

The Privacy Pulse 

**2025**

# Global Privacy Benchmarks Report

TrustArc

# Table of Contents

<b>Executive Summary: Top 5 Insights from 2025</b>	<b>03</b>
--	-----------

<b>A Global View: Survey Scope and Reach</b>	<b>05</b>
--	-----------

Demographics and Firmographics	06
--------------------------------	----

<b>Analysis and Insights</b>	<b>07</b>
------------------------------	-----------

How Privacy Teams Are Built (and Growing)	07
---	----

Privacy Challenges, Concerns, and Benefits	09
--	----

The 7 Keys to Privacy Competency in 2025	12
--	----

The TrustArc Global Privacy Index	15
-----------------------------------	----

AI Approaches and Challenges	17
------------------------------	----

Privacy Solutions	24
-------------------	----

Privacy Management Measurement	28
--------------------------------	----

Regulatory Compliance Approach	32
--------------------------------	----

<b>The Bottom Line</b>	<b>33</b>
------------------------	-----------

About TrustArc	33
----------------	----

About Golfdale Consulting	33
---------------------------	----



# Executive Summary:

## Top 5 Insights from 2025

### 1 AI is Privacy's Pressure Cooker: Yet Prepared Organizations Surge 16 Points Ahead

Artificial Intelligence is reshaping the privacy landscape and intensifying the stakes. It remains the top-ranked challenge in privacy management, with 46% rating it as very or extremely challenging, and 28% reporting vulnerabilities related to AI. The dominant struggle? Ensuring AI systems comply with privacy requirements, something 43% find difficult amid vague and shifting regulations.

The urgency is escalating. There are already enforcements happening such as on May 12, 2025, the Federal Trade Commission (FTC) issued a proposed order requiring Workado to stop advertising the accuracy of its AI detection products unless it maintains competent and reliable evidence showing those products are as accurate as claimed. The order will remain in effect for 20 years and will be enforced by the FTC through ongoing monitoring and compliance checks.

Amid the uncertainty, proactive organizations are preparing now. 61% say they feel prepared or very prepared for the EU's AI Act and 57% for the Colorado AI Act. This AI-ready segment isn't just compliant; it's outperforming. On average, it scores 16 points above the 2025 TrustArc Global Privacy Index Grand Mean.

What's driving their edge? Five stand out as defining traits across nine privacy implementations: data inventory and mapping, third-party privacy certifications, data discovery, building and maintaining a Trust Center, and data subject rights request management. These are the new foundations of AI-era privacy leadership.

### 2 A Winning Privacy Blueprint Emerges: Centralized Teams, Principles, Metrics, and Purpose-Built Tools

The privacy elite aren't lucky — they're methodical. A distinct performance formula separates high achievers from laggards on the Privacy Index.

Simply having a privacy team is now the baseline. Companies without one post failing scores (39%). However, its structure sets leaders apart: 39% use centralized privacy teams, which outperform both hub-and-spoke (34%) and decentralized (26%) models, scoring five points above the overall average.

Equally critical is the mindset. Leaders are embracing a principles-based approach to regulation, growing from 18% in 2024 to 22% in 2025 and achieving top-tier competence scores of 73%, well above the Grand Mean of 61%.

They also align with global standards like [Nymity Privacy Management Accountability Framework \(PMAF\)](#), AICPA/CICA, COBIT, and [APEC CBPR & PRP](#). These frameworks — celebrated for their structured accountability and global credibility — correlate with a 75% privacy competence score.

But the biggest divider? Measurement. A striking 82% of medium and large companies actively measure privacy programs, and their average score soars to 74%. In contrast, those who don't measure average a failing 35%. Privacy audit assessments are the most popular of nine methods, and completed internal assessments top the list of 11 KPIs.

Lastly, leaders lean into automation. Off-the-shelf privacy management software drives the highest Privacy Index performance (71%), with Trust Center-specific purchases pushing that figure to 78%. This is the new privacy tech stack for results.

### 3 Privacy Grows Up: Small Companies Triple Their Privacy Offices as Hiring Momentum Builds

The era of optional privacy is over, even for the smallest players. A privacy wave is sweeping through organizations of all sizes, and the acceleration is striking.

Nine in ten medium and large companies already have Privacy Offices — a figure unchanged from last year. But among companies under \$50M, adoption surged from 31% in 2024 to 87% in 2025. That's nearly a threefold leap in just one year.

Hiring momentum reinforces this growth. Only 3% of companies are scaling back privacy roles. In contrast, 50% anticipate growing demand, and 54% agree or strongly agree that "when it comes to privacy, we should be doing more."

With regulations expanding and risks intensifying, even smaller organizations now view privacy as a strategic, long-term investment, not a regulatory afterthought. The talent race is officially on.

### 4 Tools of the Trade: Vendor Management and Trust Centers Drive the Strongest Privacy Performance

Purpose-built privacy tech is no longer a luxury. It's the performance engine behind leading programs. The tools organizations prioritize are directly correlated with Privacy Index success.

Companies focusing on vendor management, privacy assessments, Trust Centers, and privacy-dedicated software report scores 10 – 18 points higher than peers. Vendor risk, in particular, is emerging as a top motivator: 38% cite Vendor Management & Assessments as a privacy challenge, and they're responding by scaling implementation.

The payoff is clear. Organizations with seven privacy initiatives in place report an average privacy competence score of 73%, compared to just 44% among those with only one.

That sense of urgency is spurring new investments. Among companies without current commercial privacy solutions, 77% plan to purchase tools for data risk visibility, and 72% are building or planning Trust Centers. Privacy maturity now hinges on tool adoption, not intention alone.

### 5 Trust is King — But Most Haven't Followed Through

Brand trust reigns supreme. In 2025, a staggering 88% of companies cite it as a top motivator for privacy investments, reaffirming its enduring strategic value.

But there's a trust gap. Just over one-third (36%) of companies have fully implemented more than three privacy solutions, yet data shows that full implementation drives exceptional results. Organizations with robust implementations report an average Privacy Index score of 82%.

Despite this, only 22% have purchased a comprehensive data privacy management platform. Even among those who rate brand trust as critical, the figure inches up to just 24%.

What moves the needle more than motivation? Experience. Among companies that have suffered a data breach in the past three years, 30% have already invested in an overall platform, and another 40% are very likely to do so. Fear, not aspiration, is currently the stronger catalyst.

The challenge for leadership in 2025: turn intention into infrastructure before a crisis forces the hand.

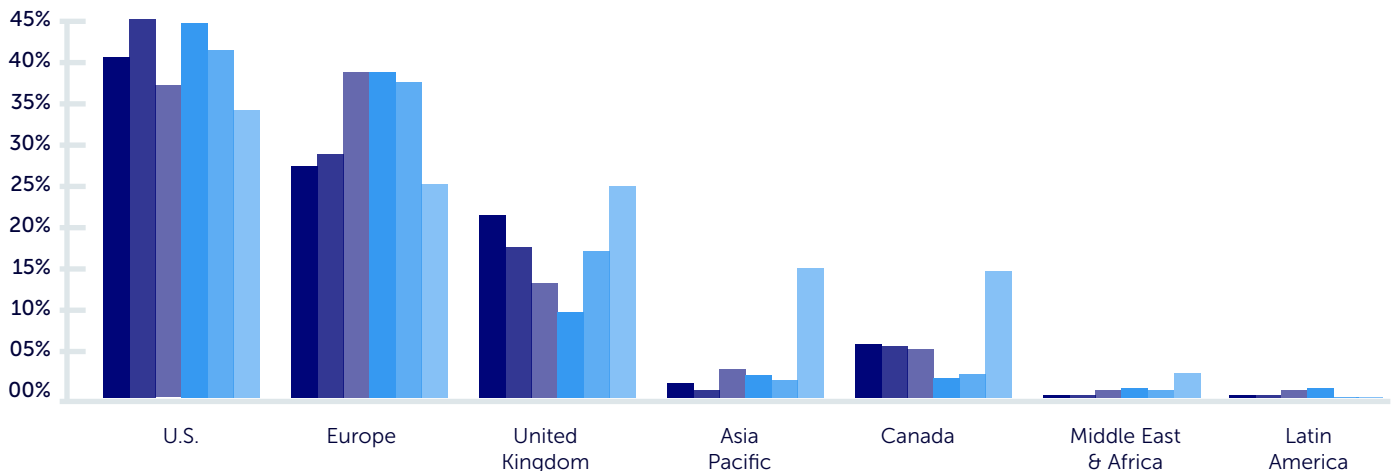
# A Global View: Survey Scope and Reach

This year's Global Privacy Benchmarks reflect the views of 1,775 professionals, including privacy team members and executives, across the U.S., Europe, the UK, Canada, Latin America, Asia-Pacific, the Middle East, and Africa. With weighting across company size, role, and geography, our 6th annual report since its inception in 2020 offers a comprehensive 360° view. This work was commissioned by TrustArc and conducted by Golfdale Consulting.

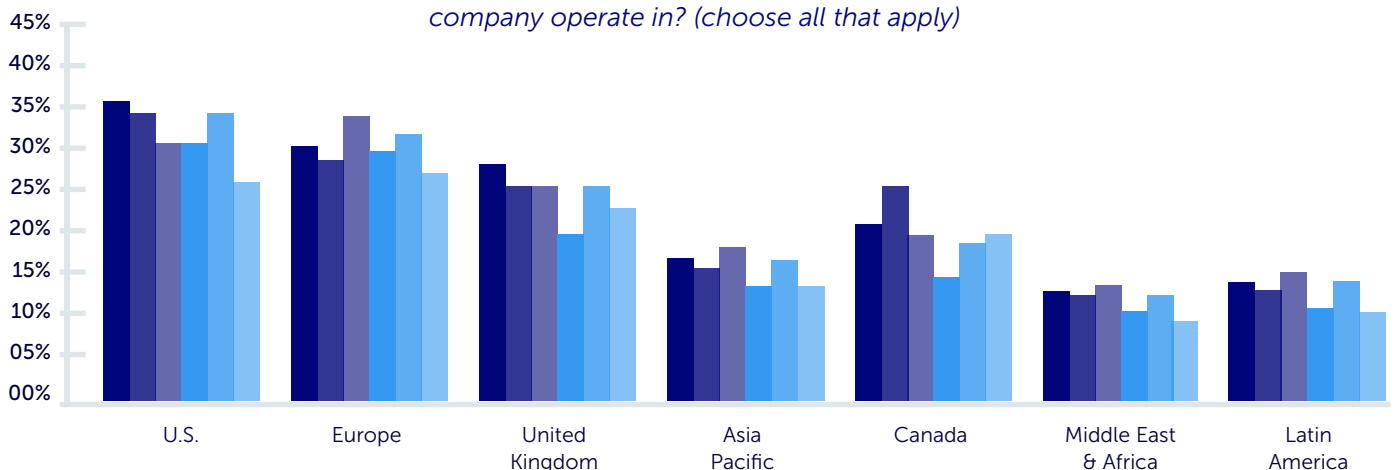
## Head Office and Operating Regions

● 2025 ● 2024 ● 2023 ● 2022 ● 2021 ● 2020

*Where is your Head Office located?*



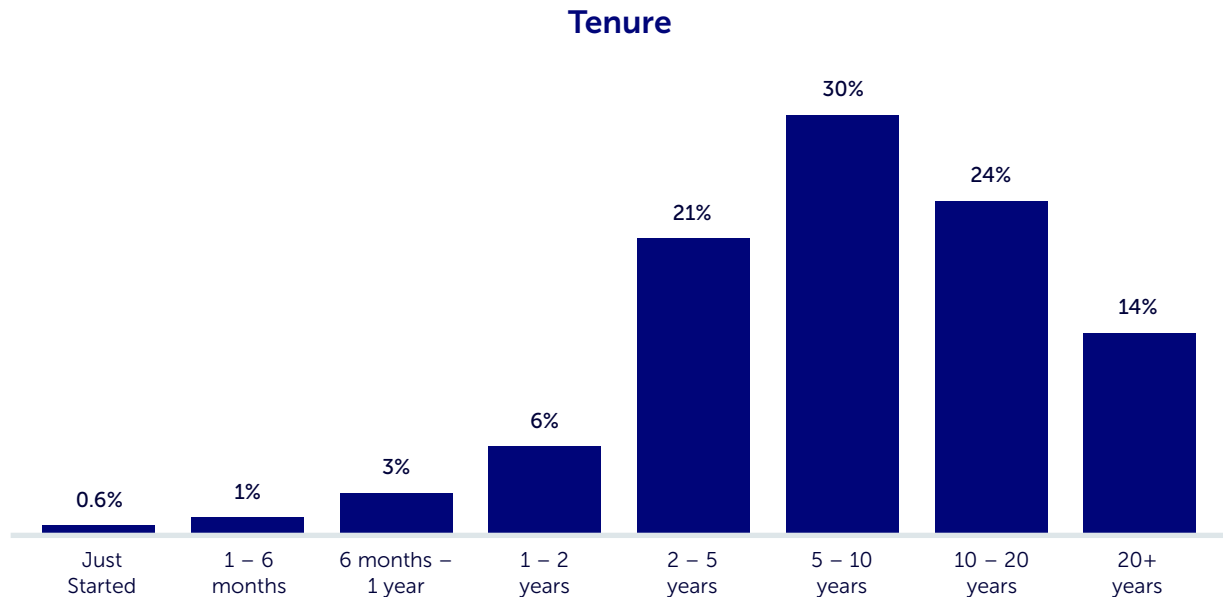
*Which of the following regions and countries does your company operate in? (choose all that apply)*



# Demographics and Firmographics

Participants represented every major industry, with tech, finance, manufacturing, and retail leading the pack. Roles included privacy executives, FTEs, general management, and others. Nearly 40% of respondents have over a decade of company tenure, reinforcing their deep operational insights.

To ensure representative equivalencies when comparing year-over-year data, results were systematically weighted across five primary roles: outside the privacy function, we surveyed executives, managers, and non-managerial full-time employees; inside the privacy function, we surveyed privacy executives and privacy team members. In our weighting schema, senior executives, managers, FTEs, are balanced with privacy team members and privacy executives equally for a comprehensive 360° view. Additionally, responses were weighted by organizational revenue to align with prior survey years.



