TrustArc

2024 Global Privacy Benchmarks Report

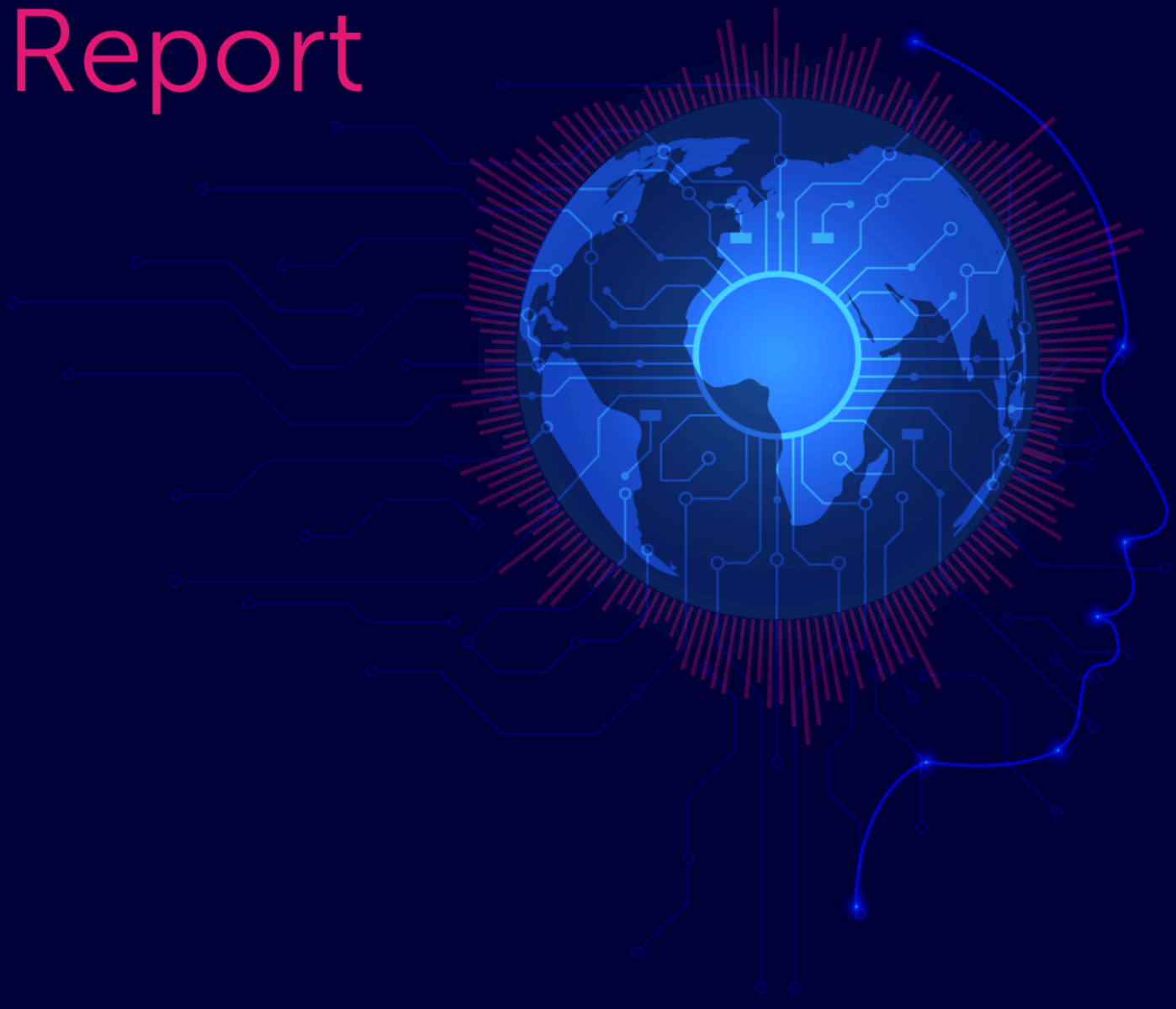


Table of Contents

Introduction

TrustArc's 5th Annual Global Privacy Benchmarks Survey provides a comprehensive corporate view into privacy developments worldwide, including insights from our Global Privacy Index. The 2024 report captures evolving challenges and threats to privacy, findings related to the adoption of AI, and insights into essential privacy strategies, priorities, and best practices.

The primary regions surveyed include the U.S., Europe, and the UK, with additional insights gathered from South America and Asia. This year's report captured 1803 participants globally.

Our methodology continues to ensure a balanced, 360° perspective by statistically weighting results across both organizational roles and by company revenue. This approach allows us to compare findings year-over-year, knowing that YoY changes are not the result of a different sample composition.

In the current climate of digital transformation and compliance, the emphasis on risk and privacy remains crucial. Many companies have elevated their privacy initiatives and increased investments in data security and data protection as core components of their operational and growth strategies. While AI presents significant new challenges, enforcing a growing list of privacy laws has intensified, demanding higher due diligence and accountability from organizations.

This report delves into how corporate priorities and strategies concerning privacy are shifting and underscores the integral role of privacy in maintaining public trust and organizational growth.

10 Key Privacy Insights Impacting Organizations

1. **The top three privacy risks for companies in 2024 are AI, brand reputation, and compliance**. Across the globe, half of respondents rated AI as either "4" or "5 – extremely challenging" for their business.

2. **Almost half of companies are making AI a priority in 2024**. Globally, 88% of those surveyed indicate it is important or very important.

3. **Maintaining brand trust remains the top privacy goal**. Regulatory compliance is closely followed as the second priority goal.

4. **Across the globe, there was an improvement in how companies tackle privacy by 8% year over year.**

5. **Taking a principles-based approach to privacy results in high privacy competence, with an average score of 74% on the Global Privacy Index.**

6. **Adopting the Nymity Privacy Management Accountability Framework (PMAF) is associated with the highest Privacy Index scores.**

7. **Privacy Management solutions score highest on the Global Privacy Index**. They score 6% higher than GRC solutions, 11% higher than internally developed systems, and 15% higher than free/open-source solutions.

8. **Measuring what you manage pays off**. Companies who measure privacy versus those who do not score 31% higher against the TrustArc Privacy Index.

9. **The top 3 areas of importance are third-party risk management, data discovery and scanning, and AI.**

10. **In 2024, the demand for privacy resources is rising, with two-thirds of people seeing the demand for privacy roles increase.**

360° View from Around the Globe

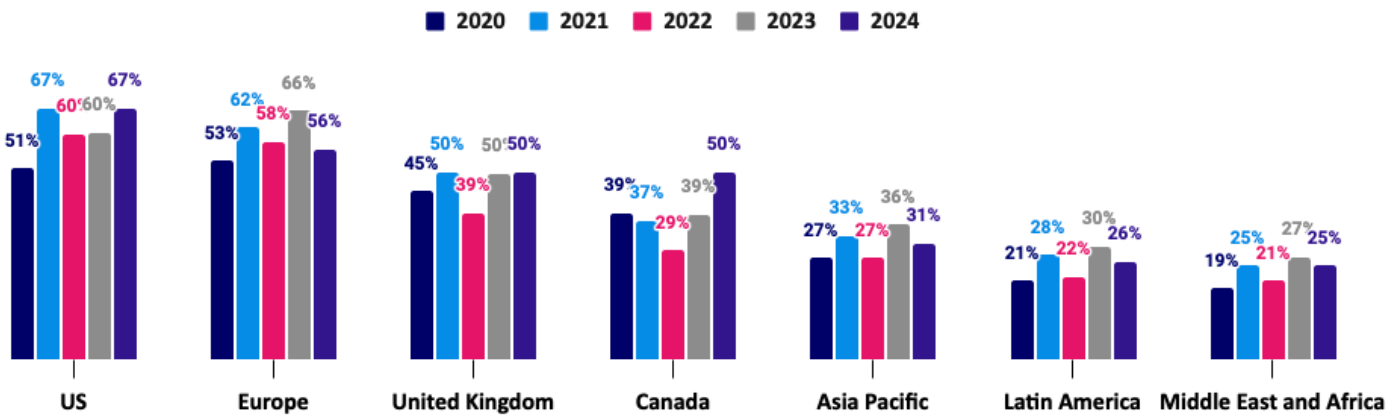
This year's Global Privacy Benchmarks Survey includes a detailed international perspective, with contributions from key geographic areas, including the U.S., Europe, the UK, South America, and Asia. This global sampling is crucial, as privacy concerns and regulations vary significantly across regions. The survey was conducted through online panels, website presence, and direct engagements, achieving a diverse and comprehensive dataset with 1803 participants.

The majority of responses came from companies headquartered in the U.S., Europe, and the UK, with substantial input from Canada, Asia Pacific, Latin America, the Middle East, and Africa. This wide geographic spread ensures that the findings reflect varied privacy landscapes and regulatory environments.

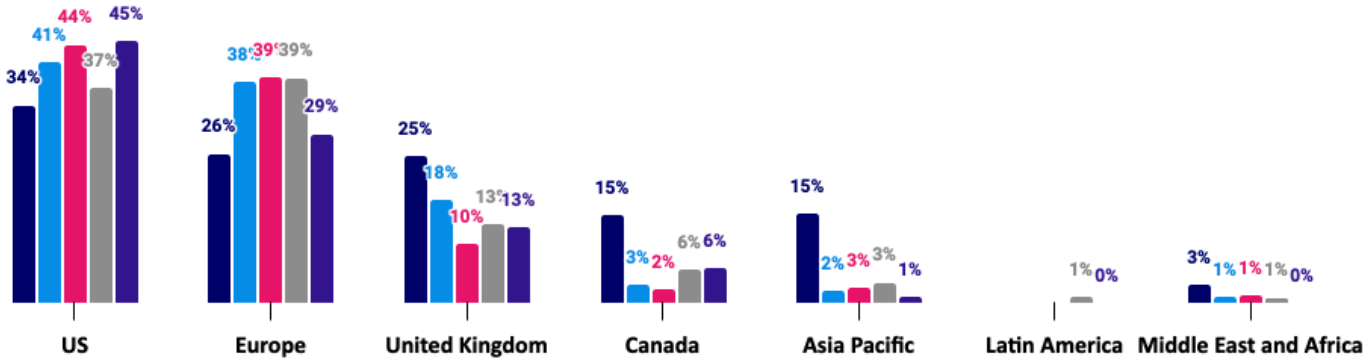
Exhibit 1: Head Office and Operating Regions

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

(Choose all that apply)



Where is your Head Office located?



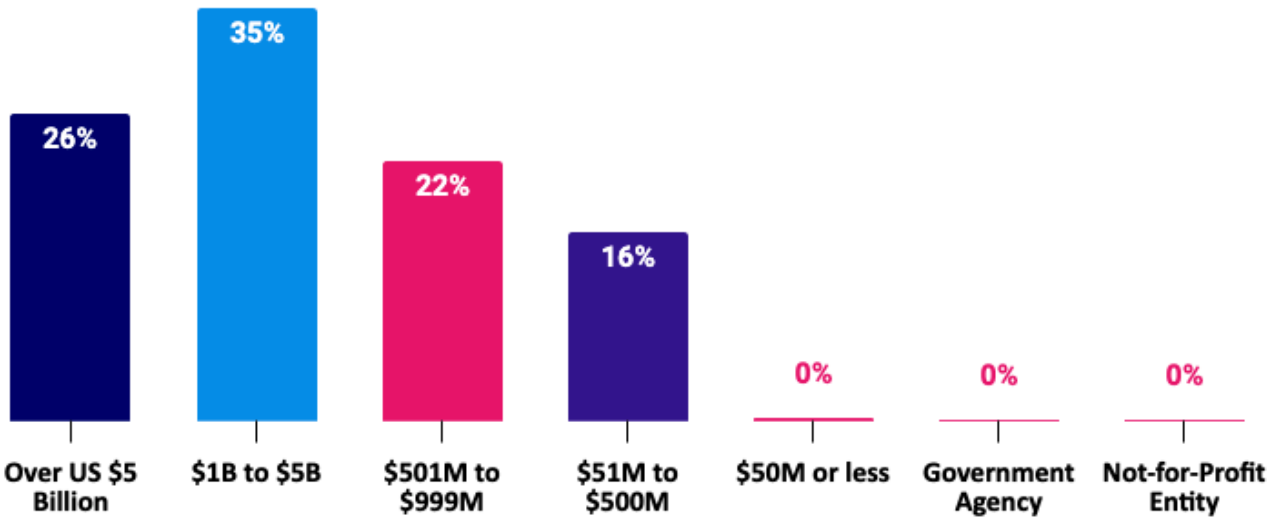
Respondents spanned a broad range of industries, with technology (20%), financial services (15%), and healthcare (10%) being the most represented. This distribution highlights the sectors that are most actively engaged in privacy management and likely to be impacted by privacy regulations.

We surveyed respondents from around the world – individuals within the privacy office, such as privacy leaders and privacy team members, senior leadership, middle management, and non-managerial full-time employees – on how well their enterprises manage privacy. The results were weighted to ensure each stakeholder group had a representative voice in the feedback.

With a sizable sample of over 1800 responses, our results include a range of company sizes across large, medium, and small businesses. Notably, over half were from companies with over $1B in annual revenue.

