



ANNUAL REPORT

The Global State of Privacy Compliance Across the Digital Experience Layer

Insights from 800 Privacy, Security and GRC Leaders Across the United States, United Kingdom, Australia and UAE



Contents

Executive Summary

Prologue	3
Findings at a Glance	4
The Current State of Privacy Compliance Across the Digital Experience Layer	5

Research Findings

Chapter 1. The Third-Party Script Landscape	
Organizations Can't Govern What They Can't Continuously See	6
Chapter 2. Consent Doesn't End with a Banner	
Deploying a Consent Management Platform Does Not Guarantee Compliance	12
Chapter 3. The Vendor Accountability Gap	
Organizations Remain Responsible for Behaviors They Cannot Always Observe	18
Chapter 4. When Compliance Becomes Evidence	
Privacy Compliance Is Increasingly Measured by What Organizations Can Prove	24
Chapter 5. The Operational Maturity Gap	
Mature Privacy Programs Still Face Significant Execution Challenges	29
Chapter 6. The Shift to Continuous Compliance	
Organizations Are Redefining How Privacy Compliance Is Managed	36

Looking Ahead

The Next Era of Privacy Compliance	41
--	----

Methodology

Research Objectives	42
Survey Methodology	42
Respondent Profile	43
About the Findings	43

About Feroot	44
--------------------	----

Prologue

For the inaugural edition of The Global State of Privacy Compliance Across the Digital Experience Layer, Feroot partnered with independent research consultancy Censuswide to better understand how organizations are managing one of today's fastest-evolving areas of privacy and compliance.

Over the past decade, organizations have invested heavily in privacy programs, consent management technologies, governance frameworks, and regulatory expertise. At the same time, websites and mobile applications have become increasingly dependent on third-party technologies, creating new challenges in maintaining visibility into how customer data is collected, processed, and shared. While consent management platforms, privacy programs, and governance processes have become standard practice, many organizations continue to face challenges validating that these controls operate as intended across increasingly dynamic production environments.

To better understand the current state of digital experience privacy, Censuswide surveyed 800 senior privacy, governance, risk, compliance, and security leaders across the United States, United Kingdom, Australia, and the United Arab Emirates.

The research explores how organizations manage third-party technologies, validate consent enforcement, govern

vendor risk, prepare for regulatory scrutiny, and plan future investments in digital privacy compliance.

Unlike many industry reports that focus primarily on regulatory requirements or emerging legislation, this research examines what is actually happening across the Digital Experience Layer—the collection of client-side technologies, third-party services, embedded applications, and digital interactions that power modern websites and mobile applications. By examining how organizations govern this increasingly complex environment, the report provides insight into where privacy programs have matured, where operational challenges remain, and how organizations are evolving their approach to continuous privacy compliance.

The findings throughout this report suggest that organizations increasingly understand what effective privacy governance requires. The challenge they now face is operationalizing that governance across digital environments that continuously evolve. As you read through the report, we hope you'll gain a clearer understanding of the current state of privacy compliance across the Digital Experience Layer, the operational realities organizations face, and the strategies privacy leaders are adopting to strengthen visibility, governance, and compliance in an increasingly dynamic digital ecosystem.

CENSUSWIDE
+
THE RESEARCH CONSULTANTS

Findings at a Glance

The Digital Experience Layer has become one of the most dynamic—and operationally challenging—areas of privacy compliance. Modern websites and mobile applications rely on dozens of third-party technologies, scripts, embedded services, and digital interactions that continuously collect, process, and transmit user data. As these environments grow more complex, organizations are finding it increasingly difficult to maintain visibility, validate consent enforcement, govern vendor behavior, and demonstrate compliance.

To better understand how organizations are responding, Ferroot commissioned an independent survey of 800 senior privacy, governance, risk, compliance, and security leaders across the United States, United Kingdom, Australia, and the United Arab Emirates. The findings reveal an important shift: organizations have largely established privacy programs, consent management infrastructure, and governance frameworks, but many continue to face challenges operationalizing privacy compliance across continuously evolving digital environments.

Key Findings

84%

operate more than ten third-party technologies.

89%

have experienced vendors changing data collection practices without notification.

