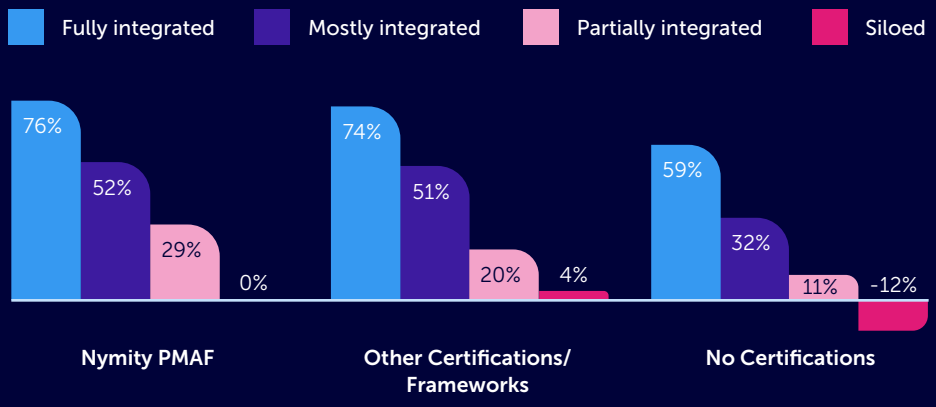
IMPACT OF NYMITY PMAF ADOPTION

Nymity PMAF Adopters Lead in Integration



More Integrated Programs Deliver Higher Privacy Performance

Global Privacy Index Score



Organizations that operationalize privacy through multiple initiatives, structured governance frameworks, and recognized certifications tend to achieve stronger privacy competence. Implementation, combined with integrated technology environments, strengthen how organizations manage data, risk, and innovation.

Conclusion

The gap between mature and developing privacy programs continues to widen. The Global Privacy Index declined to 53% in 2026 as many mid-performing organizations struggled to keep pace with rising regulatory complexity, expanding data ecosystems, and rapid AI adoption. Yet stronger programs follow a consistent path: those that implement structured operational initiatives, supported by interoperable privacy technology, achieve dramatically higher levels of competence and privacy maturity rises steadily.

At the same time, AI is accelerating pressure on privacy programs, making governance and accountability frameworks more important than ever. Organizations with coordinated initiatives and integrated technology are better able to keep pace — and far more likely to realize measurable business value from privacy investments, moving beyond compliance toward operational efficiency, customer trust, and innovation readiness.

PRIVACY IN 2026

Mature programs pull away from the pack

Laggards fall farther behind

AI pressure grows with daily adoption

Concerted initiatives ***and*** integrated tech drive ROI

Glossary of Terms

AI Governance and Oversight	Policies, procedures, roles, and responsibilities to ensure responsible, ethical, transparent, and accountable deployment, development, and monitoring of AI systems throughout their lifecycle. It includes establishing cross-functional oversight bodies, defining acceptable use policies, conducting risk assessments of AI systems, and maintaining AI inventories.
Consent and Preference Management	The set of processes, systems, and procedures an organization uses to collect, record, honor, update, and revoke individuals' consent for the collection and processing of their personal data. It spans the full data lifecycle — from how consent is obtained (e.g., opt-in checkboxes, contracts, portals) to how preferences are stored, enforced, and updated — ensuring that personal data is only used in accordance with individuals' expressed wishes.
Cookie Consent and Tracker Governance	The organizational practices and technical mechanisms used to manage the placement of cookies and other online tracking technologies (e.g., pixels, fingerprinting, web beacons) on users' devices in compliance with applicable laws. This includes deploying consent banners, categorizing trackers (essential vs. non-essential), honoring opt-in/opt-out signals, and ensuring no non-essential trackers load before valid user consent is obtained
Cross-Border Data Transfers	The rules and mechanisms governing the movement of personal data across national or regional borders. Cross-border transfers refer to sharing personal data with entities outside a jurisdiction (e.g., via standard contractual clauses, adequacy decisions, or binding corporate rules).
Data Localizations	Data localization refers to legal requirements mandating that certain data be stored and processed only within a country's own territory.
Automated Data Discovery	Automated data scanning to identify, classify, and analyze personal and sensitive data across systems.
Data Inventory and Mapping	A comprehensive catalog of all personal data assets that an organization holds, processes, or shares. It serves as a single source of truth that answers key information to comply with privacy laws across systems and builds records of processing activities to support compliance and audits.
Record of Processing Activities (ROPA)	A comprehensive, documented register — required under regulations like the GDPR (Article 30) — that captures all personal data processing activities within an organization. It includes the purposes of processing, categories of data subjects and personal data, data recipients, international transfers, retention periods, and security measures. It serves as an accountability tool, audit trail, and foundation for compliance with data protection laws.
Data Protection Impact Assessment (DPIA)	A structured process used to identify and assess privacy risks arising from new or high-risk data processing activities before they begin. Required under GDPR Article 35 when processing is likely to result in a high risk to individuals' rights and freedoms (e.g., large-scale processing, profiling, systematic monitoring), a DPIA describes the processing operations, assesses necessity and proportionality, evaluates risks to data subjects, and documents measures to mitigate those risks.