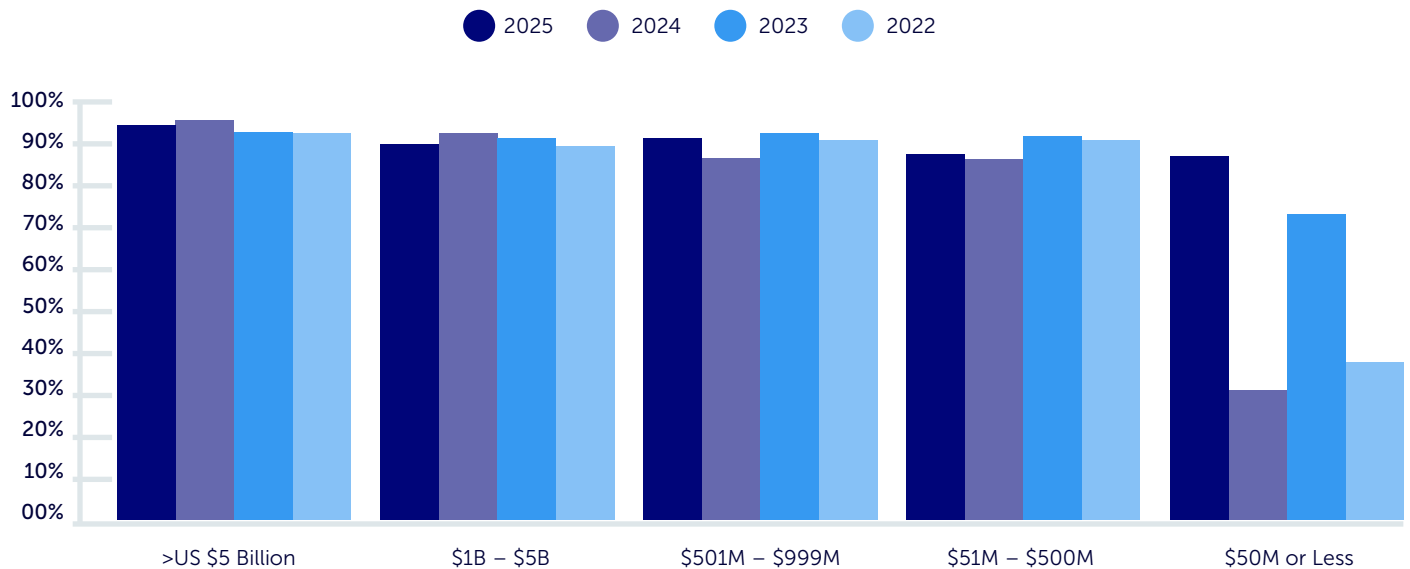
# Analysis and Insights

## How Privacy Teams Are Built (and Growing)

It's official: the vast majority of medium- and large-sized companies have dedicated privacy teams and personnel consistent with our previous year's findings. In 2025, there is massive growth among small-sized organizations, especially those with revenues under \$50 million.

### Privacy Team Composition

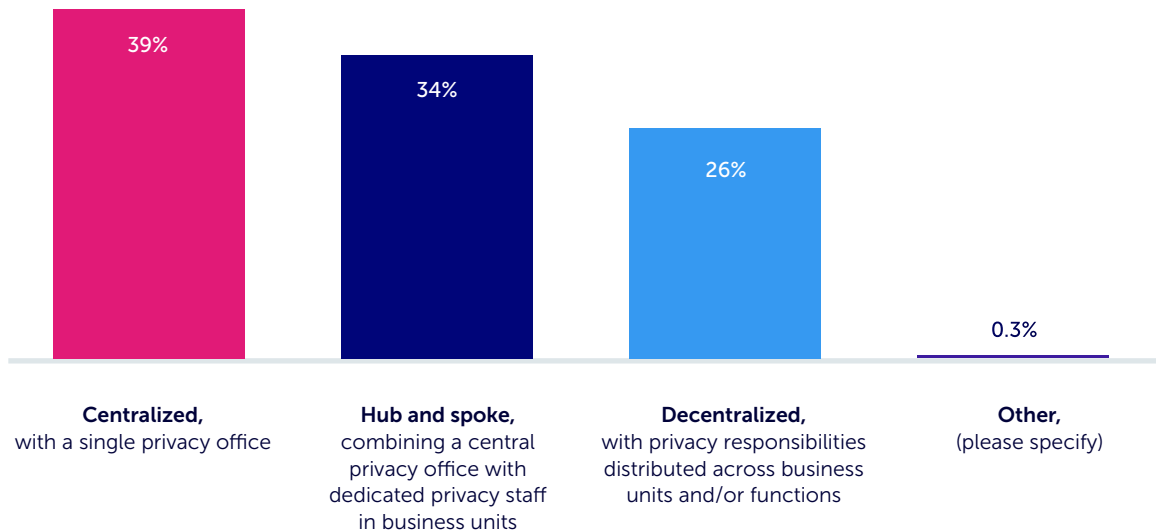
*Does your company have a dedicated Privacy Office and/or a Privacy Team that provides oversight on privacy issues at your company?*



More teams are choosing a centralized structure versus a “hub and spoke” or a decentralized approach. Centralized structures remain the most effective, with 39% adoption and top Privacy Index scores.

## Privacy Team Composition

*What organizational structure does your privacy program follow?  
(asked only of those with a dedicated Privacy Team)*



Expectations for privacy roles indicate sustained growth overall. Half (50%) of privacy executives and privacy team members anticipate increasing demand for their expertise, versus 48% indicating it will remain unchanged, and only 2% viewing the demand for their roles as diminishing over the next year.

This underscores the sustained and growing commitment to privacy across various sectors and regions, setting the stage for continued investment and evolution in privacy management practices globally.

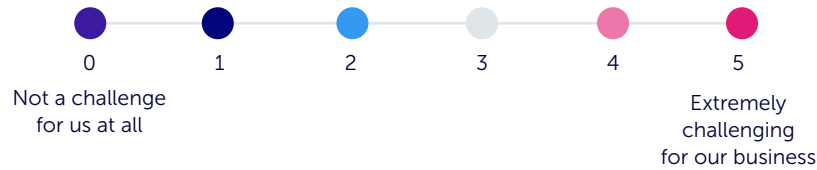


# Privacy Challenges, Concerns, and Benefits

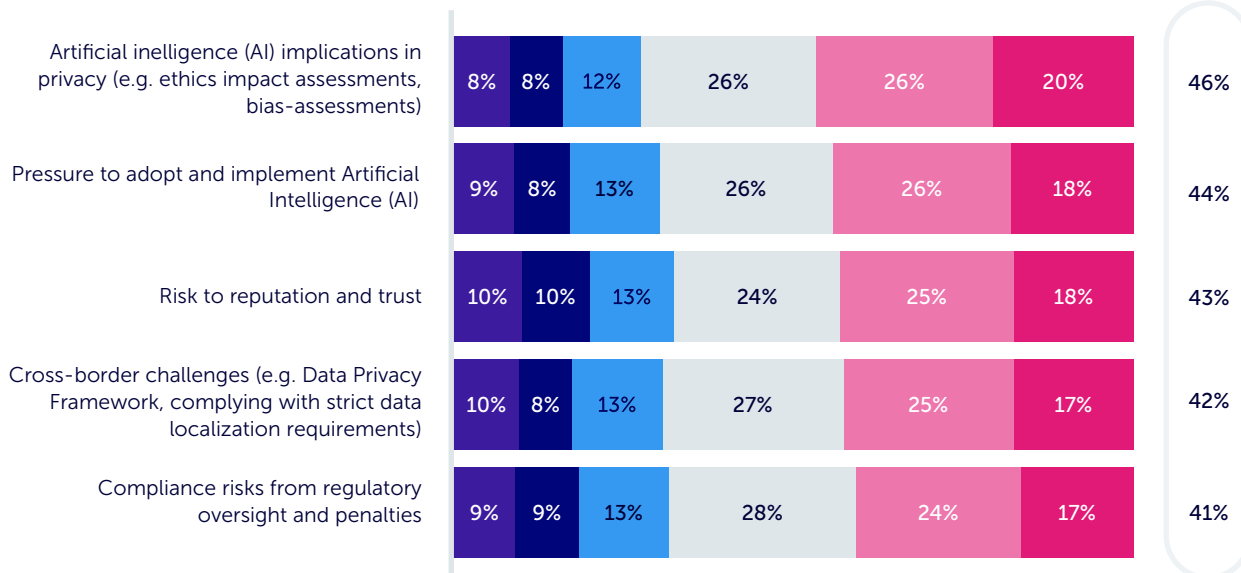
The #1 privacy challenge in 2025 is Artificial Intelligence (AI). AI is consistently rated as the top challenge from last year's findings that most enterprises face. AI-related privacy risks, compliance confusion, and real-world legal threats are continuing to make waves. Other top challenges include reputational risk, cross-border challenges, and compliance risks.

## 2025 Top 5 Challenges

*Of the following challenges that many enterprises face, please rate each of them as they relate to privacy risks that your company is likely to encounter in 2025?*



Percent 4s & 5s



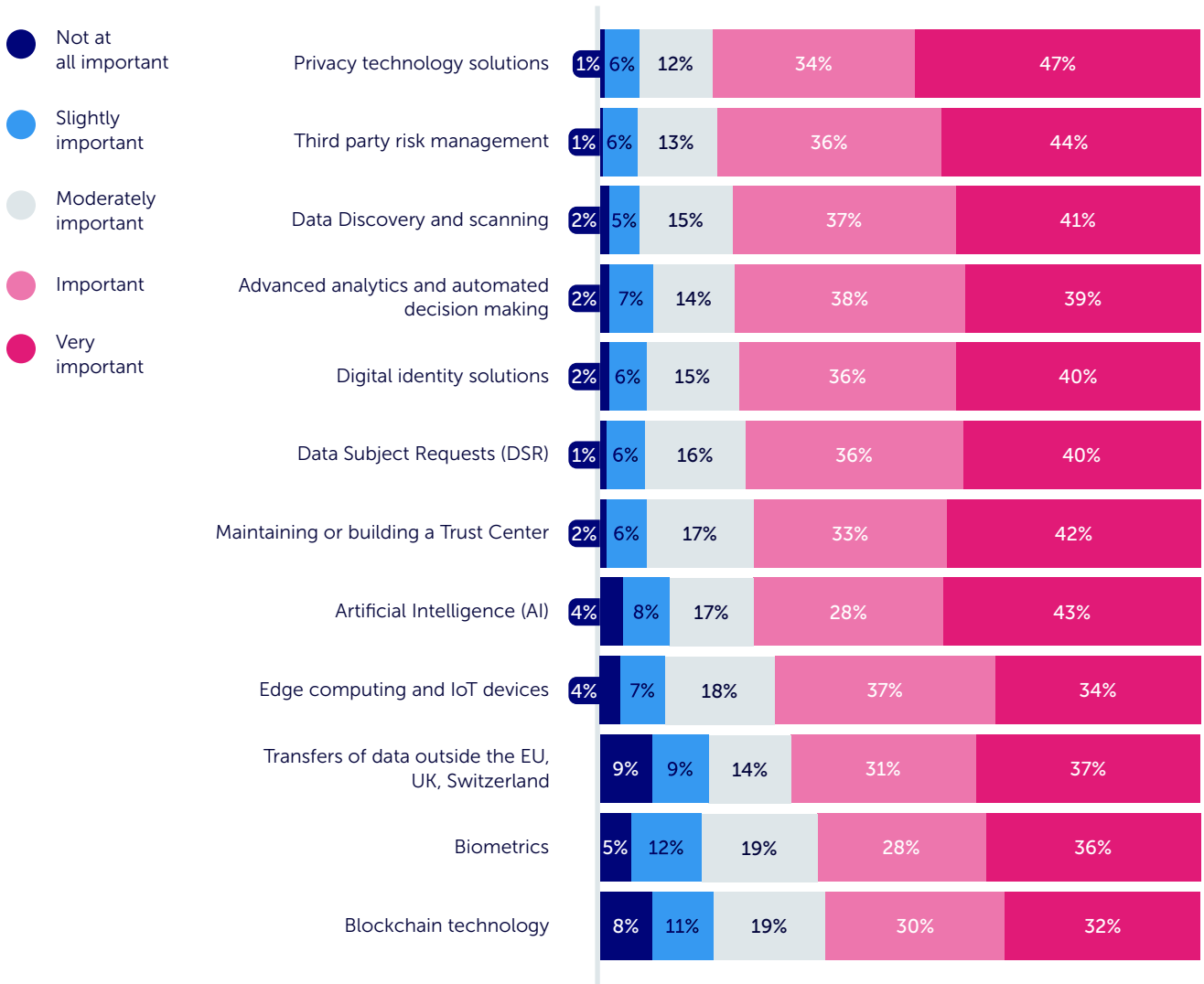
Privacy vulnerabilities continue to evolve, with the survey revealing widespread occurrences of incidents. Over the past three years, a significant number of organizations reported experiencing breaches and vulnerabilities, indicating persistent threats despite increased security measures. Following closely are reputational risks associated with privacy incidents, particularly those amplified through social media channels. The frequency and complexity of cybersecurity threats have kept these issues at the forefront of organizational concerns, underscoring the need for robust security measures.

Across both data breaches and large-scale cyberattacks, privacy teams are more acutely aware than others within enterprises. There is roughly an equal understanding of the potential negative consequences of AI adoption, and slightly elevated views on other privacy vulnerabilities among non-privacy function professionals.

In light of data and cyber risks, it is not surprising to learn that privacy technology solutions top the list of importance in terms of privacy concerns and regulations. Coming second in importance, third-party risk management continues to be a critical area of concern due to businesses' growing reliance on data mining done by external partners. Managing risks associated with these external entities has become increasingly essential as data handling expands beyond organizational boundaries. As the Internet of Things continues to expand, data discovery and scanning are essential for managing and safeguarding the increasing amounts of sensitive information for data security. At the same time, organizations increasingly embrace advanced analytics and automated decision-making processes.