24%

continuously verify consent controls.

63%

report their client-side privacy teams are under-resourced.

75%

say at least half of their client-side privacy work remains manual.

97%

plan to evaluate privacy automation tools.

Bottom Line

The findings reveal a growing gap between privacy governance and operational execution. While organizations have invested heavily in consent management, governance frameworks, and privacy programs, many continue to face challenges maintaining visibility, validating controls, and demonstrating compliance across rapidly changing digital environments.

Closing that gap will require a shift from periodic assessments and manual processes toward continuous visibility, verification, and operational evidence across the Digital Experience Layer.

The Current State of Privacy Compliance Across the Digital Experience Layer

Privacy compliance has traditionally focused on policies, consent notices, vendor contracts, and regulatory obligations. While these remain foundational elements of a strong privacy program, they provide only part of the picture.

Today's digital experiences are powered by an increasingly complex ecosystem of third-party technologies. Analytics platforms, advertising networks, content delivery services, payment processors, customer support tools, personalization engines, embedded media, and AI-powered applications all contribute code that executes within the user's browser. Together, these technologies form the Digital Experience Layer—the client-side environment where data is collected, processed, and shared in real time.

Unlike internal systems, the Digital Experience Layer is constantly changing. Marketing teams launch new campaigns, developers introduce new features, vendors update software development kits (SDKs), and third-party providers modify how their technologies collect or transmit data. These changes can occur daily, often without the knowledge of privacy or security teams.

This dynamic environment presents a new challenge for privacy leaders. Organizations are no longer expected

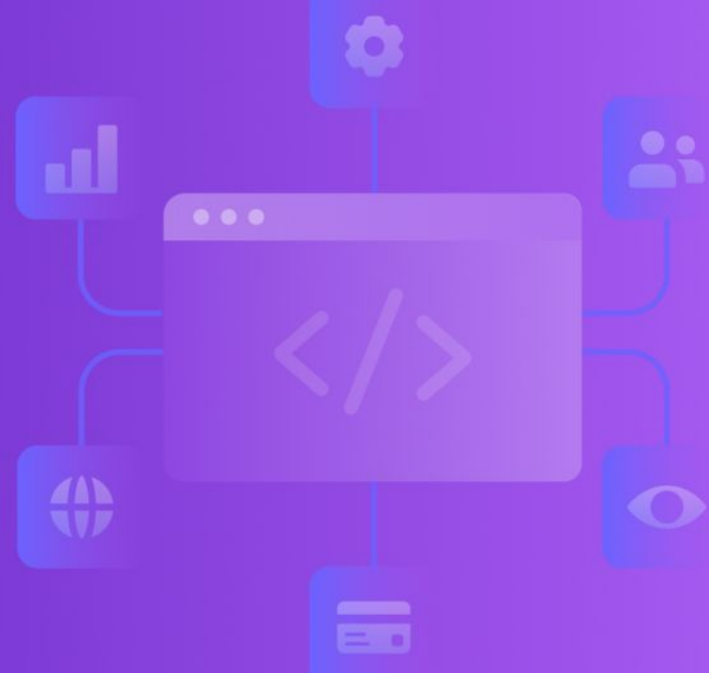
simply to publish privacy policies or deploy consent management platforms. Increasingly, regulators expect organizations to understand—and be able to demonstrate—what is actually happening across their digital properties.

That expectation represents a fundamental shift in privacy compliance. Rather than relying on periodic assessments or manual reviews, organizations must continuously verify that third-party technologies behave as intended, consent preferences are honored, and new risks are identified before they become compliance issues.

The findings in this report suggest many organizations are still adapting to this new reality. While privacy programs have matured significantly over the past decade, operational visibility has not always kept pace with the growing complexity of the Digital Experience Layer.

The chapters that follow examine six critical areas shaping modern privacy compliance: the growing complexity of third-party scripts, confidence in consent management platforms, vendor governance, regulatory enforcement, organizational maturity, and the increasing shift toward continuous monitoring and automation.

The Third-Party Script Landscape



Organizations Can't Govern What They Can't Continuously See

Modern digital experiences are no longer built solely by the organizations that own them.