Glossary of Terms

Data Subject Request (DSR)	A formal request made by an individual (data subject) to exercise their privacy rights under applicable data protection laws. These rights typically include the right to access, rectify, erase, restrict, object to, or port their personal data. Organizations are generally required to respond within a defined timeframe (e.g., one month under GDPR) and must have processes in place to verify identity, track, and fulfill such requests.
Governance, Risk, Compliance (GRC) Software	Technology platforms that help organizations align business objectives with risk management and regulatory compliance obligations.
Global Privacy Index	A composite metric measuring organizational privacy competence across seven core competencies and stakeholder outcomes, producing a standardized score from –100 to +100.
Privacy Accountability	The principle and practice by which organizations accept responsibility for protecting personal data and can demonstrate that their privacy programs are effectively implemented. Accountability comprises three key elements: Responsibility (maintaining ongoing privacy management activities), Ownership (assigning individuals to be answerable for those activities), and Evidence (documenting that activities are being performed).
Privacy Audit Assessments	A systematic examination of an organization's privacy policies, practices, and controls to assess compliance with applicable laws and standards, identify gaps and risks, and recommend improvements. Privacy audits can be conducted internally (by internal audit or the privacy office) or externally (by third-party auditors), using benchmarks such as the Generally Accepted Privacy Principles (GAPP) or applicable regulatory frameworks.
Privacy Impact Assessment (PIA)	A preventive risk management process that evaluates the potential privacy impacts of a project, program, system, or process involving personal information — ideally conducted before the project begins. A PIA identifies how personal data flows, analyzes potential risks to individuals' privacy, and recommends measures to eliminate, minimize, or mitigate those impacts. It is recognized as a best practice globally and is mandatory in some jurisdictions.
Privacy Management Maturity Levels	A framework for measuring how advanced and capable an organization's privacy program is against established benchmarks. Based on models such as the AICPA/CICA Privacy Maturity Model, maturity is typically measured across five levels: Transformative (industry-leading innovation), Strategic (risk-based value creation), Proactive (issue prevention), Compliant (meeting minimum requirements), and Reactive (responding after issues occur).
Privacy Management Software	Purpose-built software that helps organizations manage, automate, and demonstrate privacy compliance across their programs. These tools typically support activities such as data inventory and mapping, PIA/DPIA management, DSR fulfillment, vendor risk assessment, policy management, consent management, training tracking, and compliance reporting — enabling structured and scalable privacy program management.
Privacy Program	The comprehensive set of policies, procedures, communications, controls, and ongoing activities that an organization maintains to manage personal data responsibly and in compliance with applicable laws.

Glossary of Terms

Privacy Program Effectiveness	The degree to which an organization's privacy program achieves its intended goals, namely, managing privacy risks, demonstrating accountability, and ensuring compliance with applicable laws. Effectiveness is measured through ongoing monitoring, audits, metrics (e.g., training completion rates, DSR response times, breach statistics), and the ability to demonstrate that privacy management activities are embedded across the organization.
Privacy Program KPIs	Quantitative measures used to track privacy performance, such as complaint volumes, response times, assessment completion rates, and vendor scores.
Privacy Risk Management	The systematic process of identifying, assessing, prioritizing, and treating risks arising from the collection, use, and disclosure of personal data. It involves establishing context, analyzing the likelihood and impact of privacy risks, implementing controls to mitigate those risks, and continuously monitoring for changes. Privacy risk management is typically integrated into an organization's broader enterprise risk management framework.
Program Effectiveness Measurement Methods	The approaches and tools used to assess whether a privacy program is achieving its objectives. These methods include: self-assessments and internal audits, privacy maturity models (e.g., AICPA/CICA PMM, CNIL maturity tool), KPI tracking and dashboards, benchmarking against industry standards, evidence-based accountability scorecards, and feedback from regulators or external auditors.
Third-Party / Vendor Privacy Risk Management	The structured process of identifying, assessing, and managing the privacy and data protection risks associated with external vendors, processors, and service providers who handle personal data on behalf of an organization. It includes vendor tiering, due diligence questionnaires, contractual requirements, ongoing monitoring, and remediation of compliance gaps — recognizing that organizations remain accountable for personal data processed by their third parties.
Trust Center	A public-facing portal that an organization shares its privacy, security, legal, and compliance documentation with customers, partners, and regulators. Typically includes privacy policies, subprocessor lists, terms of service, disclosures, and security and privacy.