Exhibit 2: Revenue Size

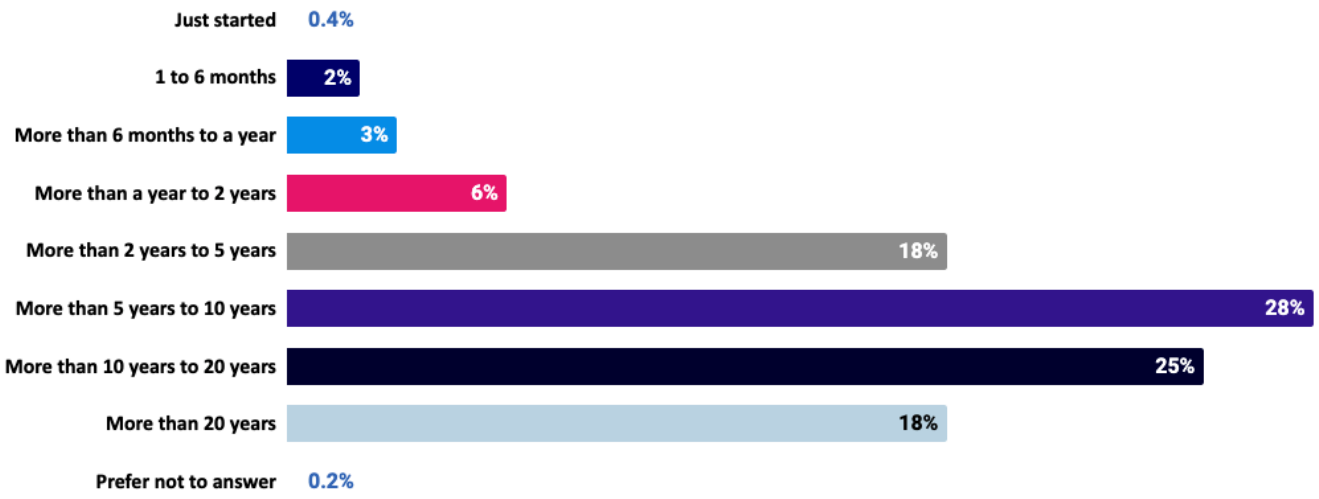
How would you classify your company's overall annual revenue in US dollars?



Fieldwork was conducted via two online survey panels, Centiment and MaruHub, along with web surveys from TrustArc email marketing pushes and open web surveys on TrustArc's website and social channels. Forty percent of survey participants had been with their company for ten years or more, another 26% more than 5 years, and the remaining third (33%) for less than 5 years.

Exhibit 3: Tenure

How long have you worked for your current company?



This work was commissioned by TrustArc and conducted by Golfdale Consulting since its inception in 2020.

Analysis and Insights

Privacy Teams and Demands

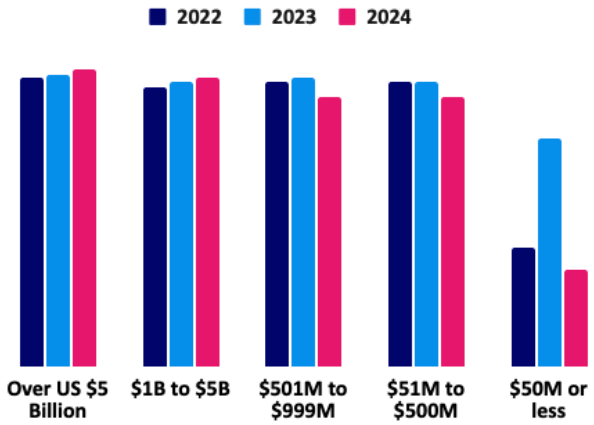
The establishment of dedicated privacy offices remains steady, with more than nine out of ten medium- and large-sized companies having one. In 2024, there is a slight increase of two percentage points by very large companies ($5B+) with a marked decrease in small companies (<$50M). The latter may be due to sampling variation as they were not the main target of the study.

Exhibit 4: Privacy Team Composition

Dedicated Privacy Office YoY

Results shown in each year for companies, $50M+ in revenue, and excluding "Don't know/Not sure"

Dedicated Privacy Office by Revenue Size

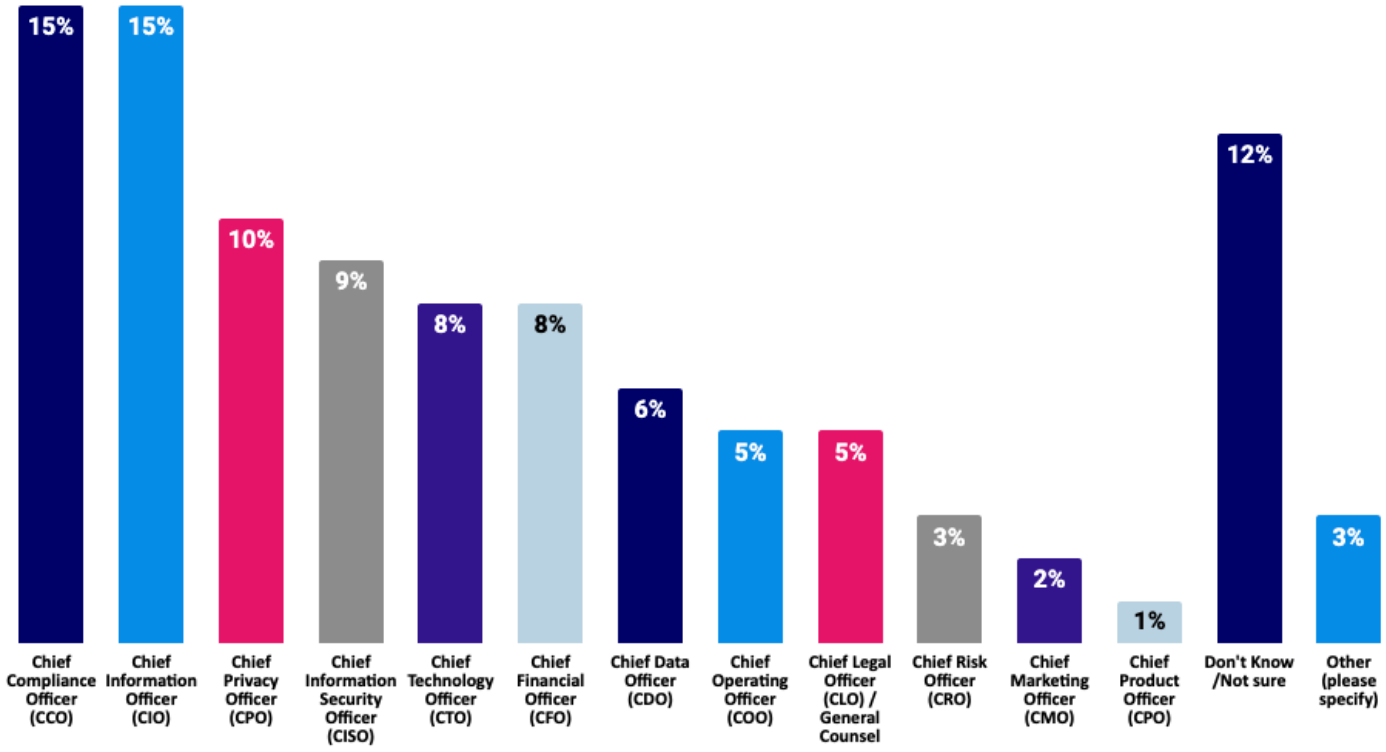


Organizational Placement of Privacy Teams

Privacy is here to stay and continues to have varying reporting structures. Privacy remains a staple in medium and large enterprises, and over the past four years, nine out of ten companies have dedicated privacy teams. That said, these teams can be found in no less than 12 different "reporting to" structures varying from the Chief Information Officer or Chief Compliance Officer (15%) through the Chief Information Security Officer (9%) to the Chief Product Officer (1%). The location of privacy within organizational structures remains varied, reflecting its cross-functional importance.

Exhibit 5: Privacy Team Reporting Structure

Which role heads up your privacy team or does your privacy team report up to?



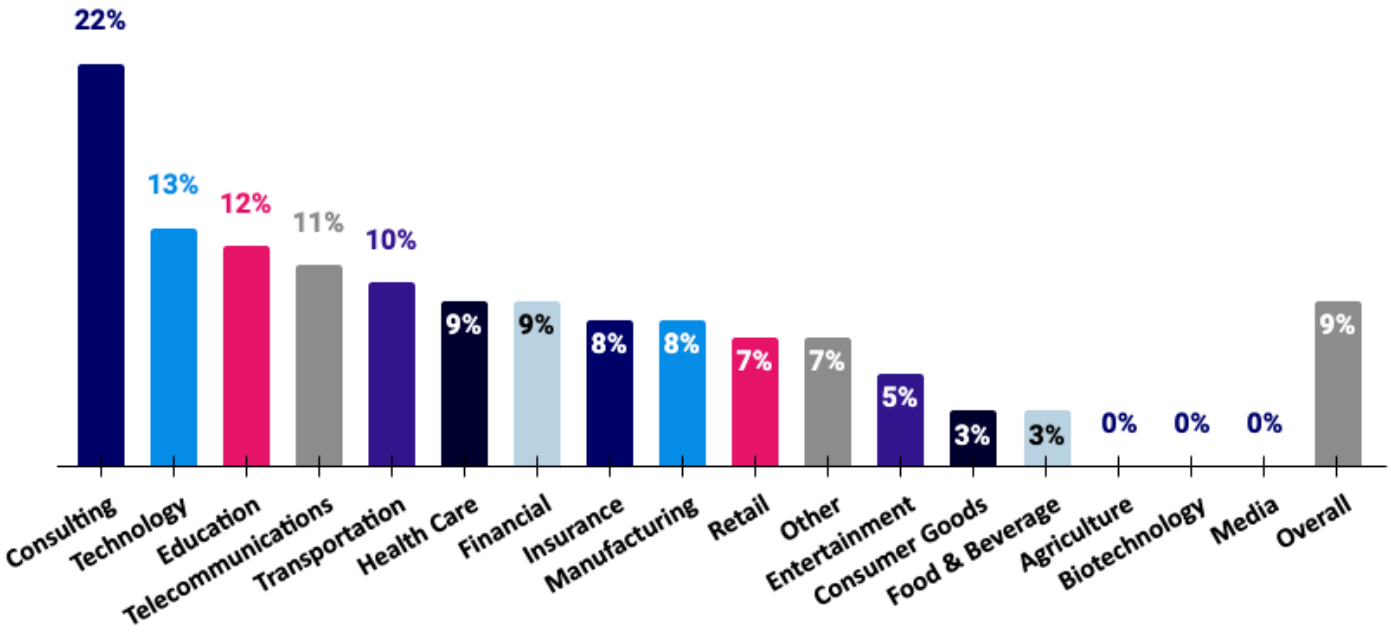
Our findings indicate that in the Consulting and Technology sectors, the Chief Information Security Officer (CISO) more frequently leads privacy initiatives compared to other industries.

Conversely, it is quite rare for a privacy team to be overseen by a CISO or Chief Security Officer (CSO) in the consumer goods and food & beverage sectors.

Exhibit 6: CISO Lead by Industry

Which role heads up your privacy team or does your privacy team report up to?
Chief Information Security Officer (CISO) / Chief Security Officer (CSO)

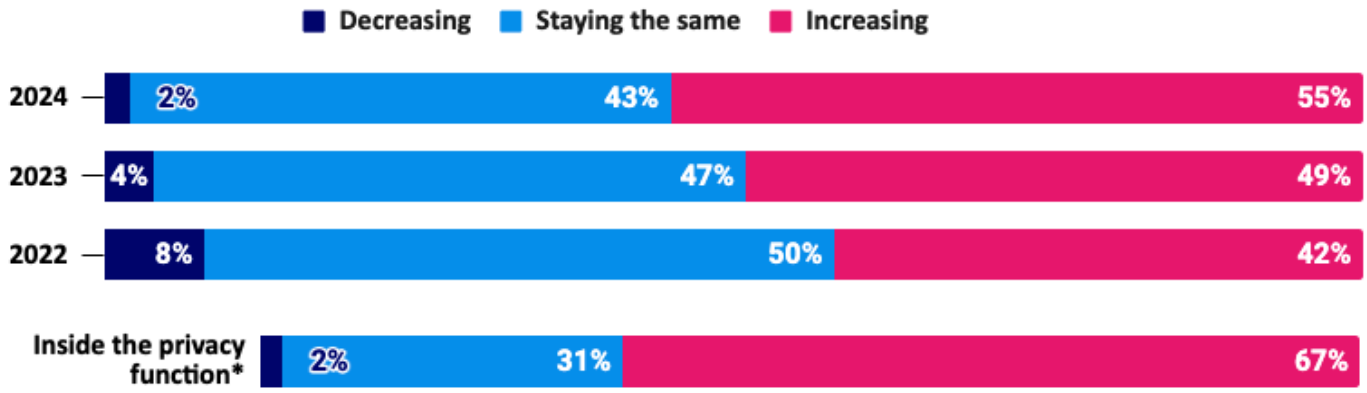
(Asked only of those with a dedicated Privacy Team)



Reflecting the increasing centrality of privacy in business strategies, 55% of respondents indicated that the demand for privacy roles within their organizations is expected to rise over the next year, an increase from 49% in 2023.