## Privacy Concerns

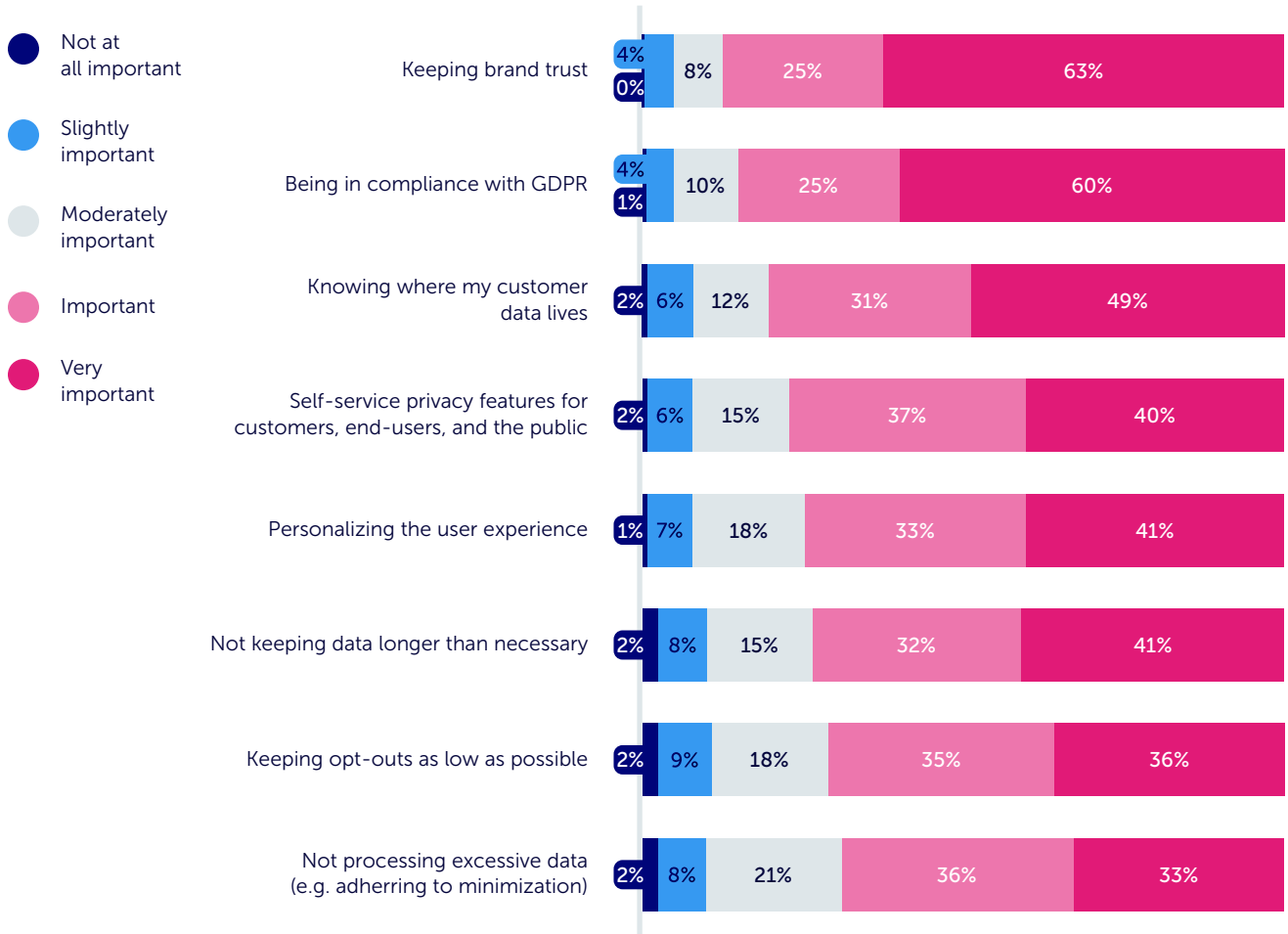
*How important are the following topics to your company as they relate to privacy concerns and regulations?*



The survey highlighted that maintaining brand trust remains the top benefit of robust privacy management, recognized as essential by most organizations. Regulatory compliance closely follows, reflecting the strategic importance of adherence to evolving privacy laws and standards.

## Privacy Benefits

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



The finding on privacy management being a critical opportunity to build brand trust is consistent and stable with our findings over the past three years.

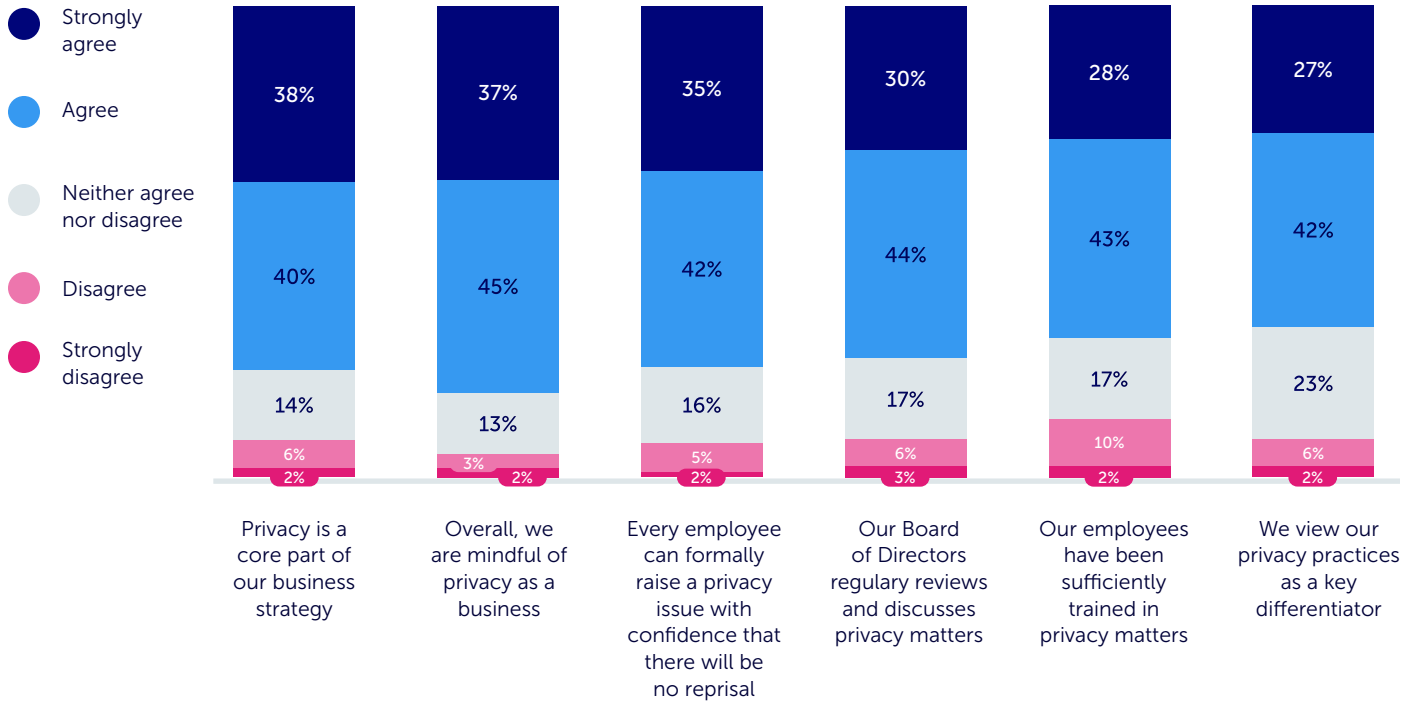
# The 7 Keys to Privacy Competency in 2025

The 2025 survey reaffirmed seven essential competencies that underpin privacy effectiveness and confidence:

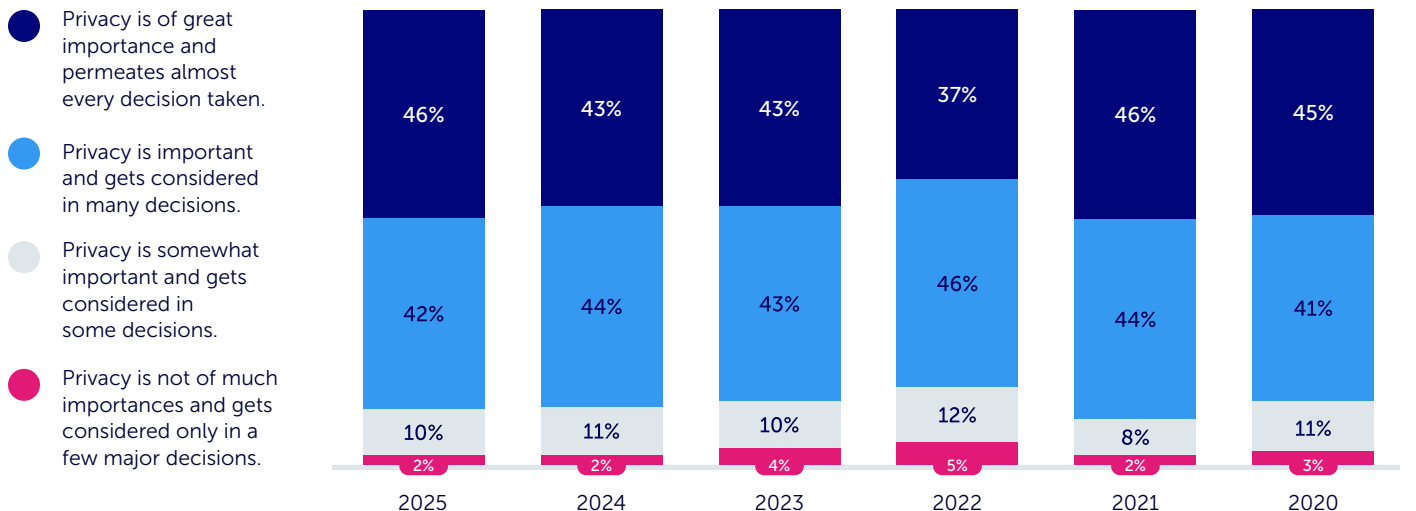
- 1 STRATEGIC INTEGRATION:**  
Over three-quarters (78%) of respondents view privacy as a core element of business strategy, embedding privacy considerations into strategic planning and decision-making processes.
- 2 PRIVACY MINDFULNESS:**  
Continuous mindfulness about privacy practices remains prevalent, with many organizations adopting proactive and preventive privacy measures.
- 3 EMPLOYEE EMPOWERMENT:**  
Organizations increasingly empower employees to raise privacy concerns confidently, without fear of reprisal, fostering a culture of openness and accountability.
- 4 BOARD-LEVEL ENGAGEMENT:**  
Regular board review and discussion of privacy issues are increasingly prevalent, reflecting the growing importance of privacy at the highest level of an organization.
- 5 TRAINING AND AWARENESS:**  
Enhanced privacy training programs continue to expand, encompassing a broader range of organizational roles and responsibilities.
- 6 PRIVACY AS A DIFFERENTIATOR:**  
The trend of embracing privacy practices as a business differentiator continues, particularly in consumer-focused sectors and brands.
- 7 OPERATIONAL MINDFULNESS:**  
Companies report significant integration of privacy into daily business decisions, demonstrating enhanced operational consideration of privacy issues.

## Keys to Privacy

Please indicate whether you agree or disagree with each of the following statements.



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?

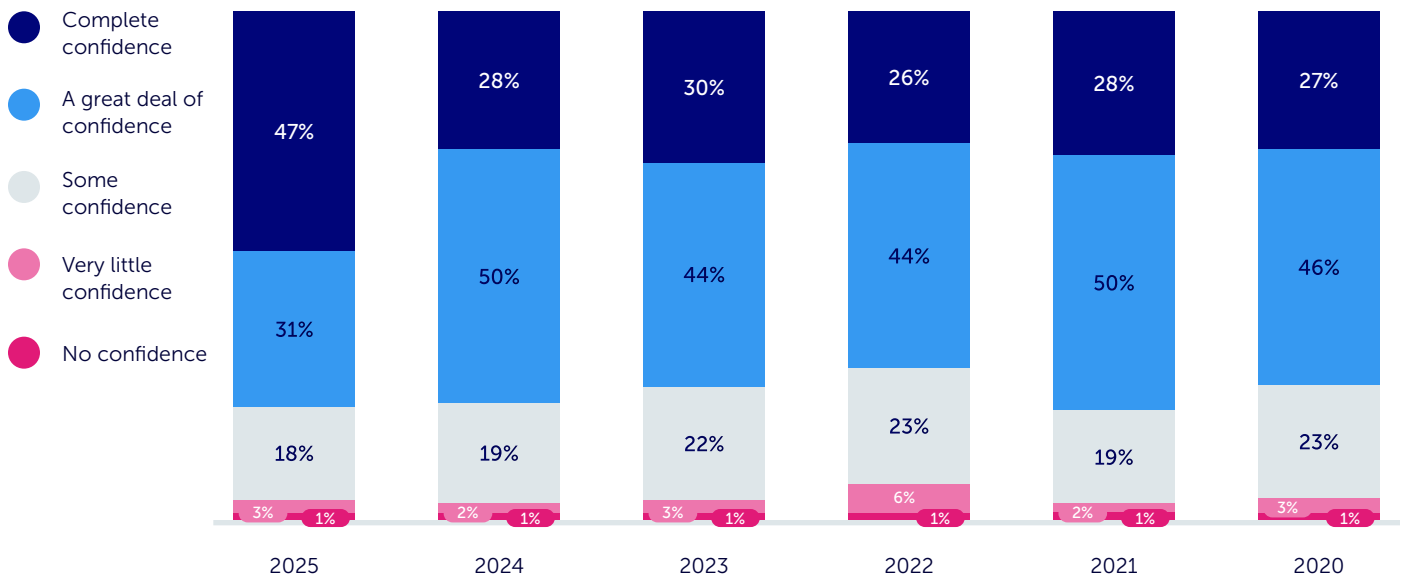




TrustArc also measures five confidence outcomes that matter to stakeholders. On the first of these measures, there was a substantial increase of 19 percentage points year over year among those who have complete confidence that employee and customer data is kept safe and protected.

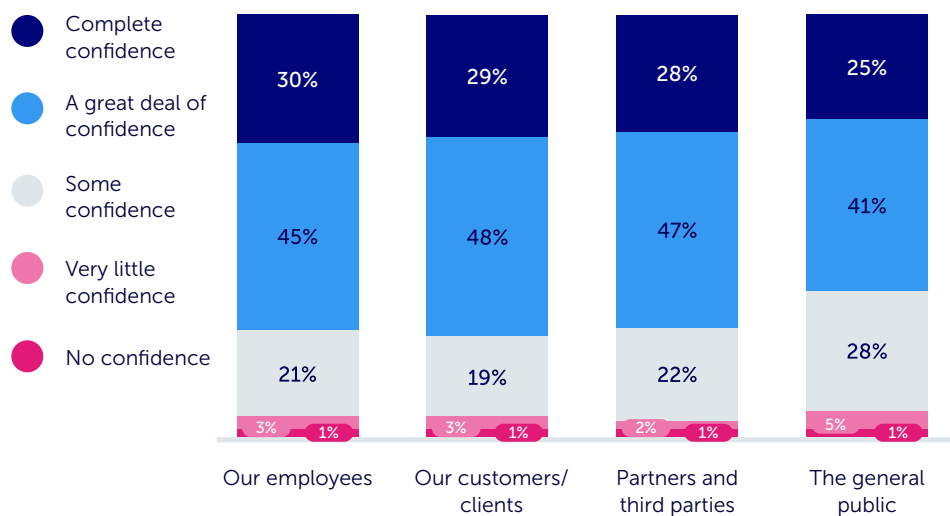
## Overall Confidence

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



Measured next was their confidence in their company's ability to manage data privacy for the four major stakeholder groups. These included Employee Confidence, which is marginally the best scoring stakeholder score, followed by Customer Confidence, Partner and Third-Party Confidence, and the General Public.