Appendix

A Global View: Survey Scope and Reach

This year's Global Privacy Benchmarks reflect the perspectives of 1,844 privacy leaders, executives, and business professionals responsible for managing data protection, governance, and digital risk. Now in its seventh year, the study provides a 360° view into how organizations are adapting their privacy programs to new operational pressures, including expanding global regulations, the rapid adoption of artificial intelligence, and rising expectations around digital trust. The study also scores participants on a proprietary Global Privacy Index meant to measure privacy competence. The research was commissioned by TrustArc and conducted independently by Golfdale Consulting, to ensure objective, high-integrity findings.

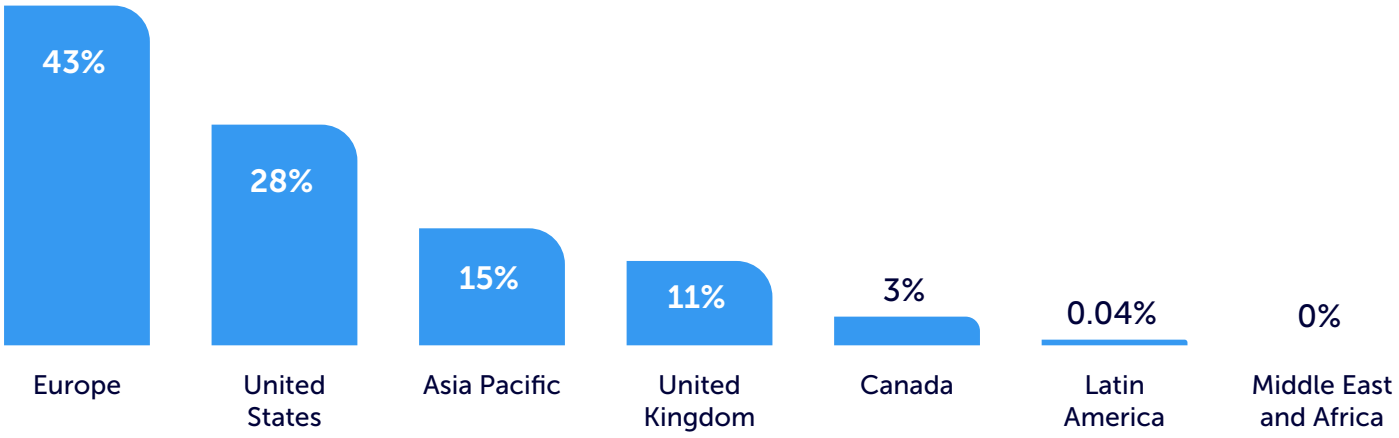
Fieldwork for the 2026 study was conducted between January 23 and February 18, 2026, using online research panels and open web surveys distributed through TrustArc's website, social media channels, and email outreach. Respondents are distributed across major global markets. Europe and the United States represent the largest shares of participation, while Asia Pacific increased significantly in 2026, accounting for 15% of the sample. This expansion reflects the growing global importance of privacy regulation, including developments such as India's Digital Personal Data Protection Act.

The study also captures the multinational complexity of modern privacy management.

> *Modern privacy management reflects how organizations embed privacy into operations, technology, and business decision-making while navigating overlapping regulations, cross-border data flows, and evolving stakeholder expectations.*

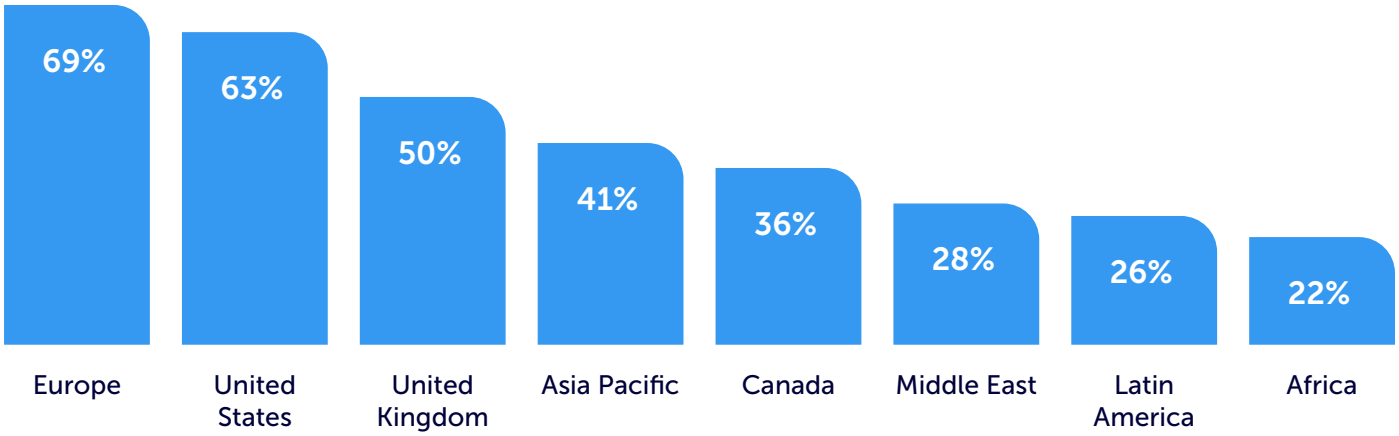
While about four in ten organizations operate in only one region, the average company in the study operates in more than three regions globally. This broad footprint highlights the challenges organizations face as they navigate overlapping regulatory requirements, cross-border data flows, and differing expectations around data protection and digital trust.