Exhibit 7: Privacy Demand Growth

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



**Privacy Executives + Privacy Team members*

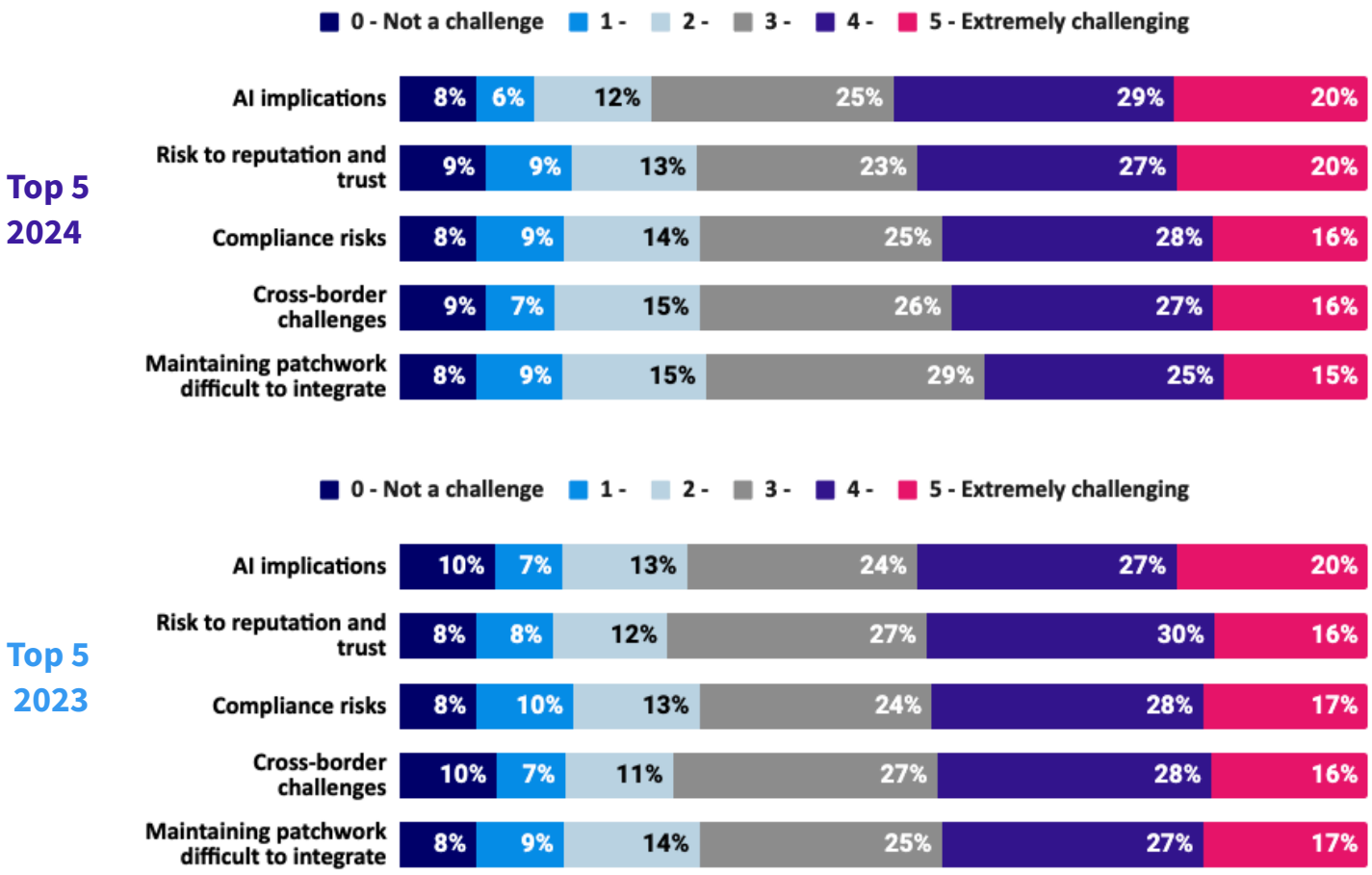
Inside the privacy function, just over two-thirds expect the demands for privacy roles to grow throughout 2024. This finding suggests a robust job market for those with privacy expertise.

Privacy Challenges and Vulnerabilities

The survey identified a set of core challenges in privacy for 2024, with Artificial Intelligence (AI) remaining the top challenge for the second consecutive year, reflecting the increasing integration of AI technologies in business processes. This year, data breaches overtook regulatory compliance risks, moving into the second spot, followed by reputational risks from social media, which remained a significant concern.

Exhibit 8: 2024 Vs. 2023 Challenges – YoY Comparisons

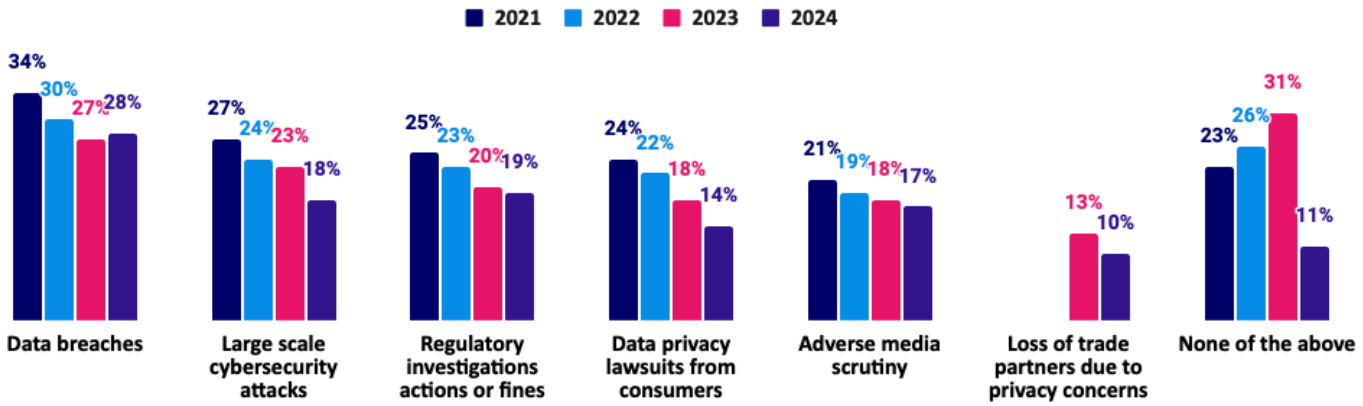
Of the following challenges that many enterprises face, please rank them from 0 "not a challenge for us at all" to 5 "extremely challenging for our business" as they relate to privacy risks that your company is likely to encounter in 2024?



The landscape of vulnerabilities shifted slightly in 2024, with data breaches continuing to dominate as the primary vulnerability companies faced, indicative of the persistent and evolving threat landscape. Interestingly, cybersecurity attacks, while still critical, saw a decrease in prevalence, aligning with improved security measures across industries.

Notably, in 2024, there was a marked decrease in those claiming "none of the above," with nine out of ten reporting that their company had fallen prey to some form of privacy vulnerability. This figure dropped to just 2% among the Privacy Team members, suggesting that many employees may not be fully aware of all the privacy-related issues and incidents that arise.

Exhibit 9: Privacy Vulnerability



In terms of privacy concerns, third-party risk management surged to the forefront in 2024 as businesses increasingly rely on external partners and service providers. This finding underscores the importance of managing and mitigating risks associated with external collaborations. Data discovery and scanning followed closely, reflecting the need for robust mechanisms to handle and protect the growing volumes of data companies digest and use.

Exhibit 10: Privacy Concerns YoY

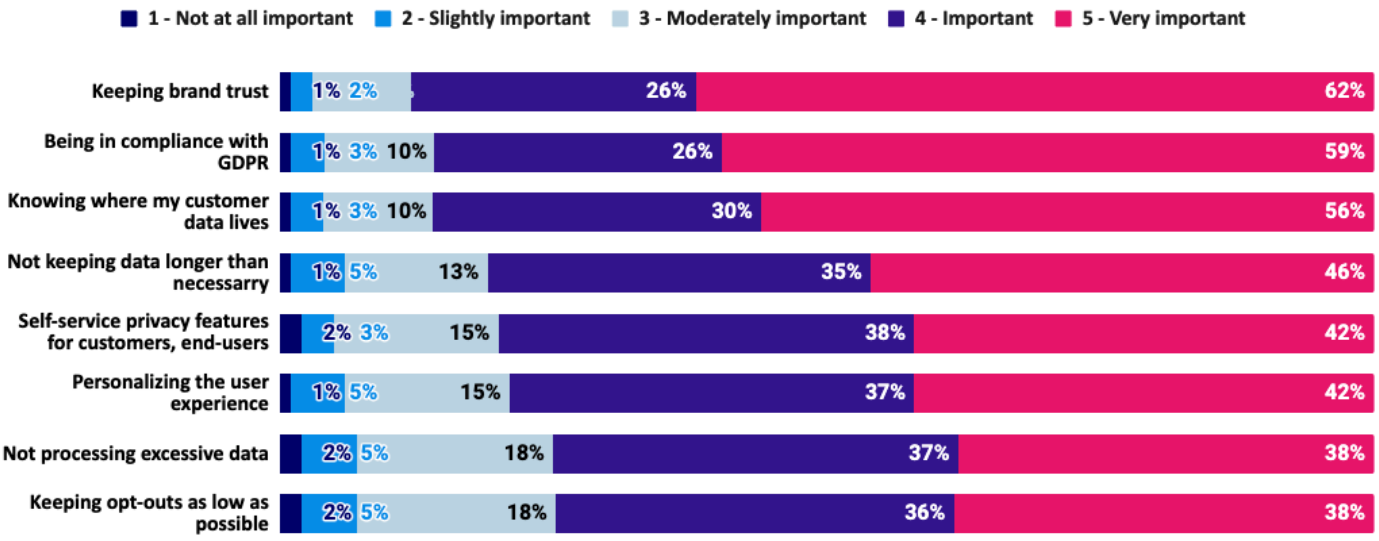
How important are the following topics to your company as they relate to privacy concerns and regulations?

Important + Very important	2024	YoY Change
Data discovery and scanning	77%	↑ +3%
Artificial Intelligence (AI)	70%	↑ +2%
Biometrics	64%	↑ +2%
Third-party risk management	78%	↑ +2%
Blockchain technology	62%	↑ +1%
Data Subject Access Requests (DSAR) technology solutions	74%	↑ +1%
Transfers of data outside the EU, UK, Switzerland	64%	↓ -3%

With both the challenges and concerns associated with privacy articulated, it is then important to look at the reverse: what are the benefits of privacy that accrue to companies that make it a priority? Consistent among the benefits year-over-year is brand trust. Building trust with all stakeholder groups continues to be a paramount goal and benefit for organizations in an era where consumer expectations around privacy are high. This element ranked as the top privacy effort. Compliance came secondary and can be interpreted as the foundational need to uphold trust and integrity. This finding emphasizes the importance of various privacy goals, including brand trust, compliance, and data management.

Exhibit 11: Privacy Benefits

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



The 7 Keys: Privacy Competencies – 2024 Update

TrustArc surveys essential competencies that build privacy confidence aimed at maintaining brand trust through effective leadership.[1] The 2024 survey results demonstrate how these competencies continue to evolve and become ingrained in organizational cultures. The seven keys to privacy competence are outlined below, shown in order of highest to lowest scoring attributes.

1) **Mindfulness:** Continuous mindfulness about privacy is becoming a standard practice, with companies increasingly adopting proactive privacy measures. While the scores appear high (84% indicating that they *agree* or *strongly agree*), it is important to note that even with this self-report measure there are 16% who do not believe their company is mindful at all about privacy.

[1] These 7 keys were identified in the first year of the study based on a psychometric assessment of numerous privacy attributes that were fielded. In the second year of study, we reanalyzed and confirmed their ongoing construct validity and reliability as core measures of privacy competence. Their statistical predictive capabilities are also demonstrated throughout the remainder of this paper.

2) **Strategic integration:** Privacy is pursued as a core part of business strategy for most enterprises, with more companies integrating privacy considerations into their strategic planning from the outset.

3) **Employee empowerment:** There is a significant improvement in empowering employees to raise privacy issues without fear of reprisal, reflecting both improved internal capabilities and a movement toward building privacy respectful cultures.

4) **Regular board review:** Ensuring the Board of Directors regularly reviews and discusses privacy matters remains paramount. More companies in 2024 reported an increased frequency of privacy discussions at board meetings. Again, while this is a generally positive finding, it is worth noting that one in five do not report this as happening.

5) **Privacy training:** Training on privacy matters has been expanded in scope and frequency, covering more roles within organizations.

6) **Business differentiation:** Embracing privacy practices as a business differentiator has seen growth, particularly in sectors where consumer trust is crucial.

7) **Operational Integration:** Privacy considerations are factored into daily business operations activities.

Exhibit 12: Keys 1 to 6

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

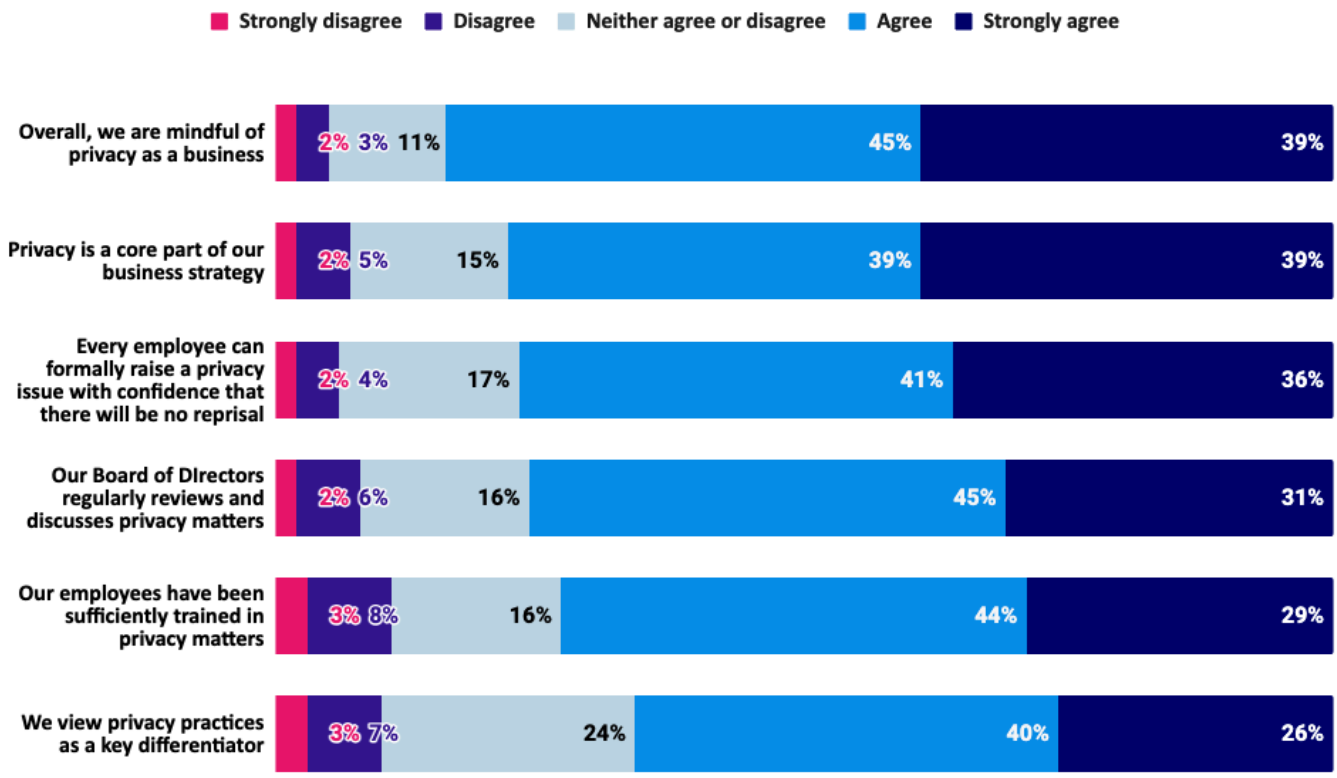
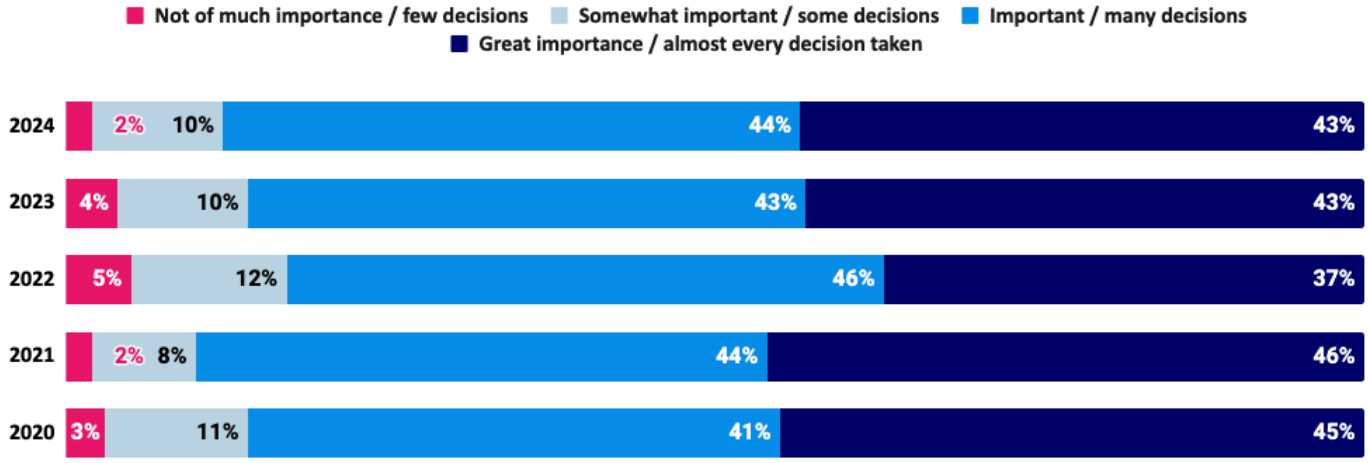