## Stakeholder Confidence



# The TrustArc Global Privacy Index

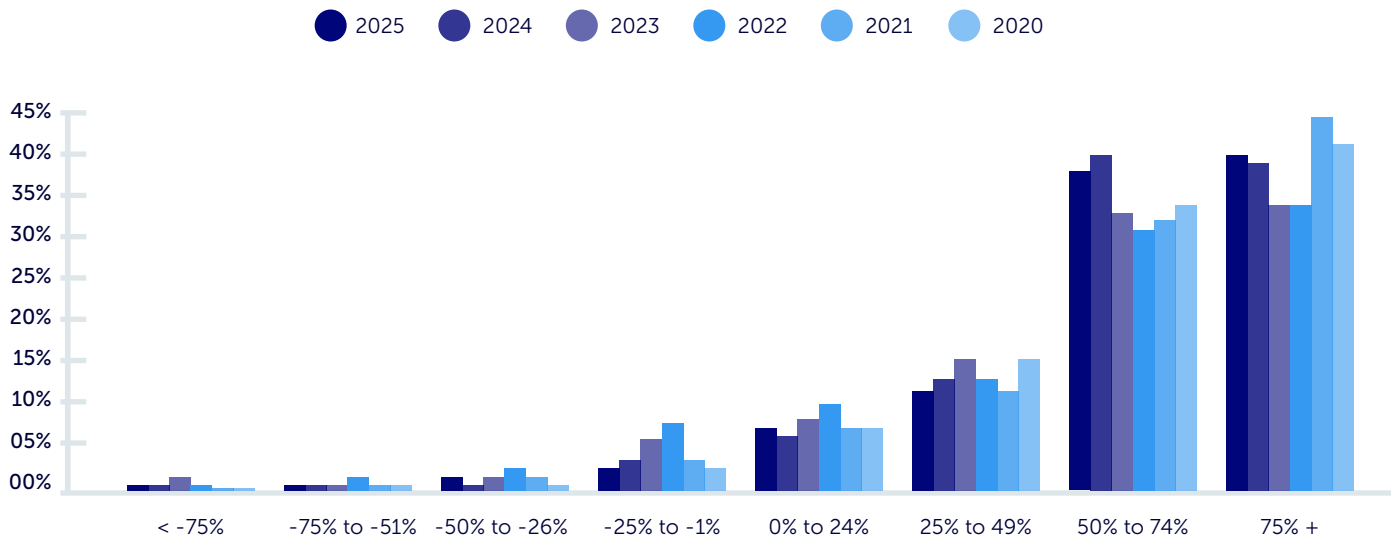
Imagine a Net Promoter Score — but for privacy. TrustArc's proprietary Global Privacy Index combines 12 key indicators (seven competencies and five outcomes) to assess an organization's privacy performance.

The scoring system results in an overall robust privacy metric. It is the result of extensive statistical modeling that was conducted in 2020 and revalidated in 2021. Scores range from -100 to +100, with deductions for low ratings.

Four stakeholder groups are equally weighted for a 360° view: execs, managers, FTEs, and privacy team members.

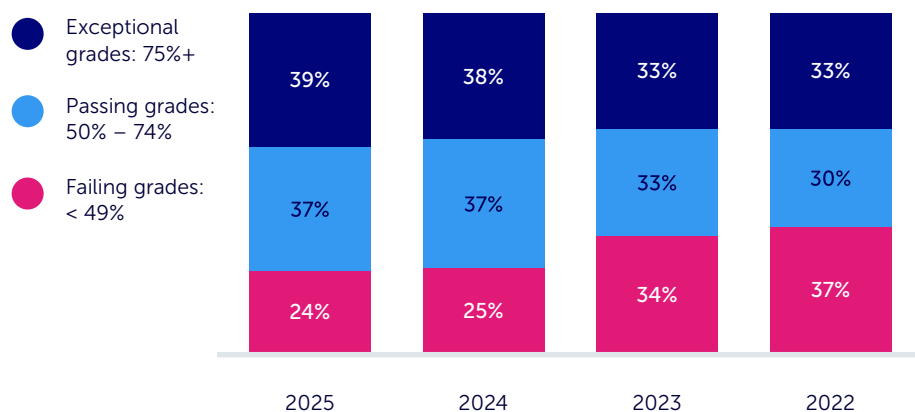
In 2025, the average Global Privacy Index score rose slightly to 61%.

## Keys to Privacy Index — Distribution YoY



Results varied widely: over a third of companies scored highly, a third received passing scores, and about a quarter failed. The increase was driven largely by gains in U.S. organizations.

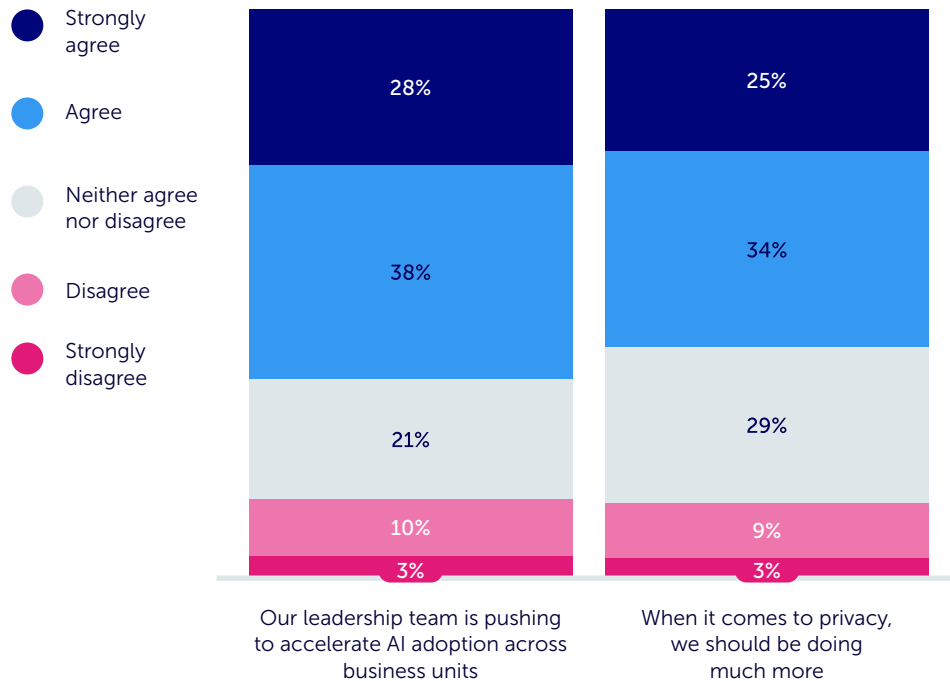
## Graded Distribution of Privacy Index YoY



High Index scores correlate with proactive leadership — 66% say leadership is pushing AI adoption, and 59% believe more should be done around privacy.

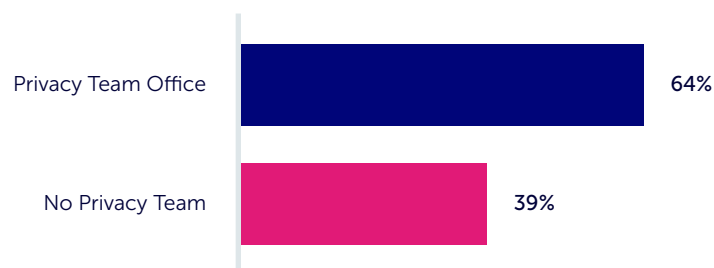
## Doing More

*Please indicate whether you agree or disagree with each of the following statements.*



The implications of having high Privacy Index scores are borne out across several measures. Building on previous results shown above, it is clear that having a privacy team is beneficial (three points above the Grand Mean average of 61%) and more "on point," while not having one is quite detrimental (22 points below average).

## Grand Mean of Privacy Index Scores for Privacy Team Offices

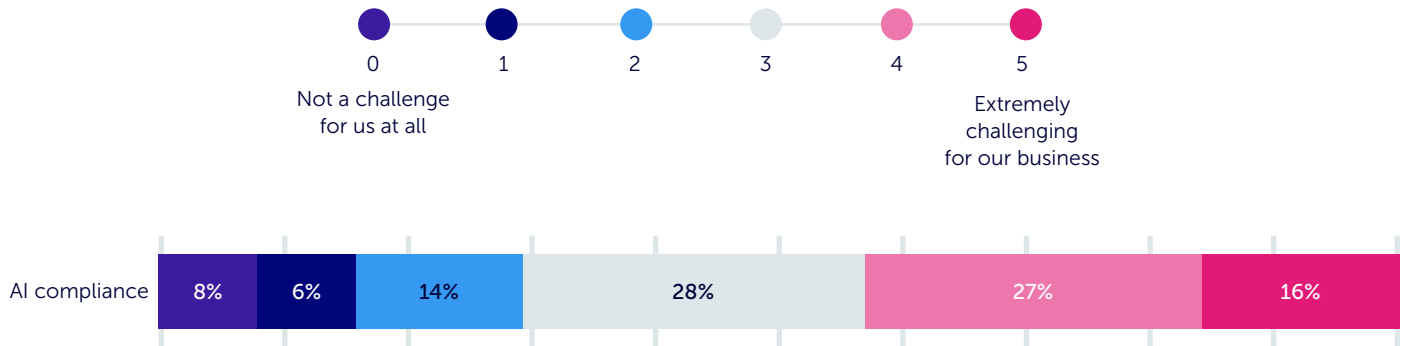


# AI Approaches and Challenges

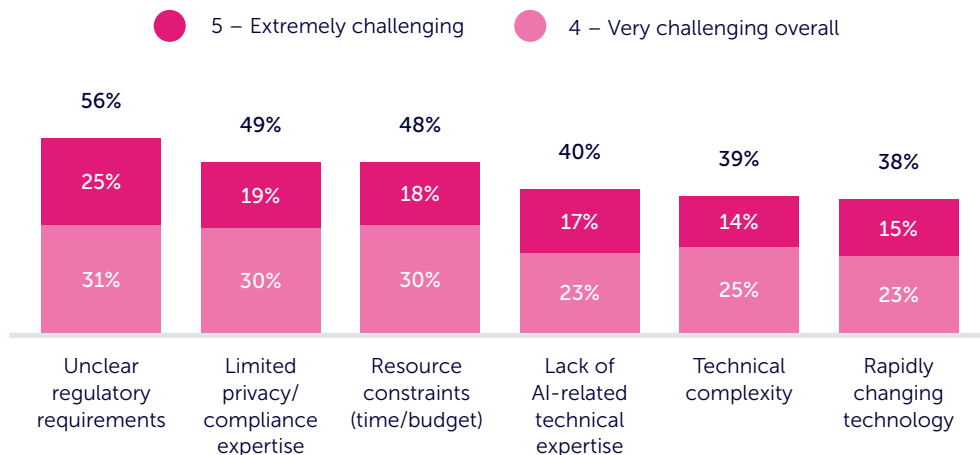
In 2025, 57% of organizations used AI for privacy tasks, while 56% implemented AI governance programs. Yet, AI compliance remains difficult due to unclear regulations, limited expertise, and resource constraints.

## AI Challenges

*How challenging is it for your organization to ensure AI systems comply with privacy requirements?*



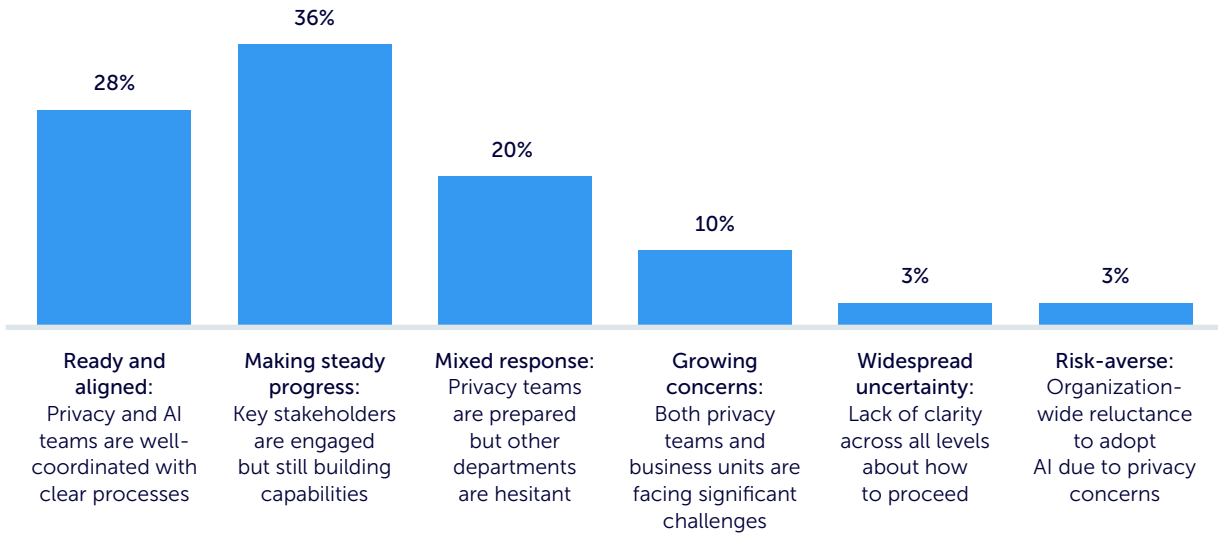
*What is challenging about ensuring that your AI systems comply with privacy requirements?  
(asked of those who scored "4-very" or "5-extremely" above)*



About 64% of companies are either aligned or making progress toward AI process alignment across stakeholders.