Where is your Head Office located?



Which of the following regions and countries does your company operate in?

Choose all that apply



Together, these responses provide one of the most comprehensive global snapshots available of how organizations are operationalizing privacy governance, investing in privacy technology, and preparing for the next phase of AI-driven regulatory change.

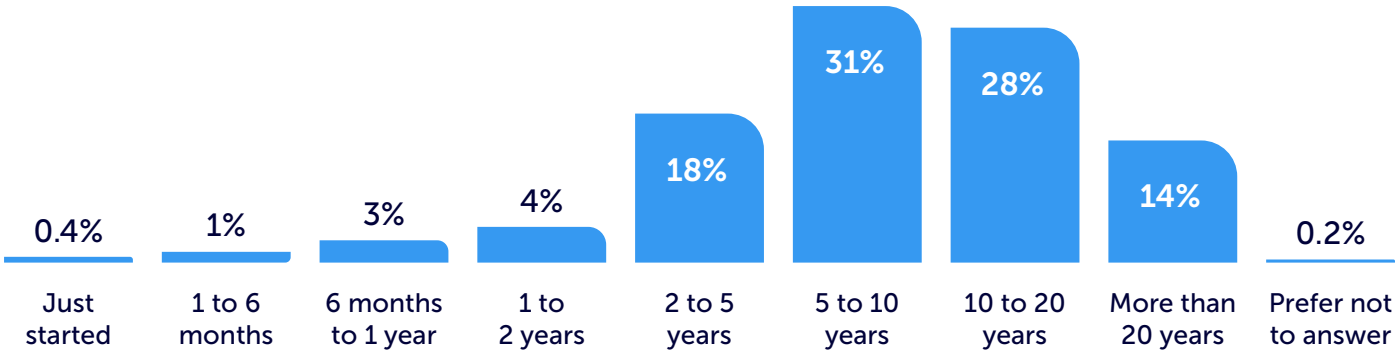
Demographics and Firmographics

Participants in the 2026 Global Privacy Benchmarks represent a broad cross-section of industries, company sizes, and roles across the enterprise. Respondents include privacy executives, members of dedicated privacy teams, senior executives outside the privacy function, managers, and full-time employees. This diversity ensures the findings reflect both leadership and operational perspectives on how privacy programs are managed in practice.

More than half of respondents represent organizations with over $1 billion in annual revenue, including a significant share from companies exceeding $5 billion. The strong representation of large enterprises reflects the reality that many of the most complex privacy programs operate within global organizations that manage significant volumes of personal data and face cross-border regulatory obligations.

The respondent base also reflects deep organizational experience. More than four in ten participants have worked at their company for over ten years, indicating that the insights captured in the survey are grounded in long-term institutional knowledge and direct involvement in the evolution of corporate privacy programs.

How long have you worked for your current company?



To maintain comparability with prior years and ensure balanced representation across enterprise perspectives, responses were weighted by both organizational revenue and professional role. The study includes input from senior executives, managers, full-time employees outside the privacy function, and members of dedicated privacy teams, ensuring that the results reflect enterprise-wide views rather than the perspective of privacy specialists alone. The TrustArc Global Privacy Benchmarks provide a 360° view into organizations' approach to privacy management around the world.

About Golfdale Consulting

Golfdale Consulting Inc., trusted advisors to growth-focused business leaders. Golfdale expertise spans three critical areas: global market research and insights, analytics strategies and application of decision sciences, and advocacy for evidence-based regulatory reform and market impact.

About TrustArc

TrustArc is redefining privacy for the AI era. With 28+ years of global privacy expertise and assurance services, we deliver the only platform that blends regulatory intelligence, automation, and AI to orchestrate end-to-end data privacy and governance. From automated DSR fulfillment to AI risk assessments and real-time compliance reporting, TrustArc helps organizations embed trust at every touchpoint. Headquartered in the San Francisco Bay Area with a global footprint, our privacy-first approach powers responsible innovation while reducing risk, ensuring our customers lead with confidence in a rapidly evolving regulatory landscape. Discover how at TrustArc.com.

TrustArc