Exhibit 13: 7th Key to Privacy

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?

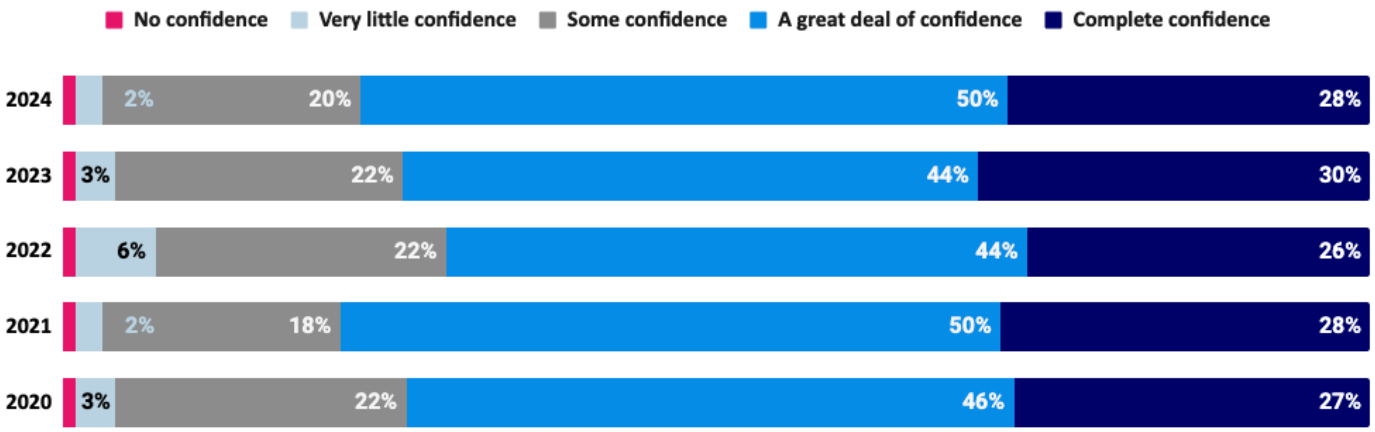
- *Privacy is of great importance and permeates almost every decision taken.*
- *Privacy is important and gets considered in many decisions.*
- *Privacy is somewhat important and gets considered in some decisions.*
- *Privacy is not of much importance and gets considered only in a few major decisions.*



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

Exhibit 14: 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?

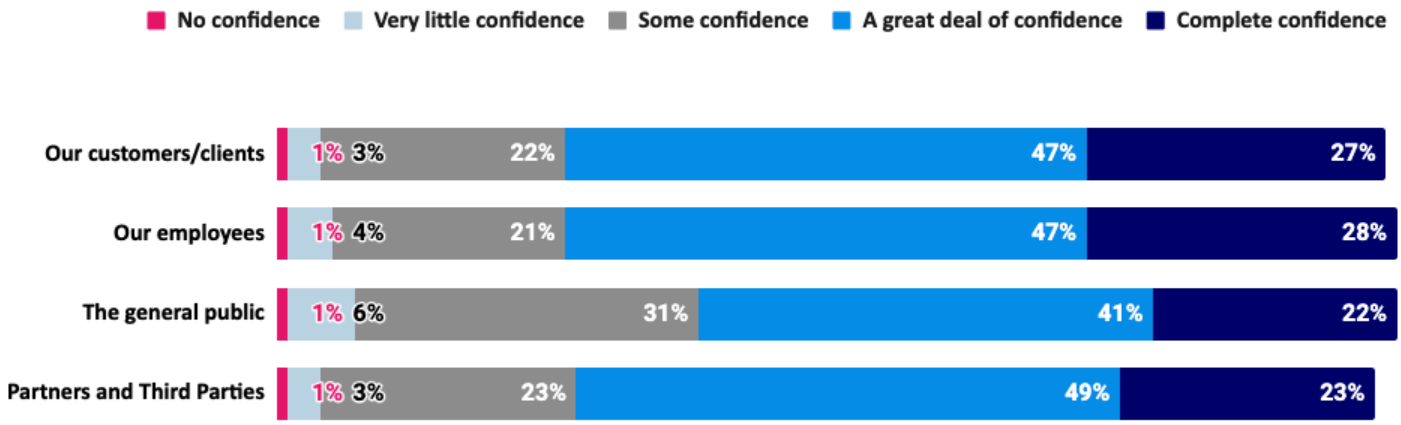


Confidence in their company's ability to manage data privacy for the four major stakeholder groups was then measured. These included:

- **Employee Confidence:** Employee confidence in their organization's privacy management remains high and is the best scoring stakeholder score, undoubtedly benefiting from increased training and more employee abilities to "speak up" on privacy matters, as evidenced earlier.
- **Customer Confidence:** Confidence levels are high in customer data privacy management and have shown improvement year over year. This may be due to more transparent privacy policies and customer communications.
- **Partner Confidence:** Confidence that partners and third parties are part of the privacy plan also appears relatively strong, which aligns with the importance of managing third parties concerning privacy. This confidence grows as companies strengthen their vendor management and risk assessment processes.
- **Public Confidence:** Public confidence shows the lowest confidence score. The ability to manage privacy for direct stakeholders is high, as evidenced above. Still, interestingly, there are many more doubts about how this translates into public perceptions of their privacy management.

Exhibit 15: Stakeholder Confidence

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



The TrustArc Global Privacy Index

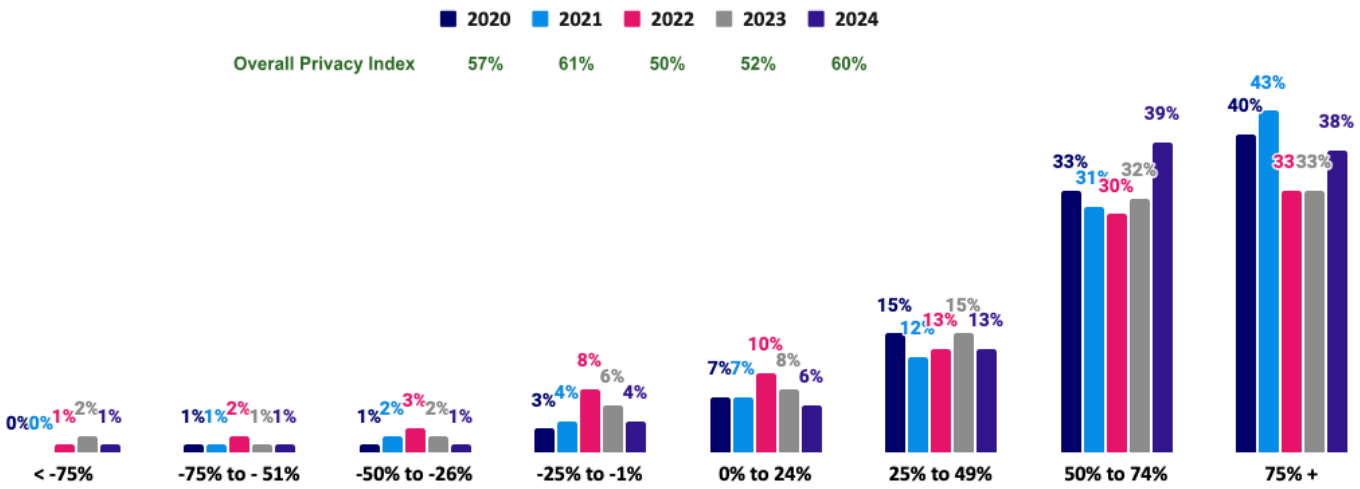
These measures are summarized into a single metric, the TrustArc Global Privacy Index. The index is a compilation of all the attributes above that assess how well companies perform on data privacy. This measure has proven useful for company self-evaluations of their current level of privacy competence[2].

The scoring system results in an overall robust privacy metric. It results from extensive statistical modeling conducted in 2020 and revalidated in 2021. These efforts resulted from the current set of 12 survey items (7 keys and 5 outcomes) from which a Grand Mean is derived. In allocating points for each item, deductions for poor ratings occur. While a 5 out of 5 on a particular question receives a full mark, a 4 receives a half mark, while either a 1 or a 2 out of 5 results in a full mark deducted.

The result is a score that ranges theoretically from -100 to +100, similar in some respects to how companies measure a Net Promoter Score (see NPS).

The Privacy Index provides an informative company self-assessment tool that weights four primary groups (senior execs, managers, FTEs, and privacy team members—with half of the latter allocated to privacy execs and half to privacy team members) equally for a comprehensive 360° view. The distribution of results across this year's survey and prior years is shown below. In 2024, the index increased by eight percentage points, reflecting overall improvements in privacy competencies and outcomes.

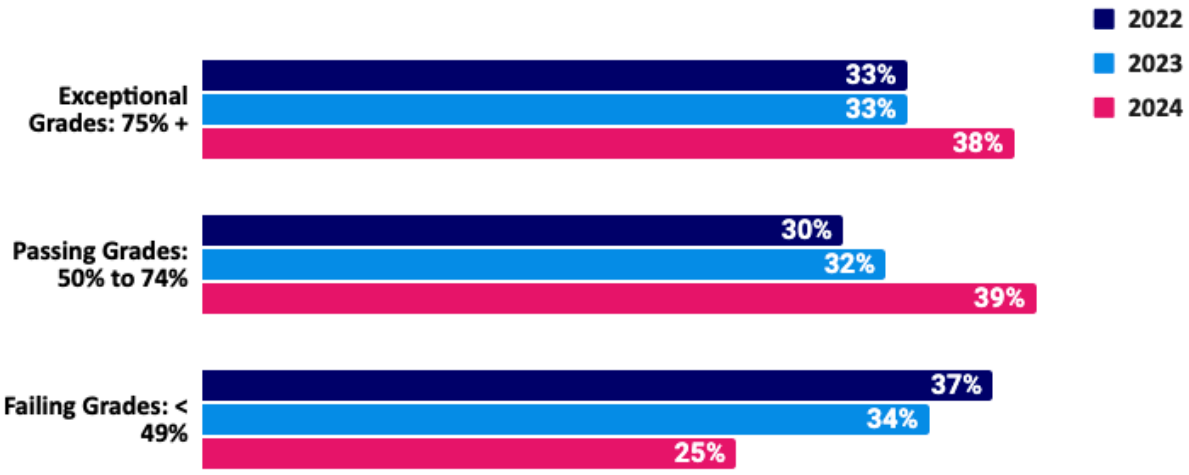
Exhibit 16: Keys to Privacy Index - Distribution YoY



[2] The scoring system results in a robust privacy metric. From the current set of 12 survey items (7 keys and 5 outcomes) a Grand Mean is derived. In allocating points for each item, deductions for poor ratings occur. The result is a score that ranges theoretically from -100 to +100, similar in some respects to how companies measure a Net Promoter Score (NPS).

What the high variance in the distribution informs us is that self-perceived competence in protecting privacy differs markedly across companies. Summarizing the range of scores, in 2023 below the results were approximately a third failing, a third doing an adequate job, and a third excelling.