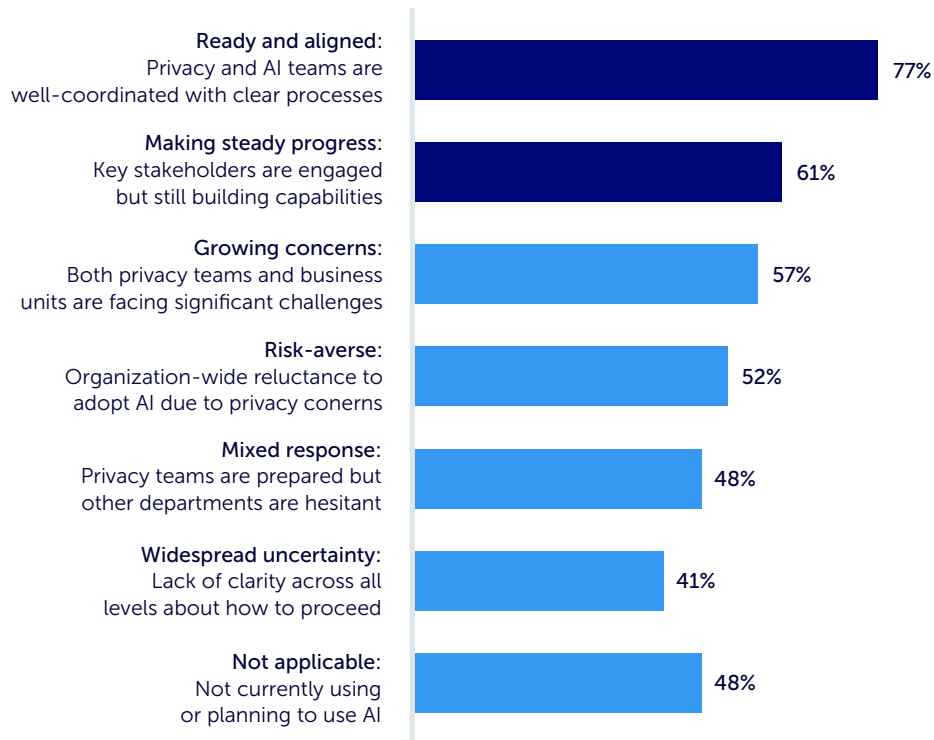
## Managing AI

Which statement best describes your organization's overall sentiment towards managing AI and privacy challenges?



The need to be **ready and aligned** is underscored by comparing companies in this category to all others on our privacy competence metric, the Grand Mean of the Privacy Index. Those making *steady progress* on AI perform at an average level on this metric. Those with strong alignment score 16 points above average on the Privacy Index.

## Privacy Competence by AI Readiness

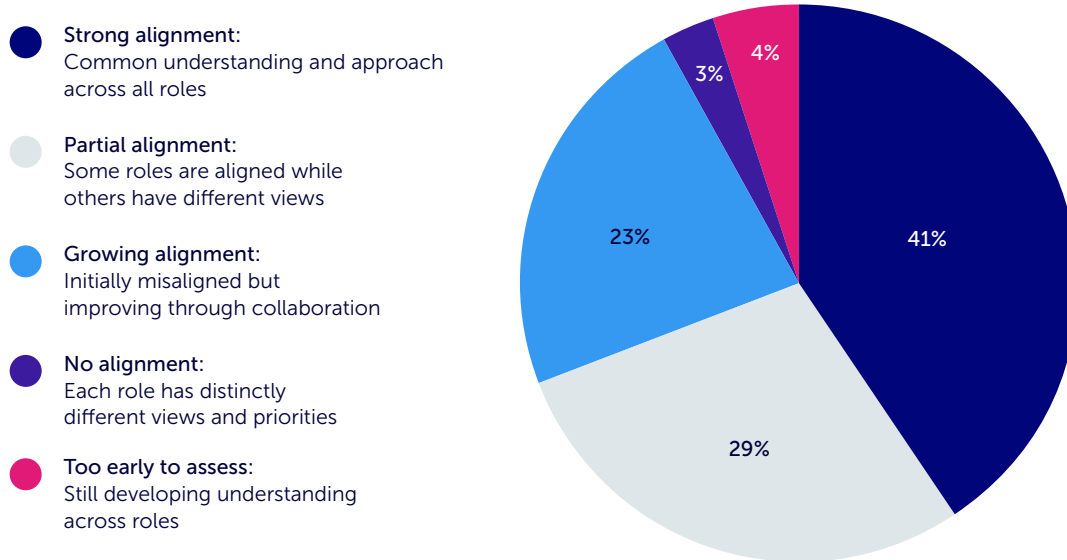


Misalignment is common, with 31% lacking shared understanding or direction.



## Role Alignment

*How aligned are different roles in your organization  
(privacy professionals, business leaders, and technical teams)  
in their understanding of AI privacy risks?*

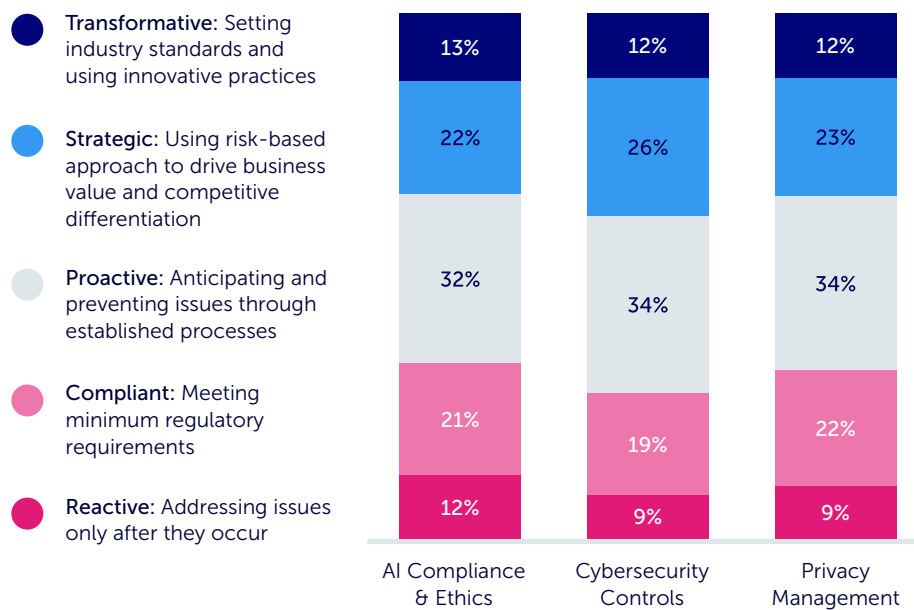


Again, we found that those with *strong alignment* achieved privacy competence scores of 77% versus those working on improvement and *growing their alignment* scoring worse than average (54% versus the Grand Mean of 61%).

The 2025 survey results reveal clear distinctions in organizational maturity across three core domains: AI Compliance & Ethics, Cybersecurity Controls, and Privacy Management. While just over one in ten see themselves as “transformative” in these areas, a further quarter or so view themselves as being strategic, leveraging a risk-based approach to drive business value and competitive differentiation. As we saw on the alignment issue prior, roughly the same percentages (34%, 28%, and 32% respectively) can be found at the opposite end of the spectrum, seeing themselves as reactive or compliant.

## Organizational Maturity

*How would you characterize your organization’s maturity in each of these areas?*

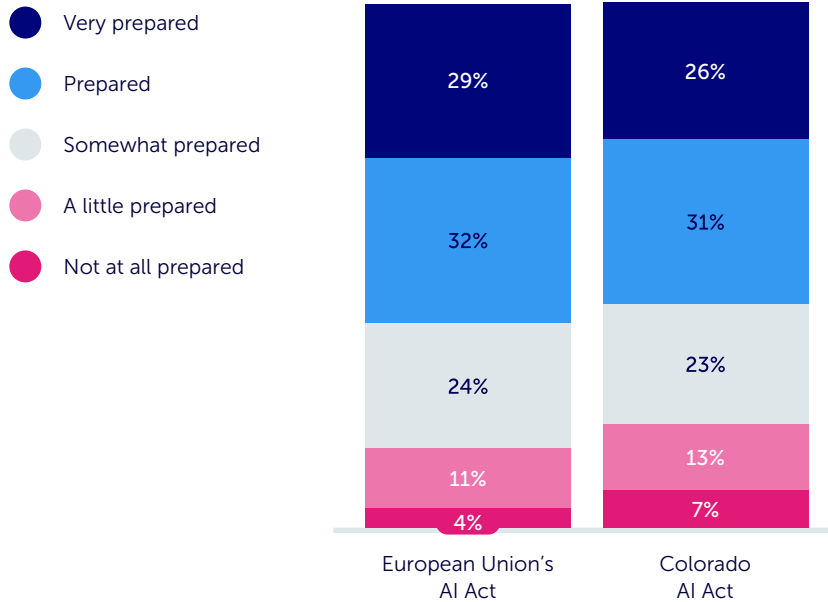


Maturity levels vary. Only 11% call themselves transformative, while most are strategic or emerging. Those prepared for AI regulations, like the EU AI Act and the Colorado AI Act, show stronger privacy competence, especially when supported by tools like data inventory, certifications, and breach protocols.

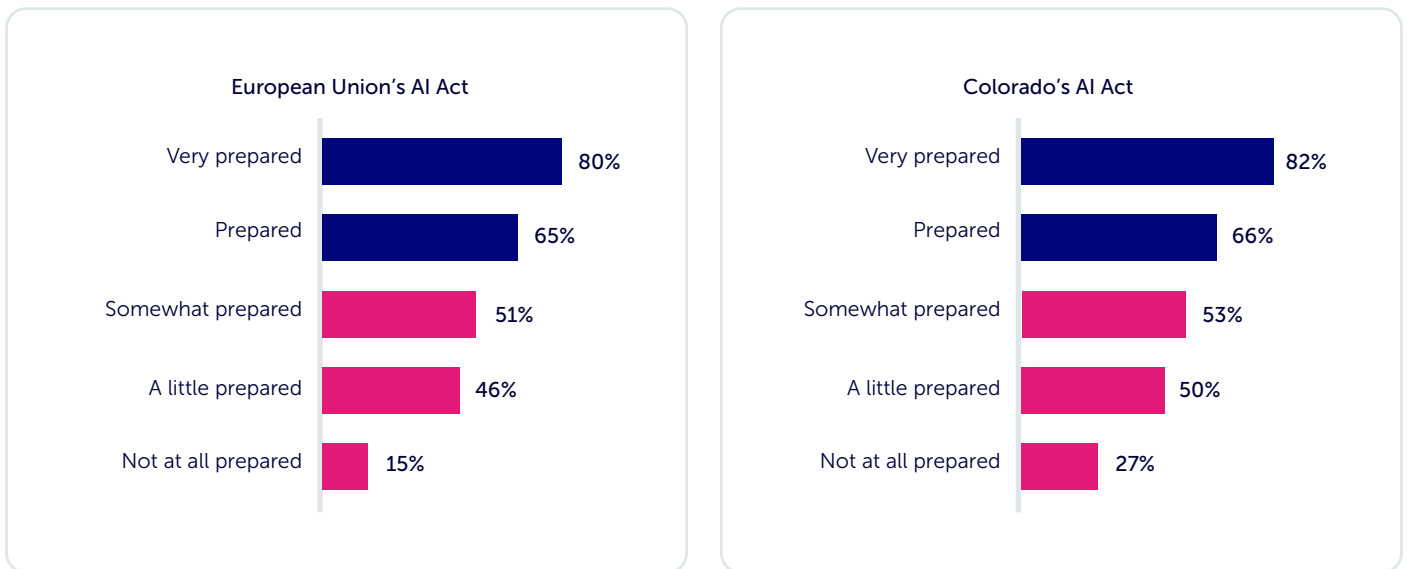
Companies that demonstrated high preparedness for AI regulations also reported much higher privacy competence, underscoring the strategic value of proactive AI compliance measures.

## AI Regulation Readiness

*How prepared do you feel your company is for enforcement of the following new AI regulations as they pertain to privacy requirements. If the particular regulations do not apply to your business, please choose "Does not apply".*

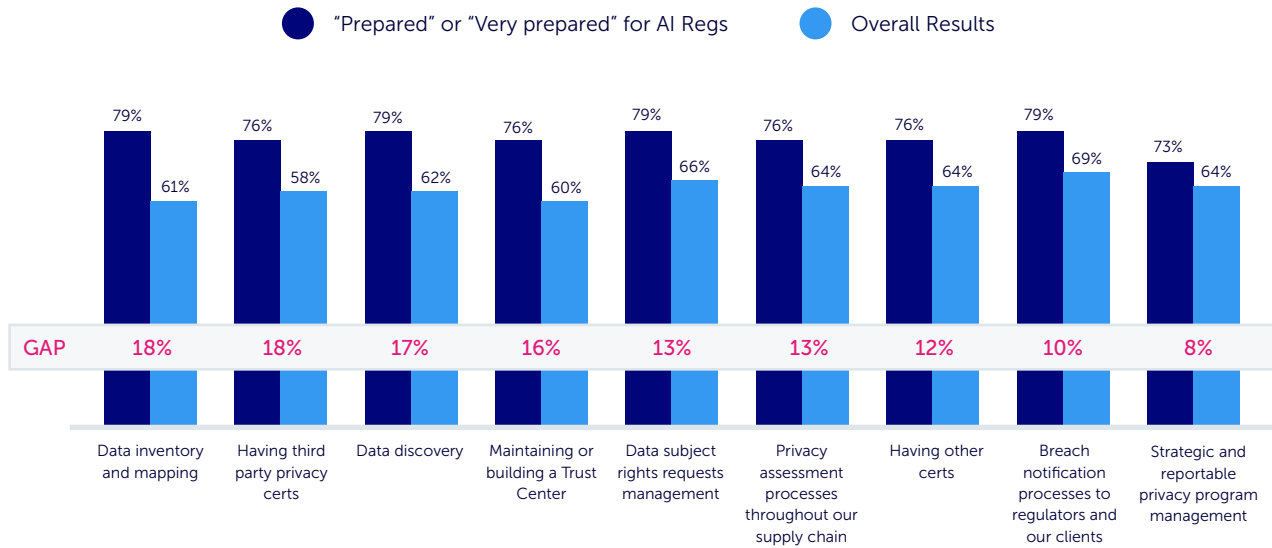


## AI Regulatory Readiness and Privacy Competence



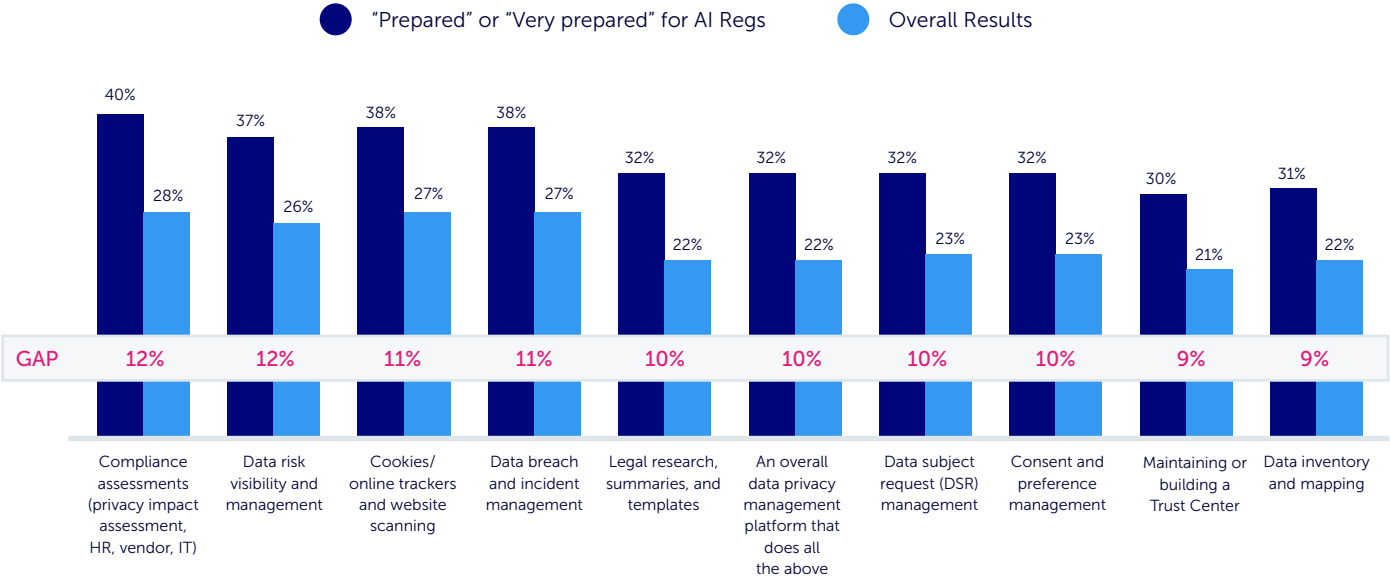
Analysis of the relationship between AI regulation preparedness across key privacy implementations and commercial privacy purchases is also revealing. Organizations that are “prepared” or “very prepared” for these AI regulations show a substantially higher likelihood of having implemented critical privacy processes like data inventory, third-party privacy certifications, and breach notification protocols.

### AI Regulation Preparedness Implications and Privacy Implementations



Adoption gaps persist. The overall adoption of these privacy solutions remains lower than needed for AI compliance to be fully realized. Organizations not investing in robust solutions face challenges bridging the gap to full compliance.

## AI Regulation Preparedness Implications and Commercial Solutions



### AI READINESS REFLECTS PRIVACY MATURITY

Organizations prepared for AI regulation, such as the EU AI Act and Colorado AI Act, consistently scored higher across privacy implementations and competence. Those aligned across business, tech, and privacy teams? They led the pack, scoring 77% on the Index vs 54% for everyone else. Those who have their core privacy culture excelling and are proactive in preparing for the regulatory landscape lead the pack.

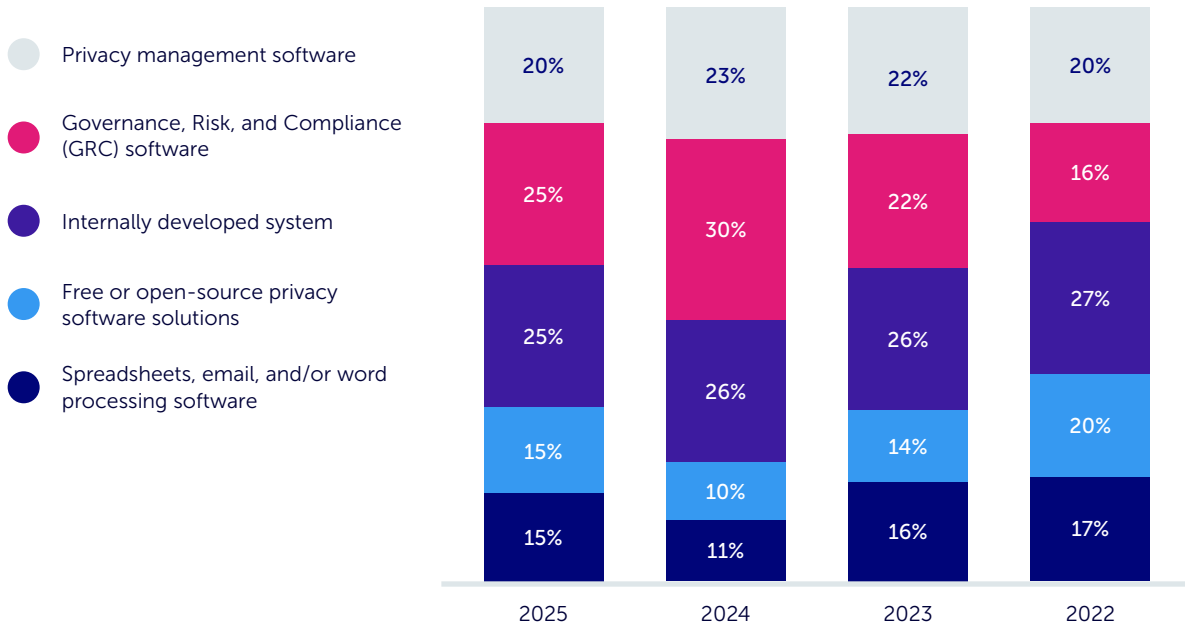


# Privacy Solutions

Companies using dedicated privacy platforms outperform those relying on spreadsheets by up to 19 points. While 45% use commercial solutions, about 30% still rely on free or homegrown systems.

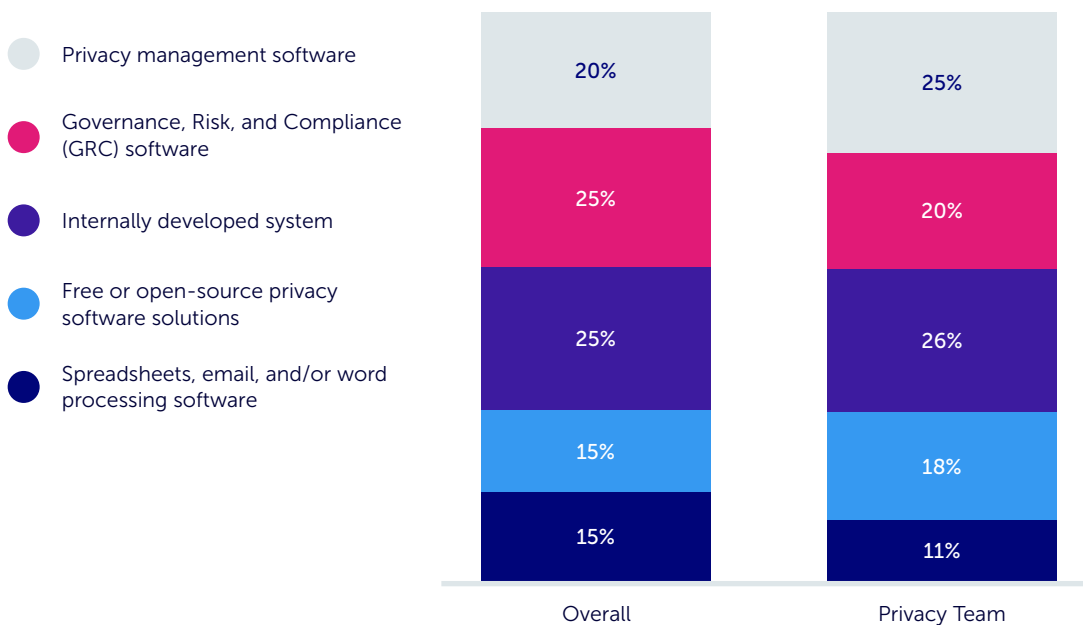
## Primary Solution

*What primary solution do you use to manage your privacy program?*



Among privacy professionals, purpose-built tools are favored over broader GRC systems and show better performance, with scores 10 points above average.

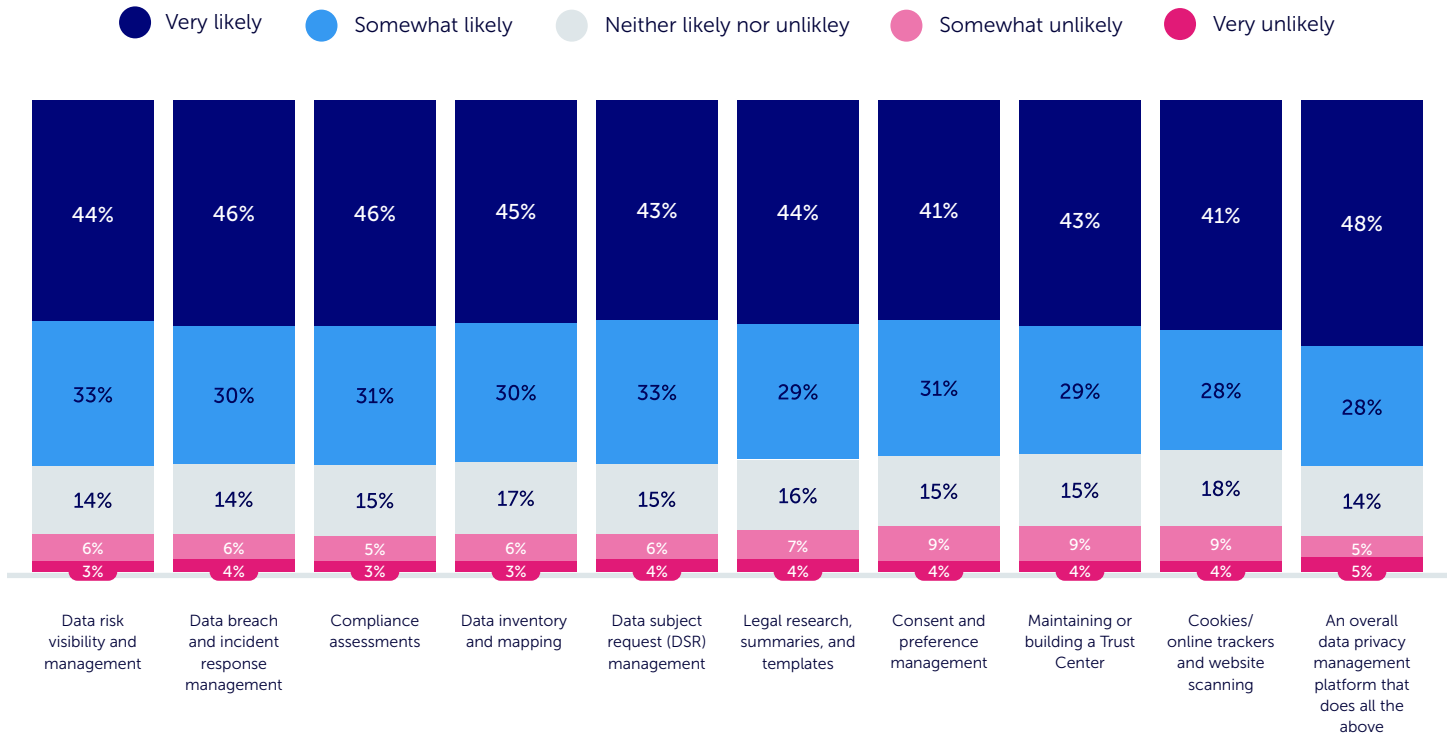
## Primary Solution (Views from the Privacy Team)



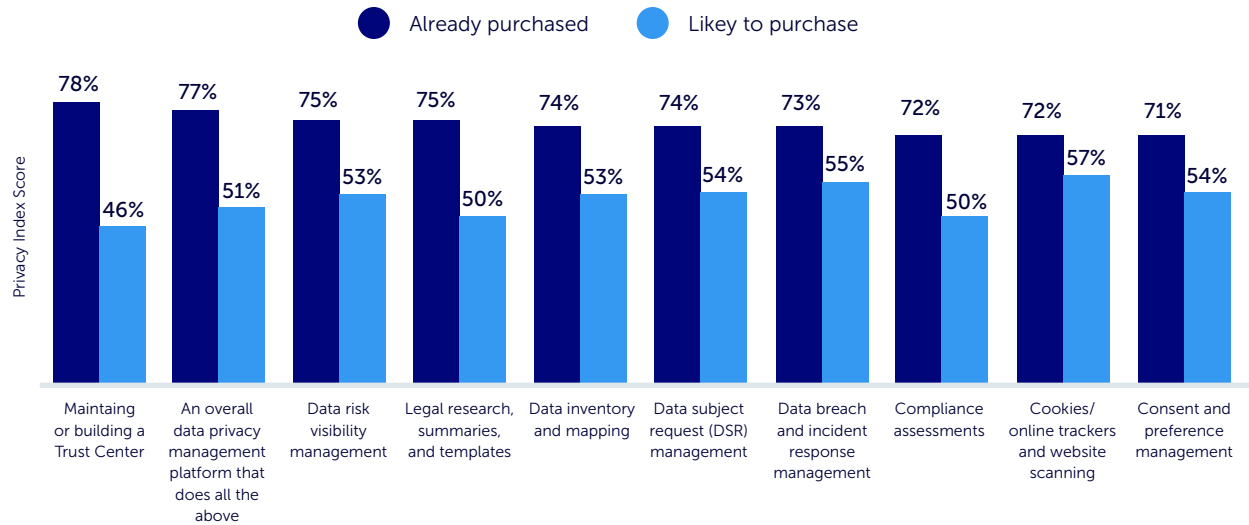
Data risk visibility and management is the highest in demand, followed by data breach and incident response management.