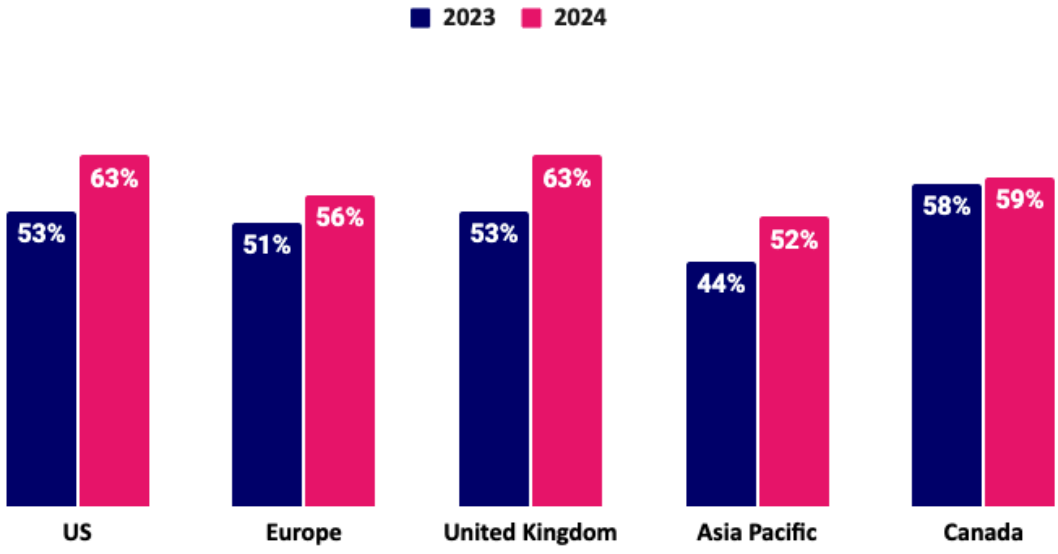
Exhibit 17: Graded Distribution of Privacy Index YoY



In 2024, the results have shifted. Notably, failing grades are now down to one quarter from a third last year, and by the same token, those with exceptional grades have risen by five percentage points. That said, notably on the tails of the distribution, 7% failed abysmally (i.e., scores in the -100 to 0 range, while 13% were truly exceptional in the 90 to 100 range.

The largest increase in the Privacy Index scores was evidenced in the US, although there were gains across all countries covered in the survey.

Exhibit 18: Privacy Index by Head Office Geography



Despite the rise in privacy competence in 2024, over half either *agree* or *strongly agree* that their company could do more to promote and defend privacy.

Exhibit 19: Doing More

Please indicate whether you agree or disagree with each of the following statements.
When it comes to privacy, we should be doing much more.

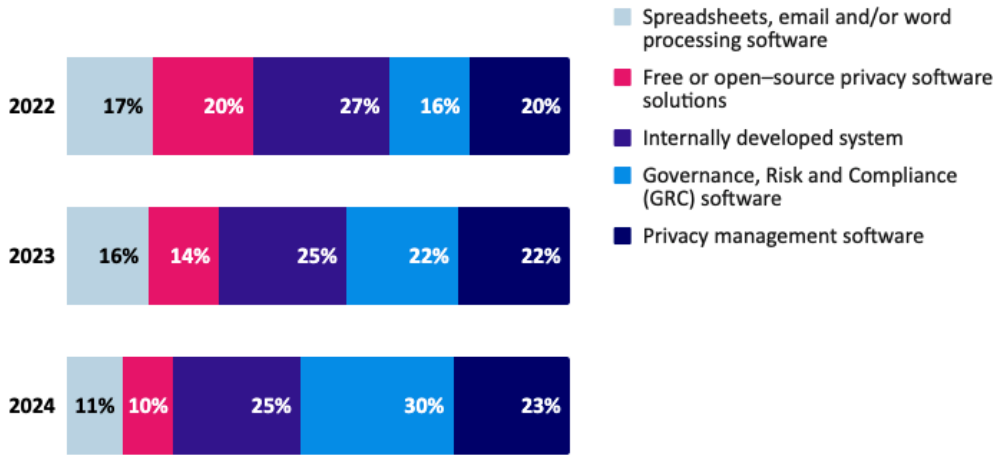
Privacy Solutions

The evolution of privacy solutions continues to be a central theme in 2024, with businesses increasingly moving away from makeshift approaches towards more integrated and sophisticated privacy management software.

In 2024, the transition from piecemeal to purpose-built privacy solutions has accelerated. Only 25% of companies use free or general-purpose software such as spreadsheets for privacy management, a decrease from the previous year. Conversely, there has been a slight increase in the adoption of dedicated Privacy Management solutions and an increase in the use of Governance, Risk, and Compliance (GRC) solutions. Just over half of medium- to large-sized companies use one of these approaches as their primary privacy management solution. Dedicated governance and program management solutions, such as TrustArc's PrivacyCentral, can provide meaningful efficiencies through the ability to map program controls across a number of regulations, frameworks, and security certifications, particularly in conjunction with automation, and proactively notify with new requirements or regulations.

Exhibit 20: Primary Solution

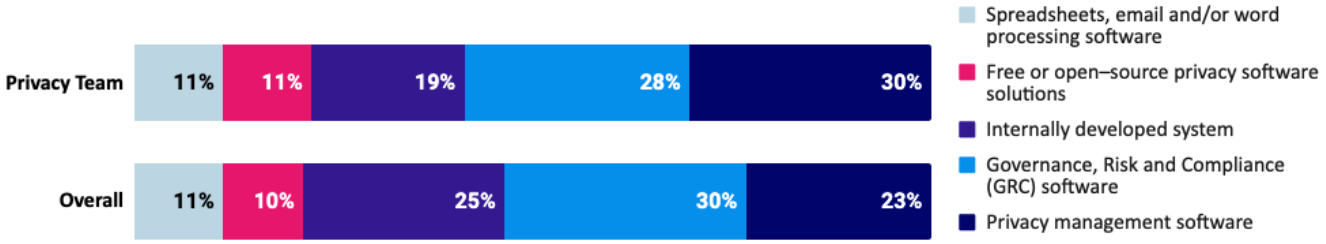
What primary solution do you use to manage your privacy program?



As the technical solutions are best understood by Privacy Team members and Privacy Executives, when looking at this specific cohort there is a more notable rise in fit-to-purpose Privacy Management software, with this solution set more prominent than GRC solutions.

Exhibit 21: Primary Solution (Views from the Privacy Team)

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

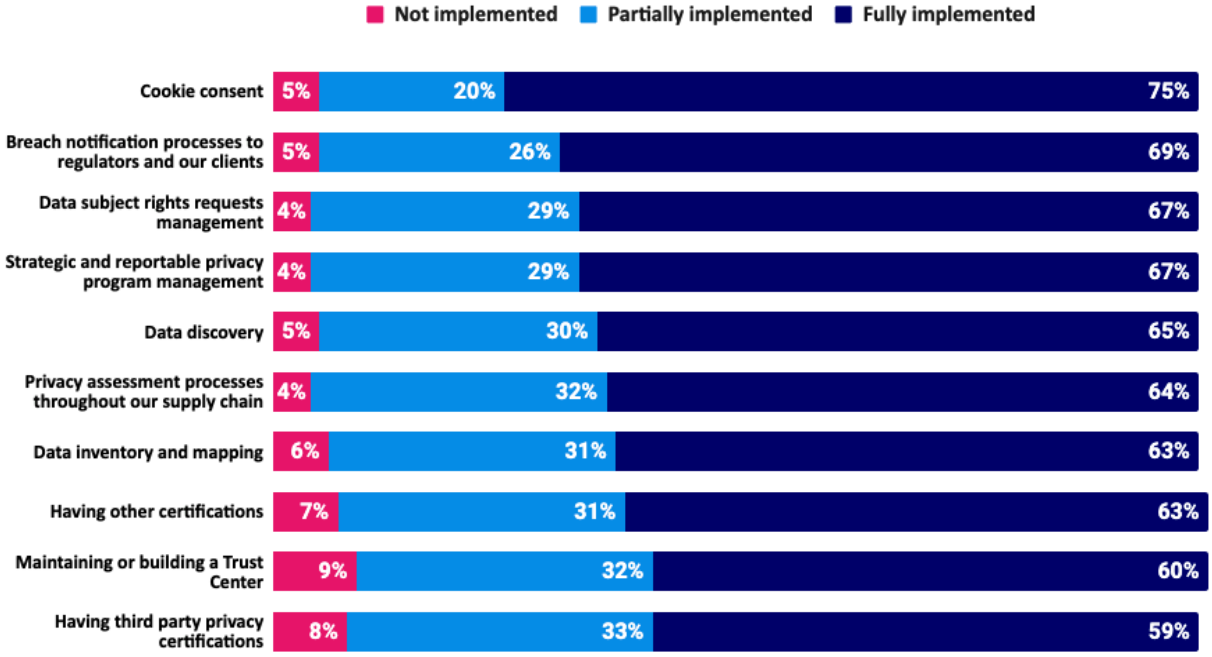


The effectiveness of purpose-built privacy solutions is clearly reflected in the performance metrics. In 2024, companies utilizing dedicated Privacy Management solutions scored, on average, 6 percentage points higher on the Privacy Index than those using GRC solutions, 11 points higher than internally developed systems, and 15 points higher than free/open-source solutions.

Looking across various implementations, not surprisingly, "cookie consent" has the highest rate of adoption and completed implementation. Breach notifications, Data Subject Requests (DSRs), and some form of strategic and reportable privacy program management follow closely. Most of these are grounded in legal or framework requirements for privacy programs (e.g., GDPR, TRUSTe Enterprise, ISO 27701).

Exhibit 22: 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")*



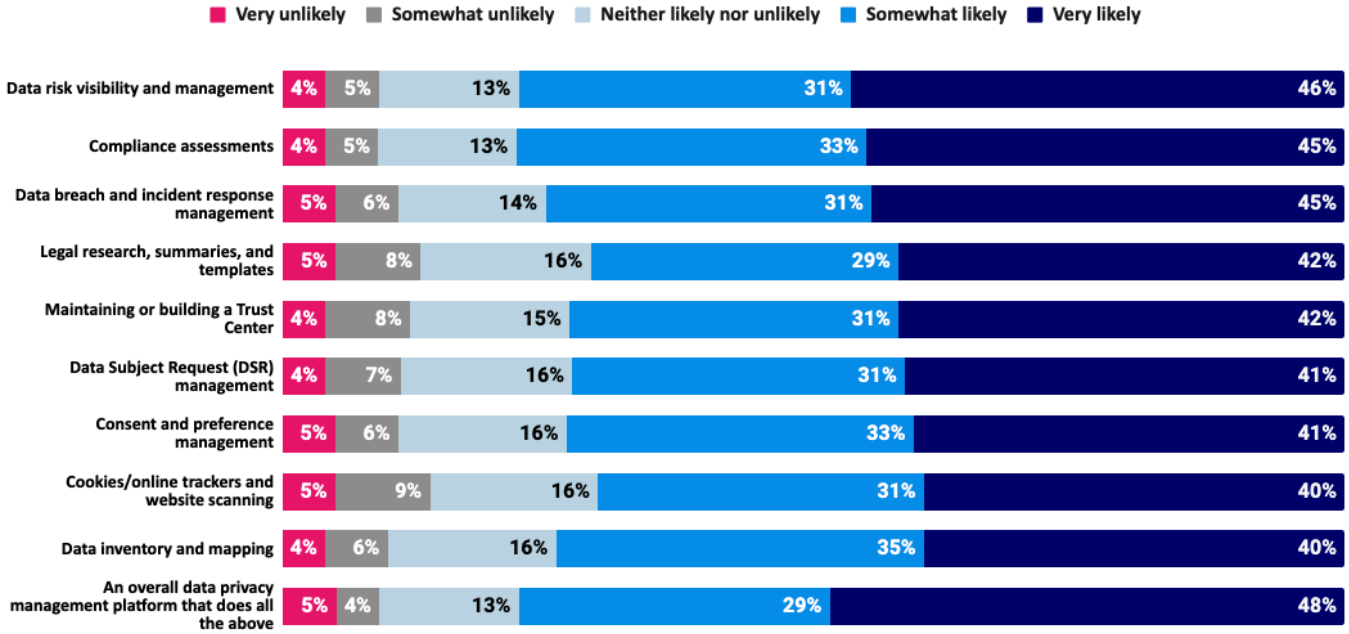
The drive towards enhancing privacy solutions remains strong, with those who have not yet invested in commercial tools indicating a high purchase likelihood in 2024. Within the next year, the top three most likely specific privacy

technology purchases will be designed for "data risk visibility and management," "compliance assessments," and "data breach and incident response management." Notably, "an overall data privacy management platform that does all of the above" would be most popular and likely to be purchased.

Exhibit 23: Likelihood to Purchase Various Privacy Products

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")

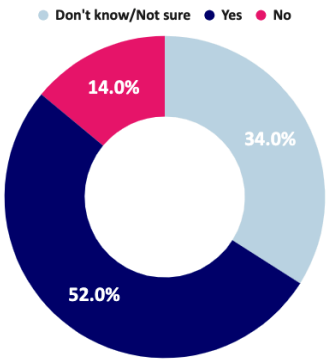


For data discovery and data scanning, while a third of respondents overall did not know if their company had one when we looked more closely at Privacy Teams (including Privacy executives), 96% claimed to know if they had one, and eight out of ten indicated they had some form of it. The most common form of scanning was for websites, SaaS, Big Data, and File/Document repositories.

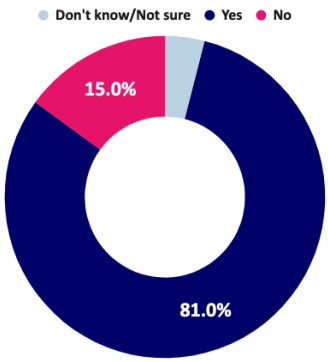
Exhibit 24: Data Scanning Solution

Has your company implemented a data discovery solution?