## Likelihood to Purchase

*How likely is your company to purchase "made to purpose" software to provide the following capabilities? (excludes "Don't know/Not sure" AND "already purchased")*



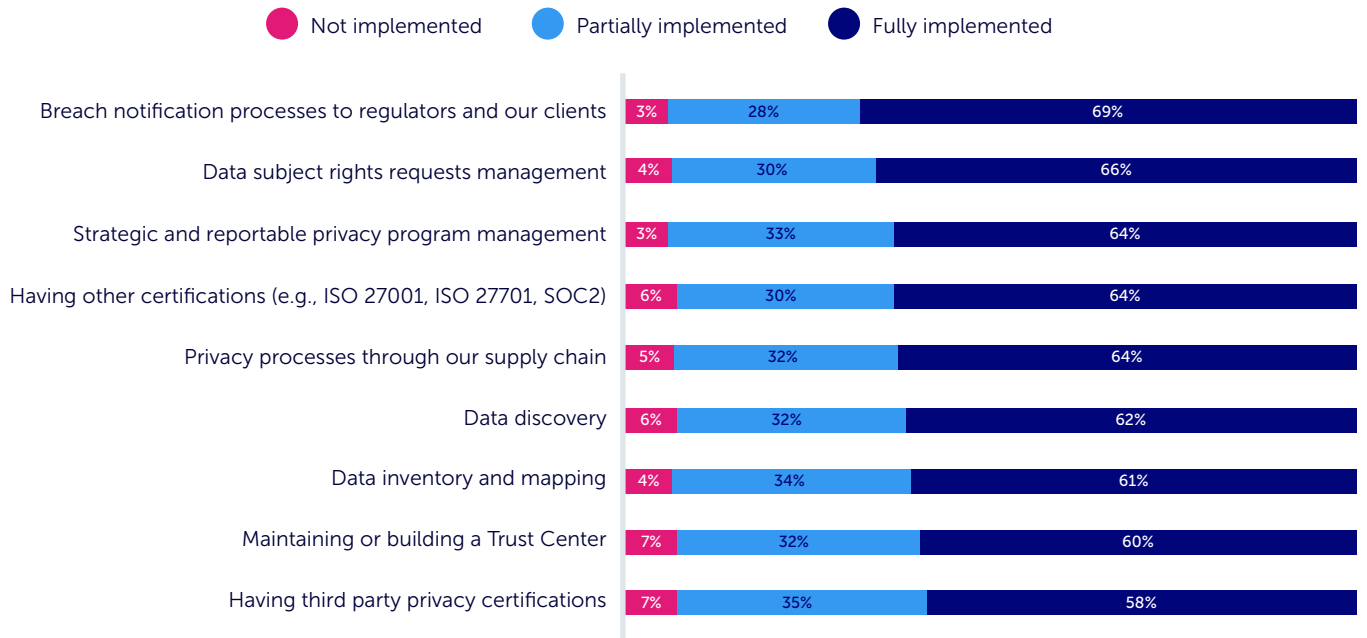
Organizations that have adopted these solutions show significantly higher Privacy Index scores, especially when most key tools are fully implemented. Those who haven't adopted such tools consistently underperform.



Not surprisingly, both breach notification processes and data subject rights requests management top the list of solutions fully implemented in companies.

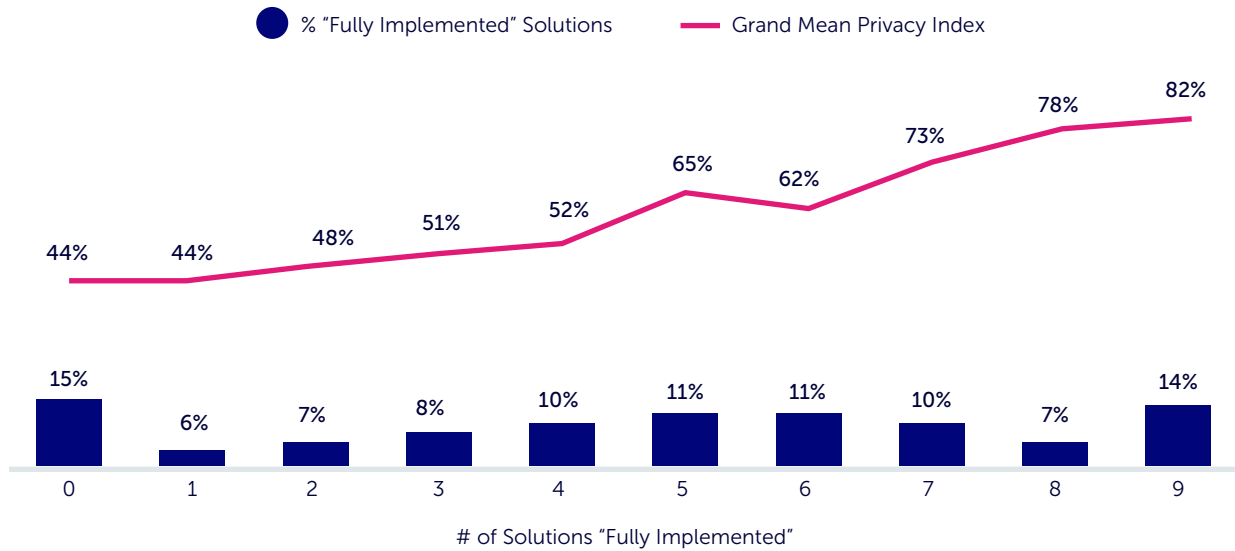
## Implementation Status

*For each of the following privacy initiatives, please indicate the state of implementation at your company currently. (excludes "Don't know/Not sure")*



Quite tellingly, the more solutions that are implemented, the better the scores on the Privacy Index. Unless companies have tackled at least half of the solutions needed, their privacy competence lags. Conversely, those who have fully implemented most to all needed solutions score 10 to 20 points higher than the average of 61%.

### Number of “Full Implementation” Solutions and Privacy Competence

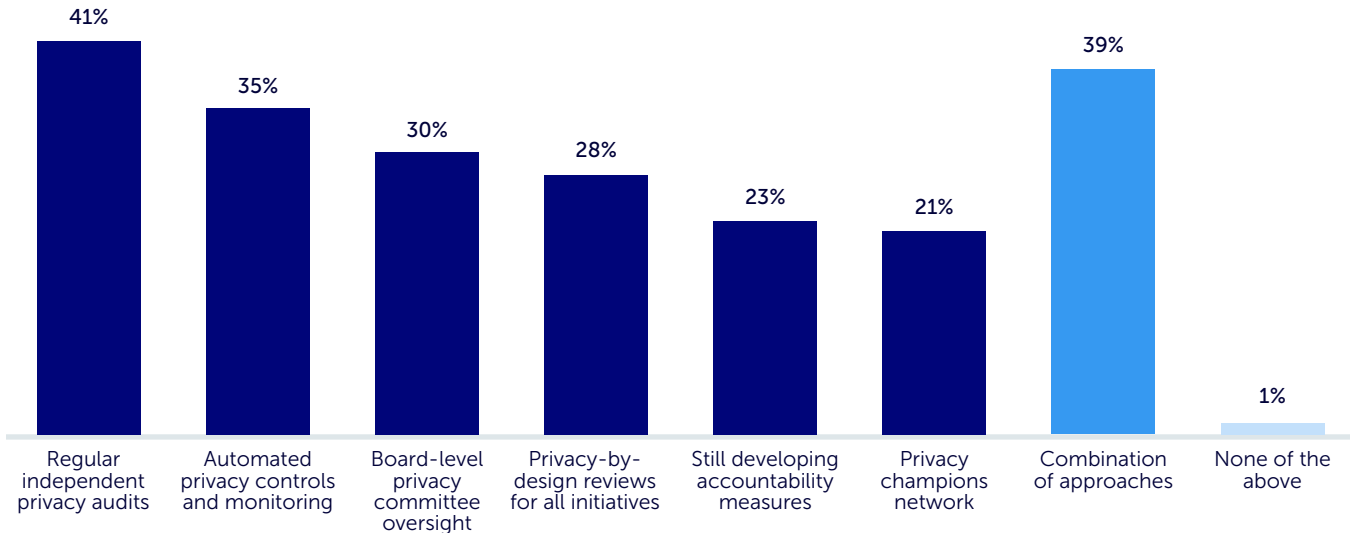


# Privacy Management Measurement

Measuring privacy effectiveness remains a key focus in 2025. There is a wide variance in accountability approaches, with over a third of companies (39%) using a combination of approaches.

## Privacy Accountability

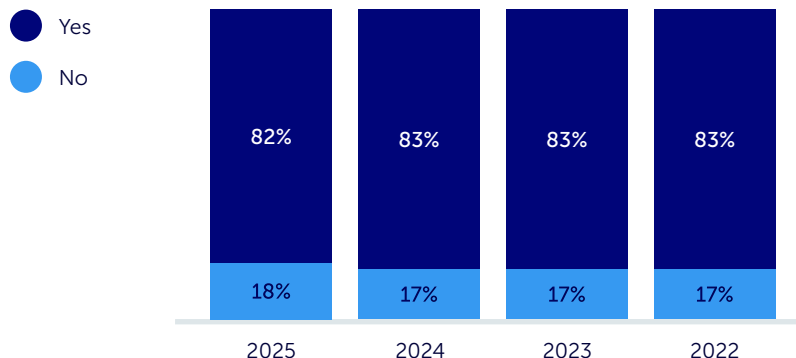
*How does your organization ensure privacy accountability?  
(choose all that apply)*



In 2025, the percentage of companies measuring the effectiveness of their privacy programs will virtually remain the same as the last four years, at just over eight in 10 (82%).

## Measuring Privacy

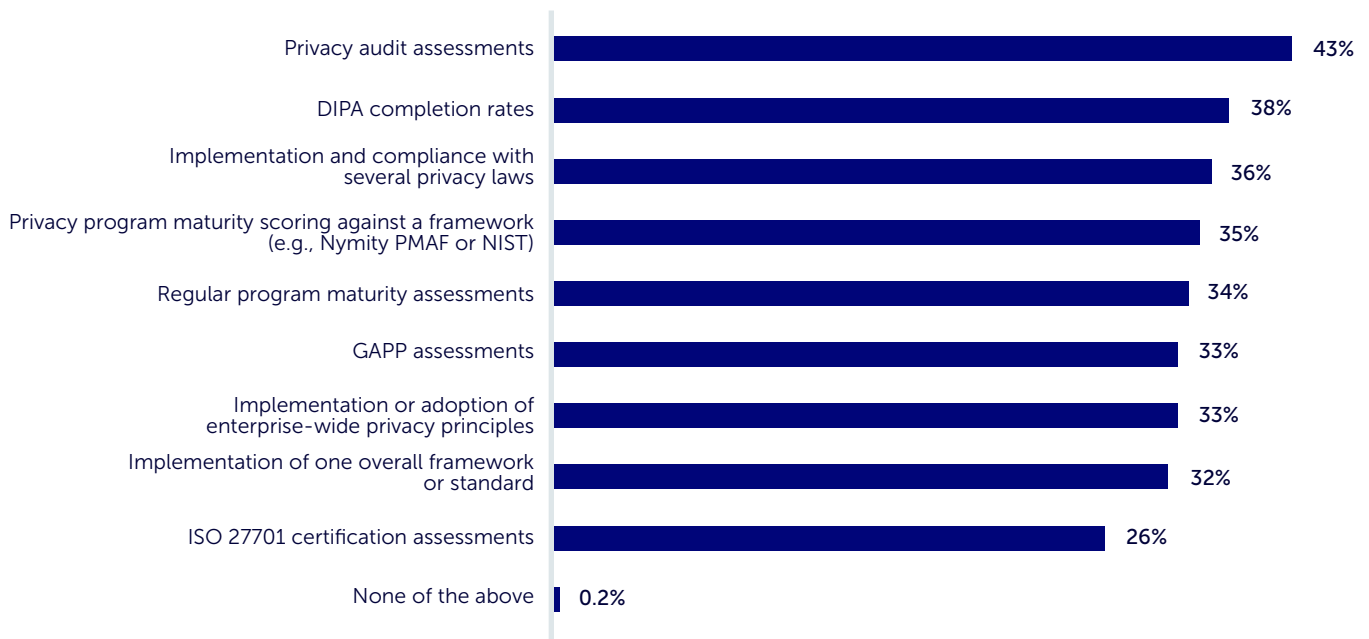
*Does your company currently measure the effectiveness of its privacy program?*





Most companies (82%) are measuring privacy effectiveness with regular, independent audits ranked as the top method. DPIAs and compliance tracking follow.

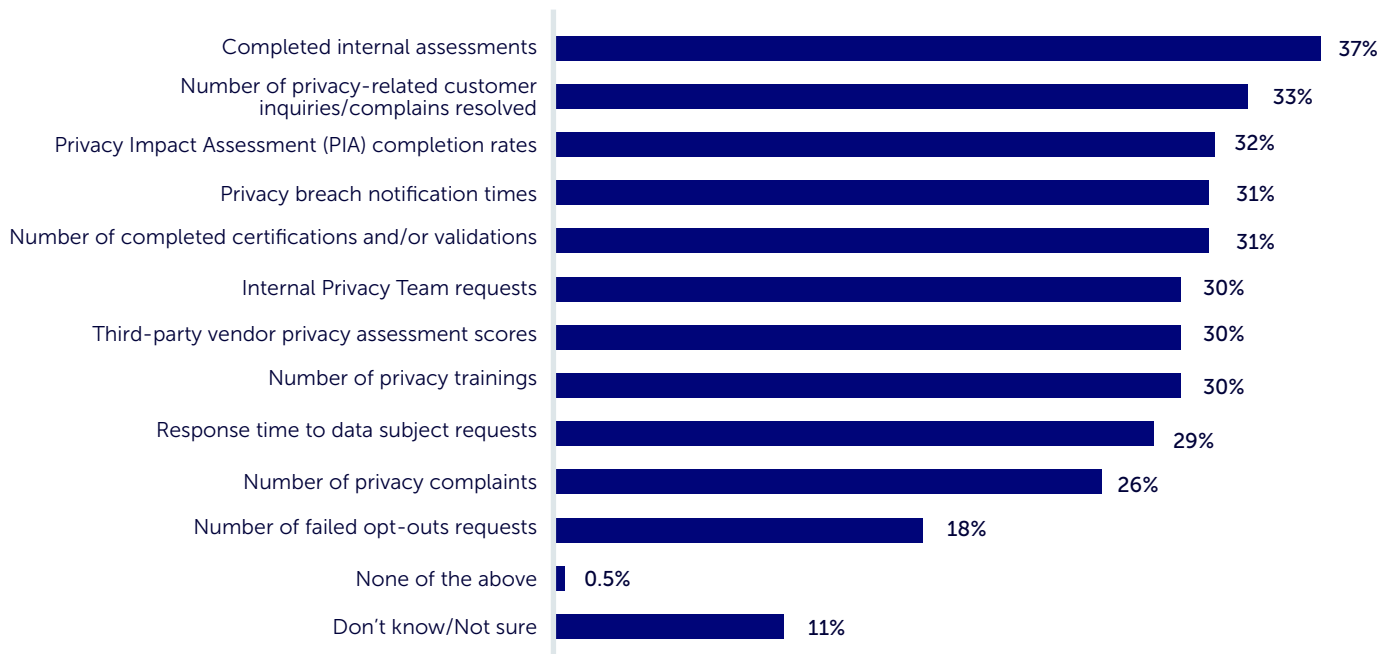
### Primary Measurement Methods



Completed internal assessments are the most-used Privacy Program KPI.