Overall

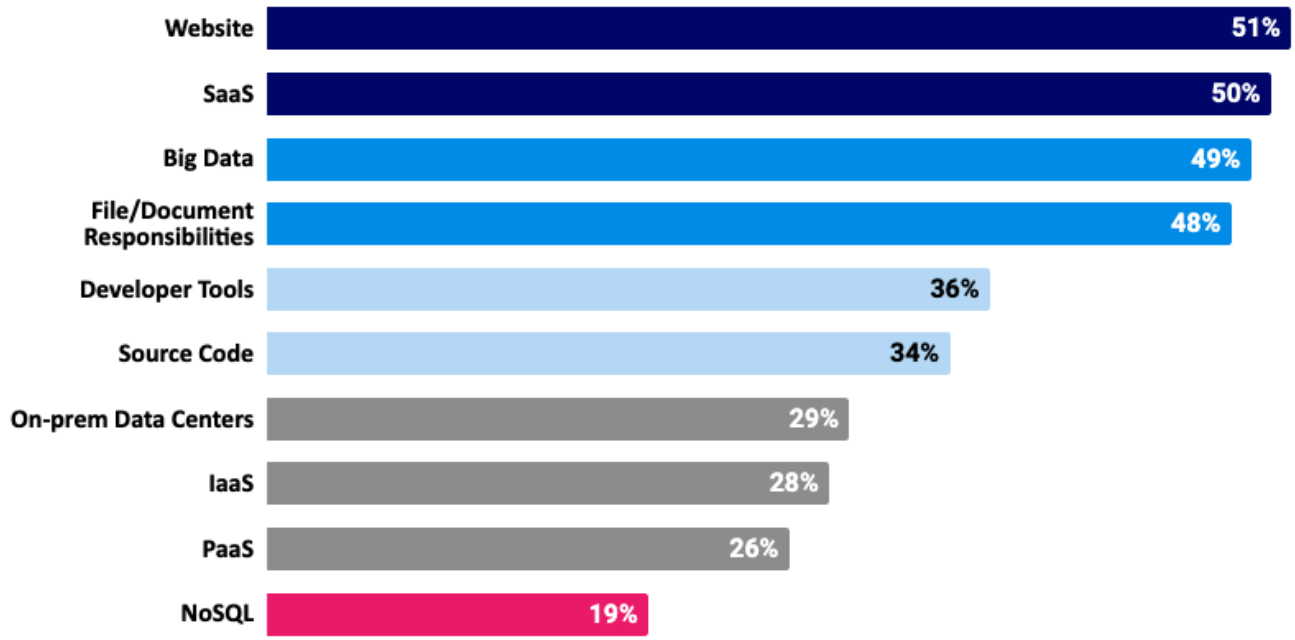


Privacy Team



What kind of data are you scanning?

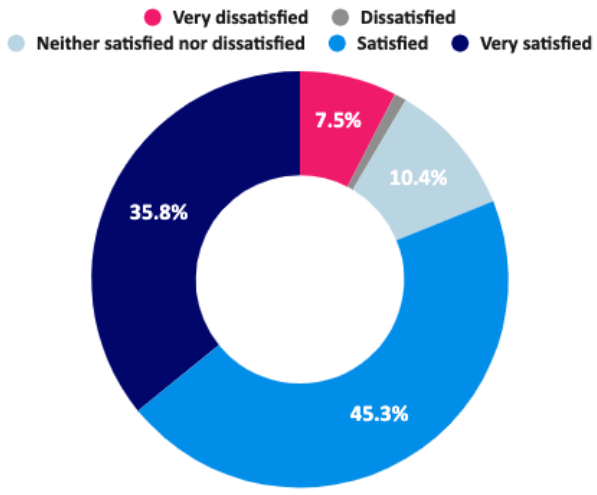
(Choose all that apply, excludes "Don't know/Not sure")



Those who had purchased a data discovery solution were by and large satisfied with it (i.e., 86% either *Satisfied* or *Very Satisfied*).

Exhibit 25: Satisfaction With Data Discovery Solution

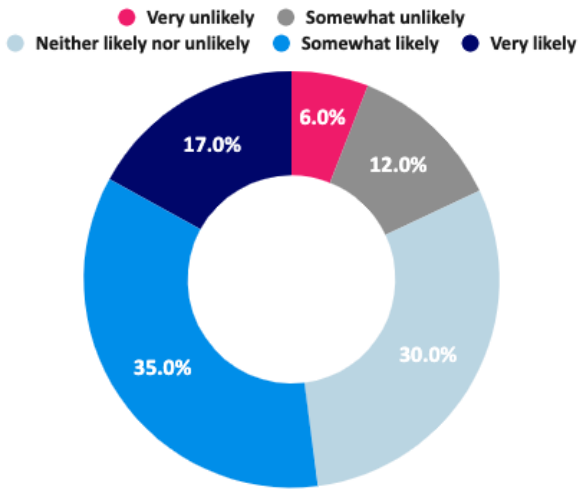
How satisfied are you with your company's data discovery solution?



Of those who did not have a solution, just over half (52%) indicated they were likely to buy a solution in 2024.

Exhibit 26: Data Discovery Purchase Likelihood

How likely is your company to purchase "made to purpose" data discovery solution?



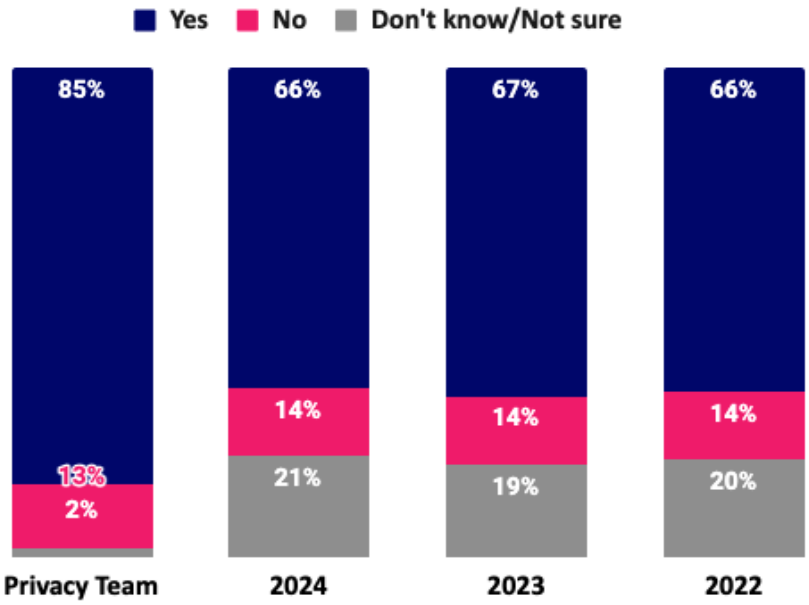
Privacy Management Measurement

In 2024, the focus on measuring privacy management effectiveness continued to be a significant area of development within the privacy domain. As privacy solutions mature and market needs evolve, more organizations recognize the importance of quantifying their privacy management to steer their programs better.

This year, the trend of measuring the effectiveness of privacy programs held steady, with two-thirds (66%) claiming their company actively measures the effectiveness of their privacy programs. Notably, one in five do not know if their company measures privacy. For companies where privacy is a priority, all employees should be aware of it and understand their contribution. Looking more closely at companies with Privacy Teams and their views on this topic, 85% indicate that their company measures privacy effectiveness.

Exhibit 27: Measuring Privacy

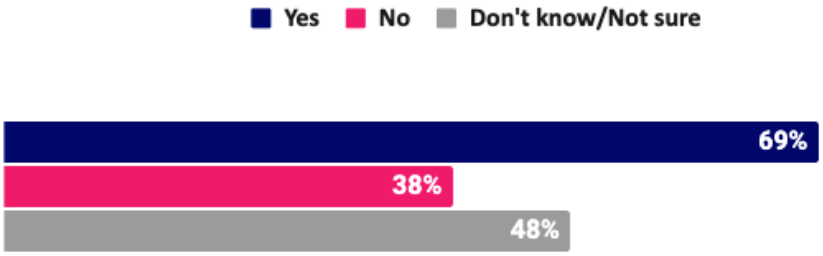
Does your company currently measure the effectiveness of its privacy program?



The data continues to underscore a significant disparity in privacy competence between organizations measuring their privacy effectiveness and those that do not. The Privacy Index scores reveal a 31-percentage point difference between these groups in 2024, further emphasizing that measurement can dramatically enhance an organization's ability to effectively manage and improve its privacy outcomes.

Exhibit 28: Privacy Index Scores by Measurement

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

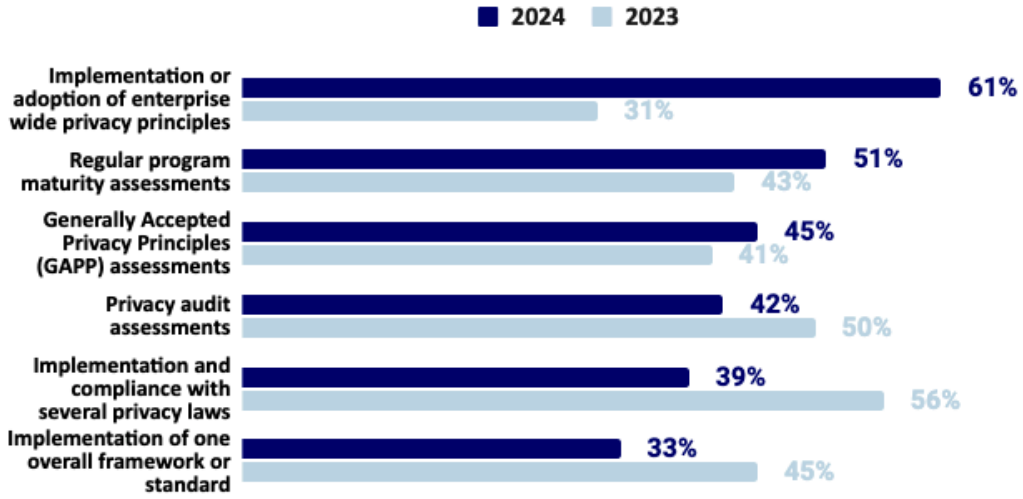


The results not only illustrate the stark differences in Privacy Index scores between companies that measure their privacy practices versus those that do not, but they also call attention to those that effectively communicate their measurement internally. Respondents who did not know or were not sure whether their company measured privacy scored 12 points lower than the average Privacy Index score (48% vs. 60%).

Organizations utilize various methods to measure their privacy programs, with the top surveyed methodology being the "implementation or adoption of privacy-wide privacy principles." With the proliferation of new privacy laws all over the globe and a significant portion of the world's population being covered by modern privacy laws by the end of 2024, it is not unexpected to see organizations begin to trend towards a broader holistic model, as seen by the top survey result. This approach appears to have gained significant traction in 2024 versus 2023. The second primary measurement method used by survey respondents was utilizing "regular program maturity assessments" akin to an "Objective and Key Result" (OKR) framework. This method provides a structured way to ensure privacy goals align with broader business objectives.

Exhibit 29: Primary Measurement Methods

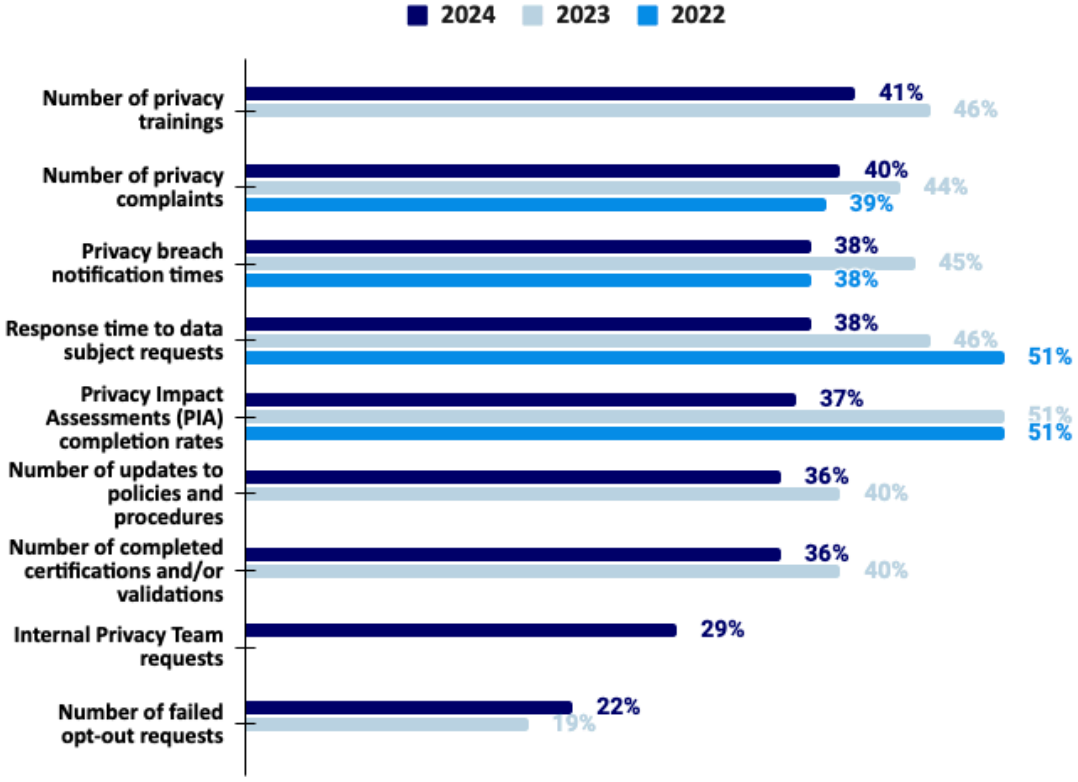
What are your company's primary methods for measuring your privacy program?



Specific KPIs related to privacy were also assessed. In 2024, an additional indicator was added, "Internal Privacy Team requests." Top among these performance measures was the "number of privacy training," followed by the "number of privacy complaints."

Exhibit 30: Privacy KPIs

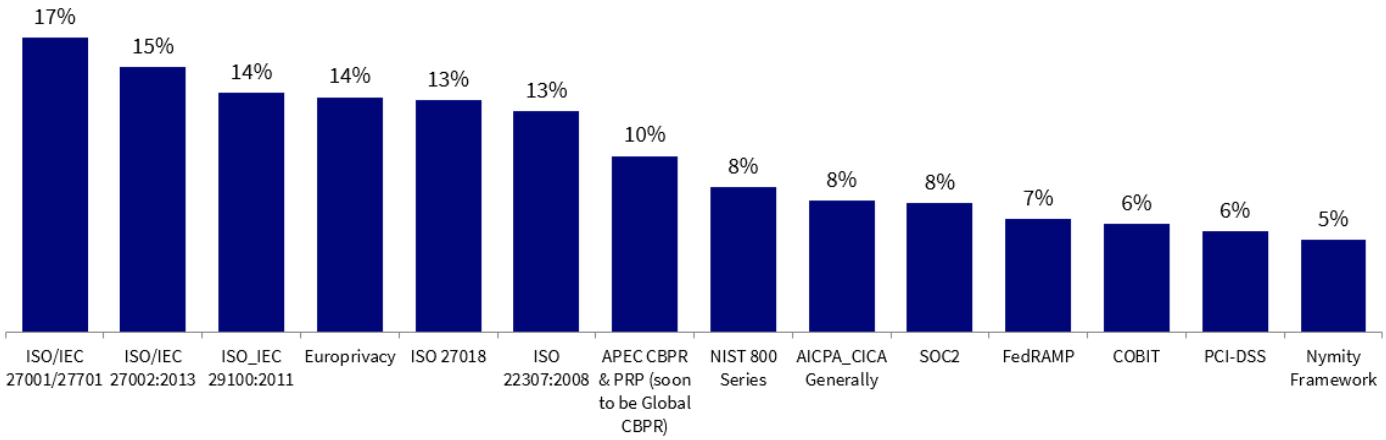
What are your company's privacy program KPI's?



The value of privacy certifications continues to be recognized, with various ISO measures being the most popularly valued certifications.

Exhibit 31: Value of Standards

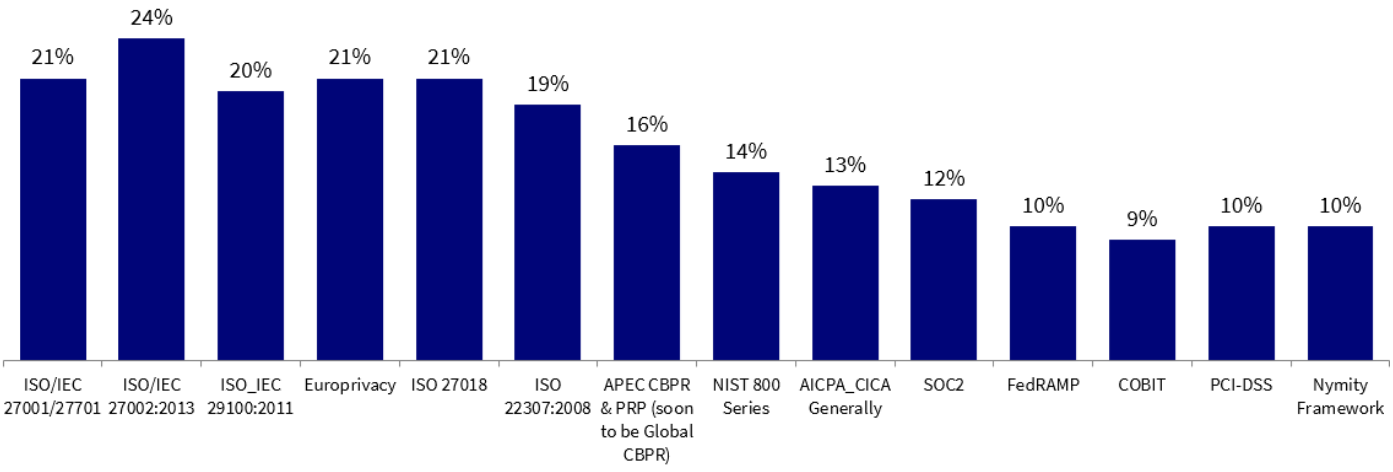
Which certification or compliance standards are most valuable to your company?



Looking more closely at the Privacy Teams views, we see higher frequencies of each certification being valued across all standards.

Exhibit 32: Value of Standards by Privacy Team

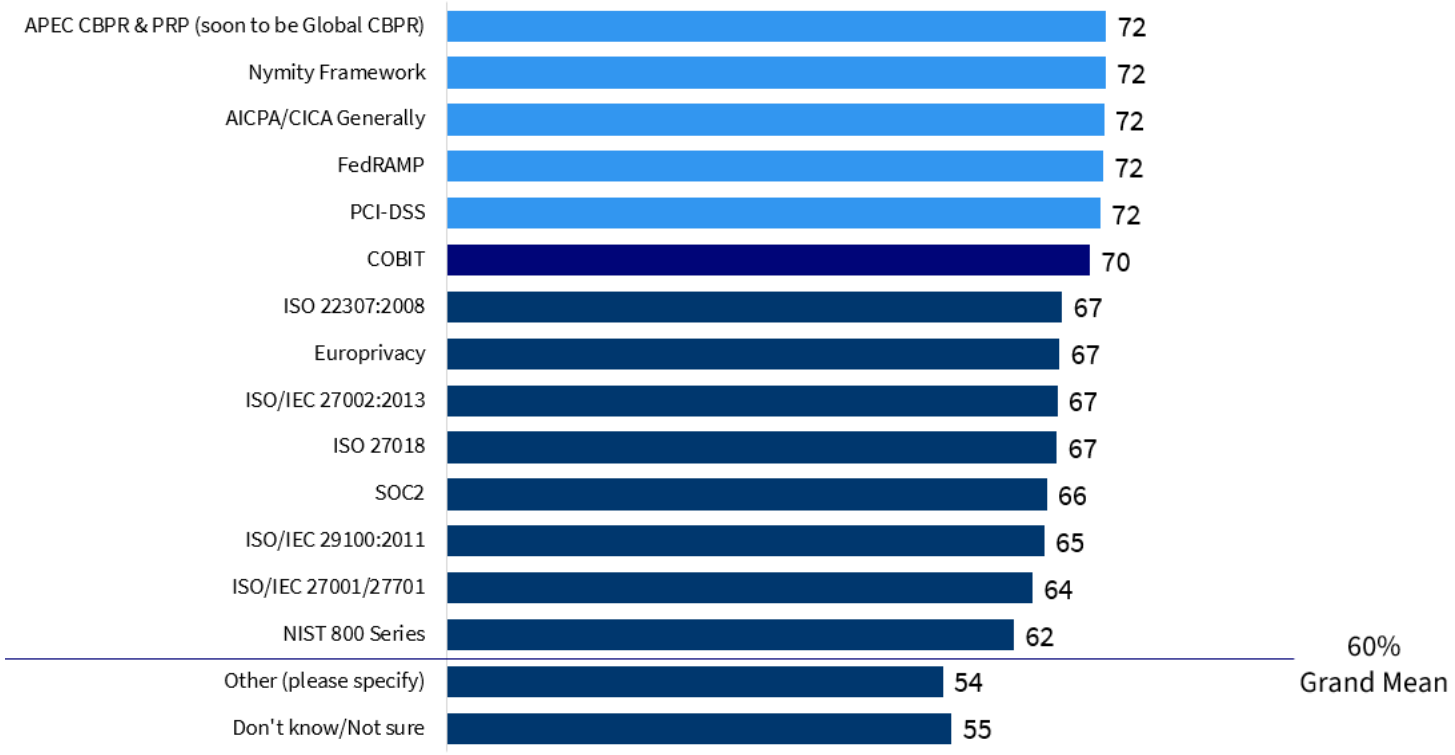
Which certification or compliance standards are most valuable to your company?



More tellingly, when we look at the TrustArc Privacy Index scores associated with each standard, it is clear that certifications that cover more comprehensive privacy aspects and have stringent compliance requirements tend to instill better privacy practices. The adoption of the Nymity Privacy Management Accountability Framework (PMAF),

while not as widespread, is associated with the highest Privacy Index scores among those who have adopted it, demonstrating its significant impact on privacy competence.

Exhibit 33: Privacy Index Scores Based on Certifications Valued



Clearly, adopting standards and certifications can help organizations achieve better privacy outcomes. TrustArc's TRUSTe Assurance certifications help organizations demonstrate compliance with various standards such as APEC CBPR/PRP and EU-US DPF.

Approach to Artificial Intelligence (AI) and AI Regulations

This year's survey highlights companies' ongoing efforts and investments in AI and their preparedness for compliance with evolving AI regulations.

In terms of AI adoption and usage as a priority, almost half (46%) claim it is either a high priority or it has already happened within their organization. For Privacy Teams, two-thirds (65%) believe it is so.

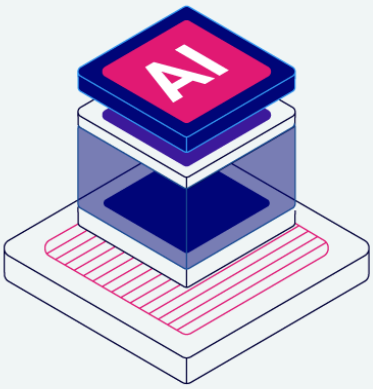
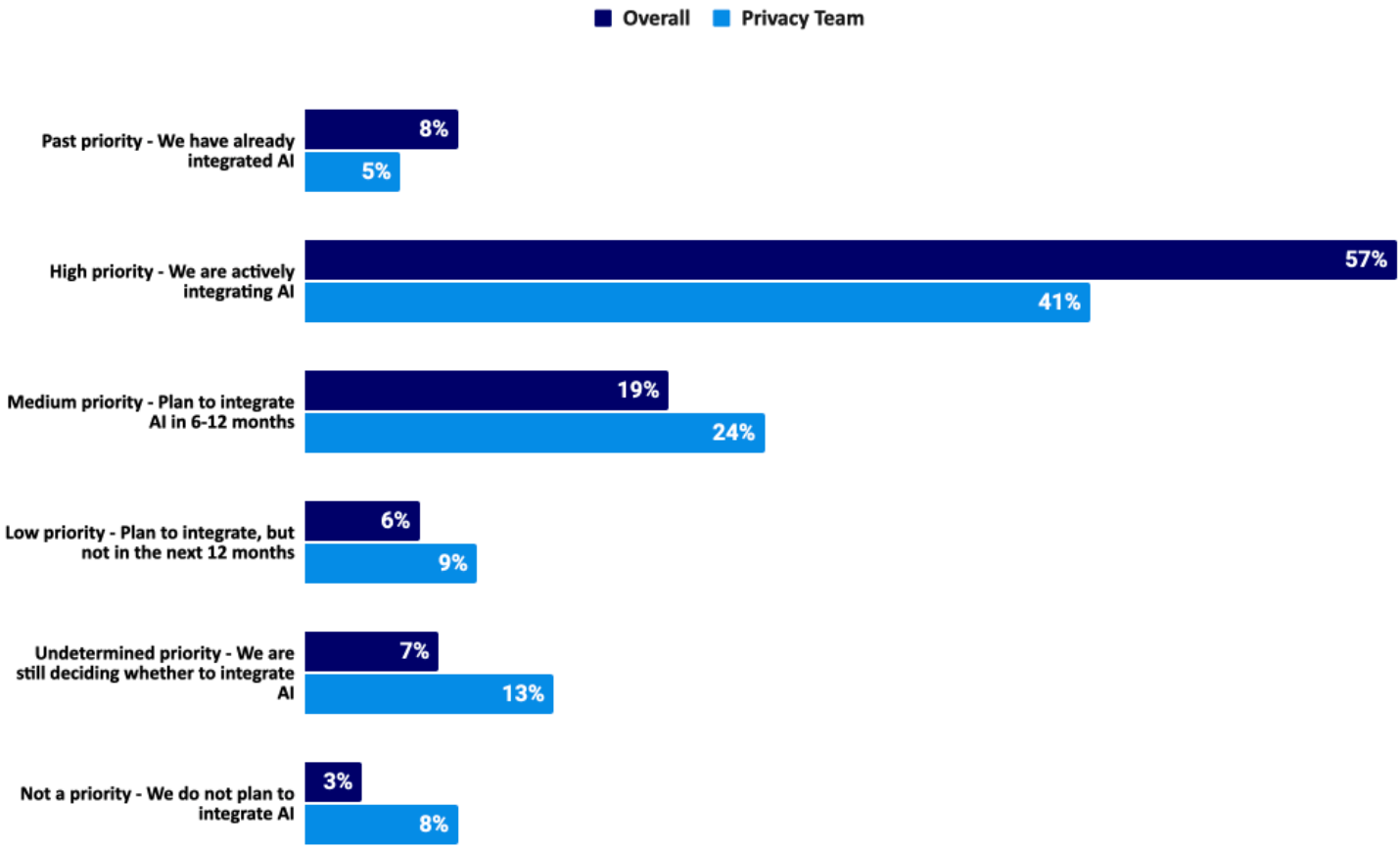


Exhibit 34: AI Priority

What is your organization's priority for integrating AI models into your products and services?