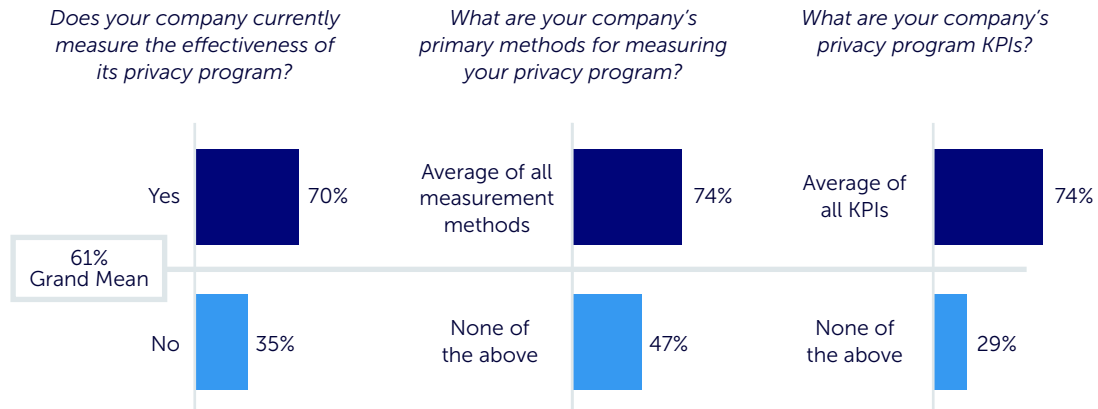
### Privacy KPIs

*What are your company's privacy program KPIs? (choose all that apply)*



Companies that measure their privacy efforts outperform non-measuring peers by 35 points on the Privacy Index. This indicates clear benefits of accountability and that what gets measured, gets managed.

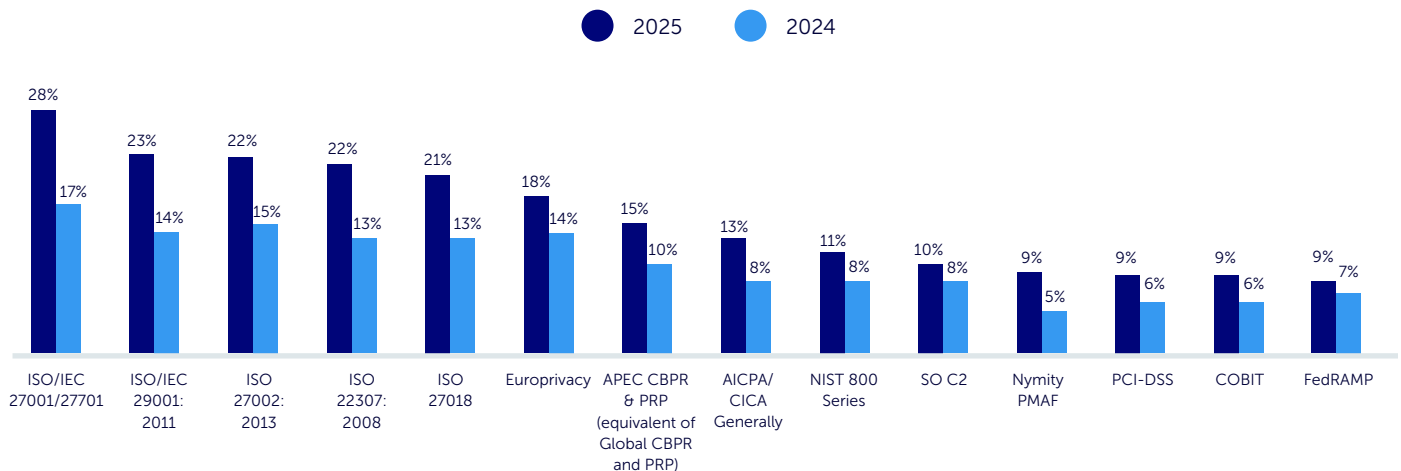
## Privacy Index Scores by Measurement Initiatives



The value of industry standards grew substantially year over year, with various ISO measures being the most popular.

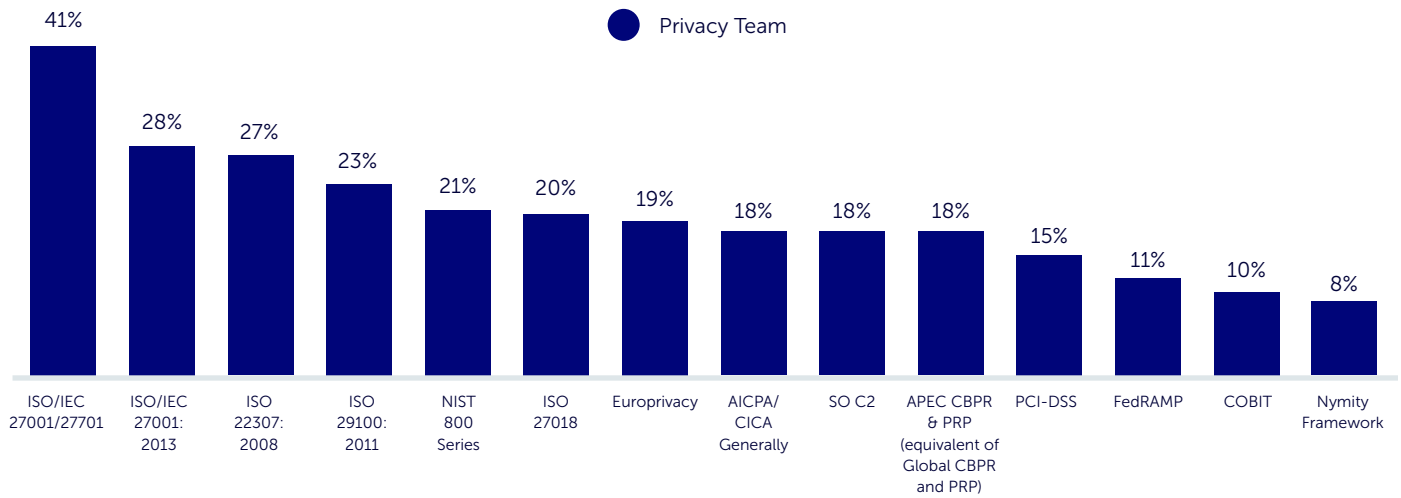
## Value of Standards

Which certification or compliance standards are most valuable to your company?  
(choose all that apply)



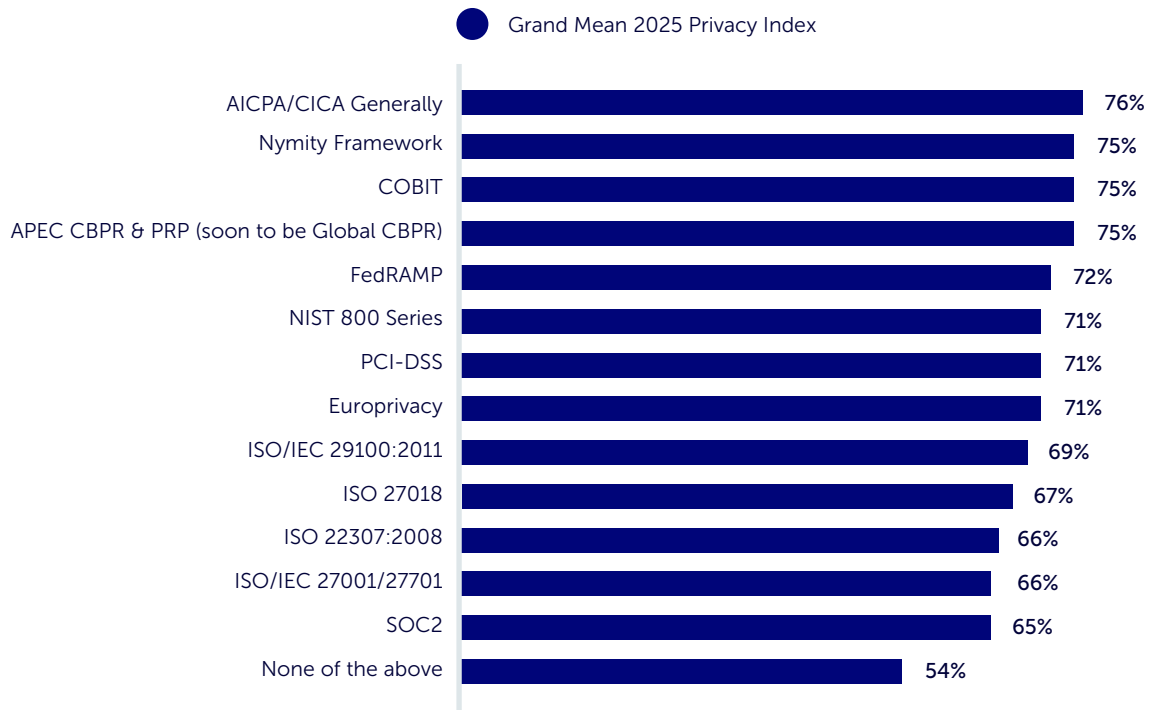
Looking more closely at the Privacy Teams' views, we see higher frequencies of industry-recognized standards being valued across all standards.

### Value of Standards by Privacy Team



Standards with more comprehensive coverage and robust requirements lead to stronger privacy practices, all scoring above the 61% average. The [Nymity Privacy Management Accountability Framework](#) (PMAF), though less adopted, delivers one of the highest scores, alongside AICPA/CICA, COBIT, and [APEC CBPR & PRP](#).

### Privacy Index Scores Based on Certifications Valued



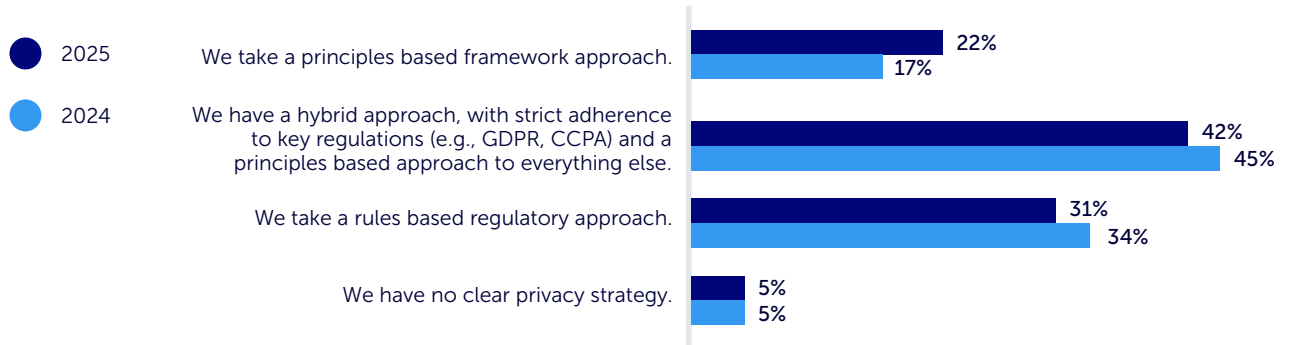
Clearly, adopting standards is helpful and aligns with our findings on principles-based program approaches.

# Regulatory Compliance Approach

For the second year running, participants were again asked what approach their company took toward privacy in terms of regulatory compliance. A shift occurred year over year, with a five-point increase in organizations taking a principles-based approach. That said, the hybrid approach remains most popular, followed by strict adherence to a rules-based regulatory approach.

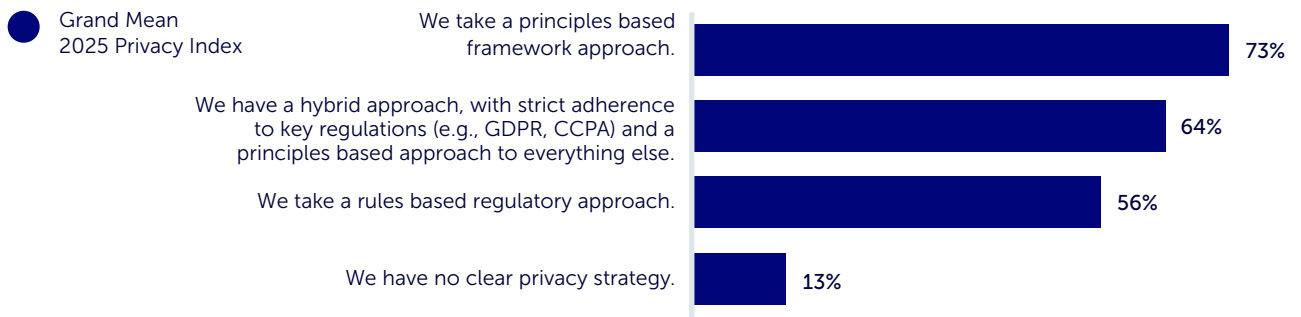
## Approach to Regulations

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



The principles-based framework approach scored 12 points above average on the Privacy Index and 17 points higher than a rules-based approach. In contrast, having no clear strategy led to a failing score of just 13%.

## Privacy Index by Regulatory Approach



### RULES VS PRINCIPLES: A SHIFT IN THINKING

2025 marked a five-point increase in companies adopting a principles-based regulatory compliance approach. It's not about checking every box. It's about doing what a consumer would expect to be a fair and equitable approach — and it works. These companies scored 12 points higher than those with a rigid, rules-based method.

# The Bottom Line

Privacy in 2025 is no longer a checkbox. It's a catalyst for trust, a strategic differentiator, and increasingly, a reflection of organizational maturity. This year's Global Privacy Benchmarks make one thing clear: the gap is growing between those who treat privacy as a core business function and those who still see it as compliance overhead.

Organizations that are winning on privacy aren't improvising. They're investing. They've centralized their privacy teams, operationalized measurement, embraced frameworks, and implemented purpose-built tools. They're embedding privacy not just in IT workflows, but in boardroom decisions, product design, and brand promises. These leaders are rewarded with performance: their Privacy Index scores outpace the average by up to 20 points, and their confidence in protecting stakeholder data is meaningfully higher.

But the urgency is real. AI-driven risk, global regulatory shakeups, and consumer expectations are evolving faster than many privacy programs can keep up. Small companies are catching up quickly. Procurement priorities are shifting toward vendor oversight and Trust Centers. Yet many organizations still lack the foundational infrastructure needed to respond at scale. Fewer than one in four have purchased a full privacy management platform, and fear, not foresight, is too often the trigger.

## So what's next?

This report is more than a benchmark. It's a blueprint. The path to high performance is well-lit: align teams, measure outcomes, embrace standards, and fully implement the tools that scale and sustain your efforts. Privacy isn't just about avoiding breaches; it's about earning trust before it's tested.

## Now is the time to act.

If your privacy program isn't evolving, it's falling behind. Learn from the leaders. Identify your gaps. Take the next step toward building a privacy program that's not only compliant but confident, credible, and future-ready.

---

## 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](https://TrustArc.com).