(i.e. Integrating AI services from OpenAI, Microsoft or others)



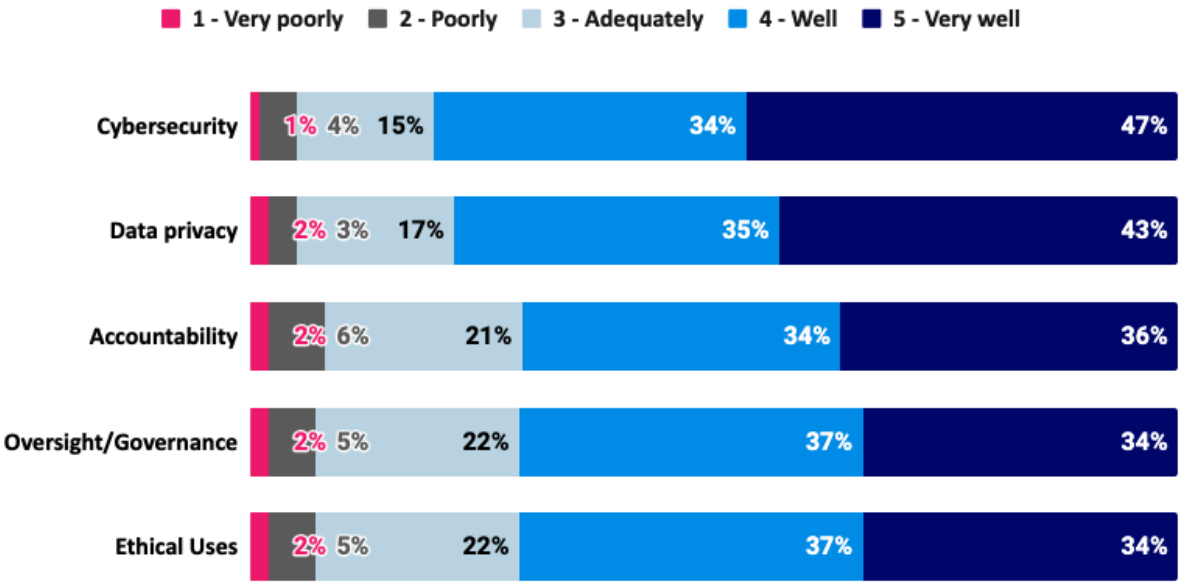
Interestingly, setting AI as a priority appears not to be associated with any carelessness toward privacy. The opposite is true. Companies that have already integrated AI into their products and services are 16 percentage points higher on the TrustArc Privacy Index vs. the average (Grand Mean) of responses; those that have it a priority are 9 points higher.

Exhibit 35: Privacy Index by AI Priority

Looking at areas important for the responsible use of AI, both cybersecurity and data privacy stand out. So aside from regulatory preparation, operational preparation runs fairly strong with most giving their companies reasonably high marks in each area of AI oversight. As part of its unique value proposition, TrustArc's Nymity Research service includes a wide array of resources and templates called "Operational Templates'', designed to aid the modern privacy and security professional – from procurement and training checklists to "plug and play" policies and procedures. Additionally, TrustArc recently updated its Operational Templates repository to include several AI-specific policies, procedures, and checklists to aid clients in responsibly managing their AI programs while mitigating potential privacy and security risks associated with AI adoption.

Exhibit 36: Meeting AI Requirements

Below is a list of areas important for the responsible use of AI. On a scale of 1 to 5, please rate how well you believe your company is meeting these AI requirements?

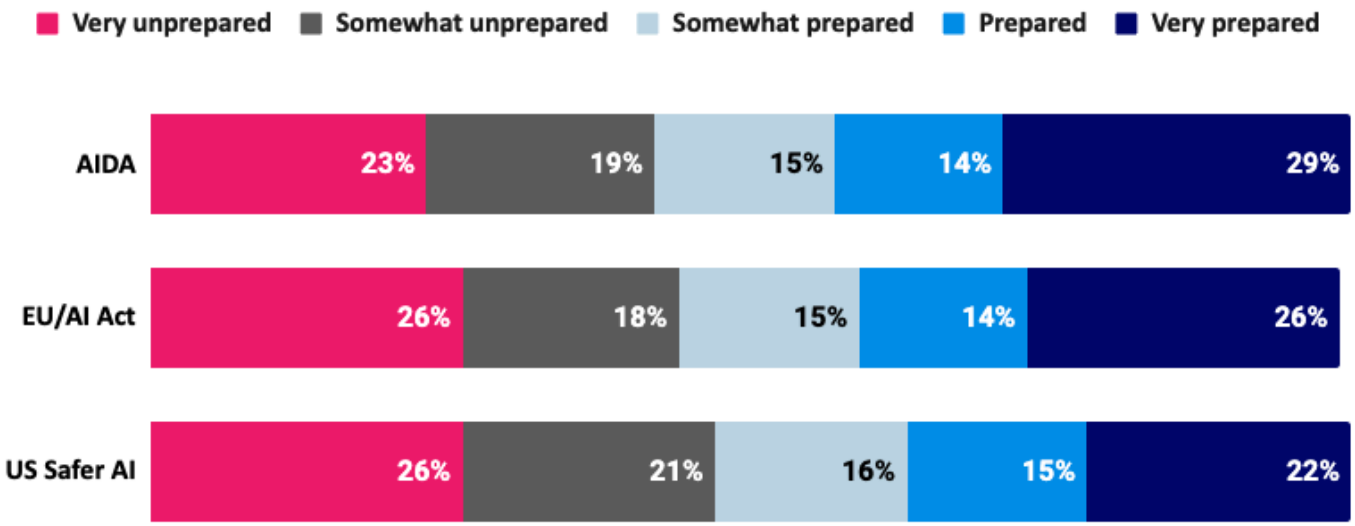


Respondents were asked about their perceived levels of preparedness for the various regulations being put in place (rating only those that apply to their company). Respondents from companies that operate in Canada reported the highest level of preparation (43% *prepared* or *very prepared*). Across all anticipated AI regulations and guidelines, about as many companies are prepared as there are companies unprepared. Navigating evolving privacy laws, guidelines, and emerging technology laws around AI globally can be done easily and cost-effectively with tools like TrustArc's Nymity Research and NymityAI.

Exhibit 37: Preparations for AI Regulations

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

(Excludes "Does not apply" and "Don't know/Not sure")



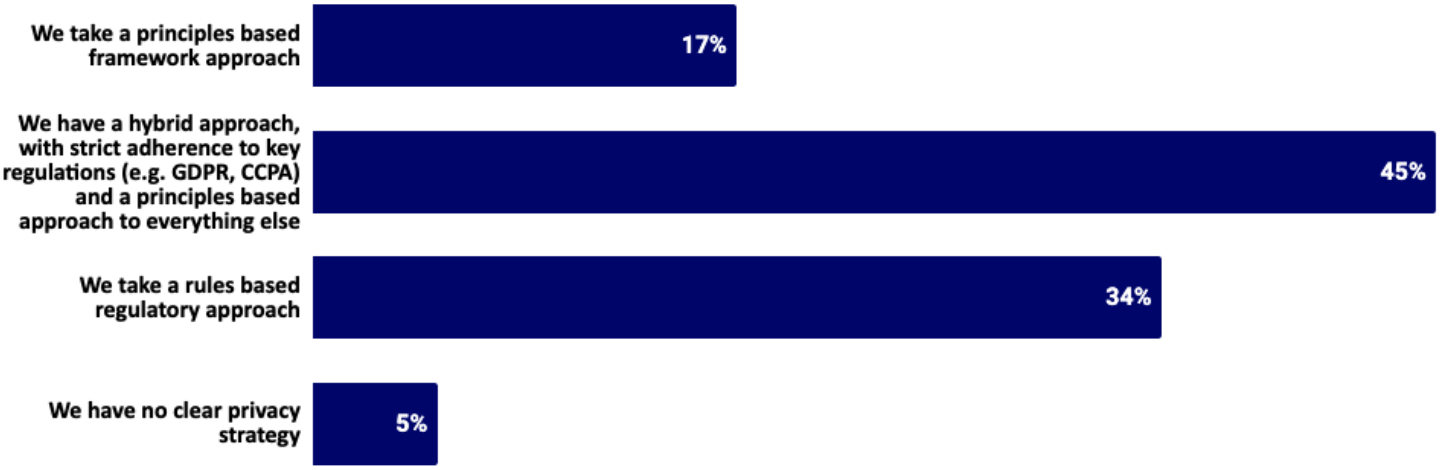
Regulatory Approach

Rounding out the results from the 2024 study, participants were asked what approach their company took toward privacy in terms of regulations – particularly whether or not they had a strategy and, if so, whether it was primarily focused on strict adherence to a particular legal framework, primarily focused on a "framework" or "values"-based approach (e.g., a privacy "Northstar"-type viewpoint), or a hybrid approach (taking the best of both worlds).

By far the most popular approach was hybrid, with strict adherence to two regulatory mainstays (GDPR and CCPA) and a principles-based approach to others. This approach was followed by strict adherence to the rules of all applicable regulations. Only half as many again, stated that their company took a principles-based approach. Lastly, only one in twenty (5%) claimed to have no clear privacy strategy.

Exhibit 38: Approach to Regulations

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



While these findings were not surprising, what was remarkable was how the approach taken correlated with the Global Privacy Index scores. On the negative side, having no clear privacy strategy was associated with a dismal score of just 11 (again, with a reminder that scores could range from -100 through 0 to 100, with the overall average being 60 in 2024). A strict rules-based approach was not associated with success, falling below average, versus a hybrid approach associated with a moderately higher score than average. What was remarkable was that a purely Principles-based approach to privacy netted an average Global Privacy Index score of 14 points above average (74).

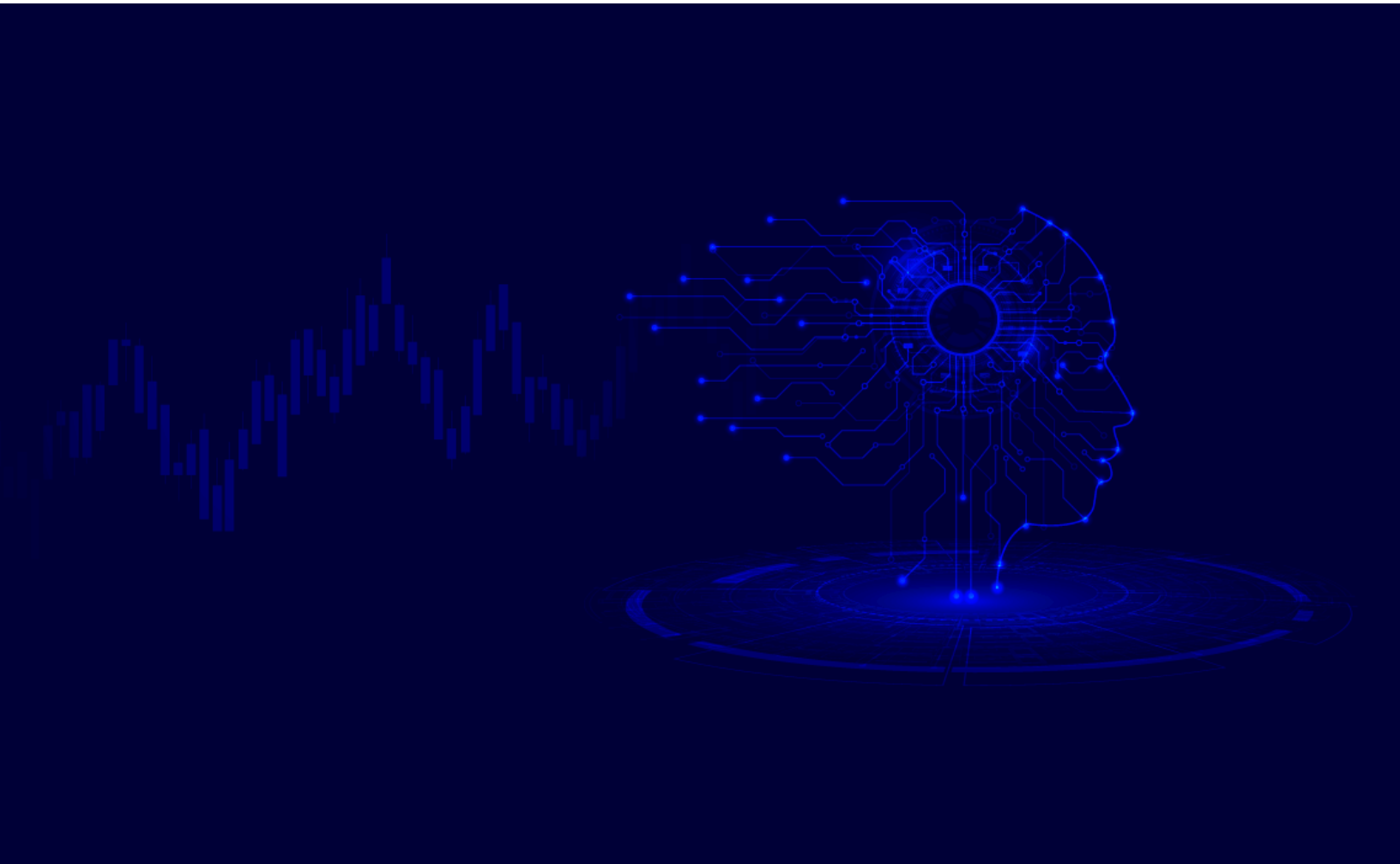
Exhibit 39: Privacy Index by Regulatory Approach

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

Conclusion

In 2024, it is clear that the landscape of privacy management is both challenging and dynamic. The high prioritization of AI, the onset of AI regulatory environments, and the crucial emphasis on data security underscores the complexities that privacy professionals face. Notably, the survey highlights a significant improvement in privacy competencies globally, with an increase in the TrustArc Global Privacy Index. This finding suggests that companies are not only recognizing the importance of robust privacy strategies but are effectively integrating these practices into their core operations. Moreover, the success seen in adopting a principles-based approach, particularly those utilizing the Nymity Privacy Management Accountability Framework (PMAF), underscores its effectiveness in fostering superior privacy practices that resonate with comprehensive compliance and operational excellence.

The findings from this survey serve as a crucial barometer for the state of privacy management across industries. The increasing reliance on sophisticated privacy management solutions indicates a move towards more systematic and integrated approaches. Yet, the stark differences in privacy competencies between companies that actively measure and manage their privacy effectiveness and those that do not call for a broader adoption of strategic measurement tools. For organizations aiming to maintain or improve their privacy posture, the path forward involves continuously re-evaluating their privacy frameworks, operational commitment to regular training and awareness programs, and a strategic and holistic approach that embraces privacy from the front line to the Boardroom. As the digital landscape evolves, so must the strategies that govern privacy, including providing and adopting privacy software and certifications.



About TrustArc

As the leader in data privacy, TrustArc automates and simplifies creating end-to-end privacy management programs for global organizations. TrustArc is the only company to deliver the depth of privacy intelligence, coupled with the complete platform automation essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk, and build trust. For additional information, visit TrustArc.com.

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.

US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com