Every customer interaction on a website or mobile application is shaped by an ecosystem of third-party technologies operating behind the scenes. Analytics platforms, advertising networks, payment providers, customer support tools, content delivery networks, embedded media, personalization engines, fraud prevention technologies, and increasingly, AI-powered services all execute code within the user's browser. While these technologies enable richer digital experiences and support business objectives, they also create an increasingly complex environment for privacy, security, and compliance teams to govern.

This complexity represents one of the most significant shifts in modern privacy compliance.

Unlike traditional enterprise systems, the Digital Experience Layer is highly dynamic. New technologies are deployed to support marketing campaigns, vendors update software development kits (SDKs), website features are modified, and third-party services change how they collect and process data. These changes can occur daily, often without the direct involvement—or awareness—of privacy and security teams.

As a result, organizations face a fundamental challenge: **How can you govern what you cannot continuously see?**

Our research suggests that many organizations are still struggling to answer that question.

Third-Party Ecosystems Have Become Increasingly Complex

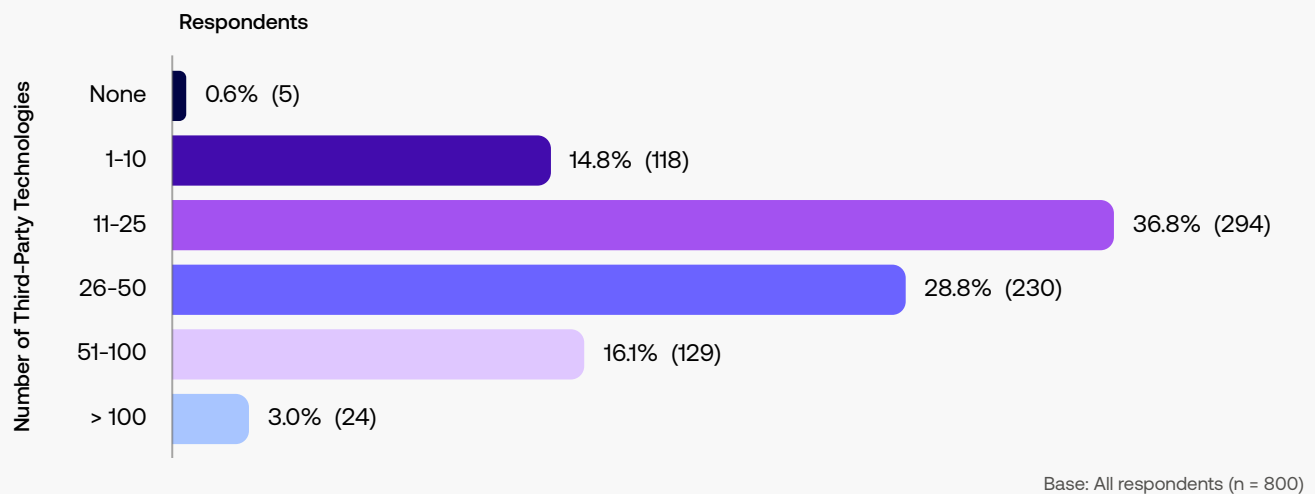
Third-party technologies have become foundational to modern digital experiences. Nearly every organization surveyed reported relying on external technologies to support customer experiences, analytics, payments, advertising, personalization, and other business-critical functions.

The survey found that organizations manage an average of 33.6 third-party technologies across their customer-facing digital properties, including public websites, web applications, customer portals, and mobile applications.

FIGURE 1

Organizations Manage Large Third-Party Technology Ecosystems

Survey Question: How many third-party vendors, if any, have scripts actively running on your websites right now? (analytics, advertising, chat, session replay, A/B testing, etc.)



These findings highlight an important reality: privacy compliance is no longer about governing a single website or application. It is about governing a continuously evolving ecosystem of technologies, vendors, and data flows.

As organizations expand their digital experiences, every additional third-party technology introduces another potential source of data collection, another vendor relationship to manage, and another compliance obligation to monitor.



Key Insight

Modern digital experiences are no longer built by a single organization. They are assembled from dozens of independently managed technologies, creating a level of operational complexity that traditional privacy governance models were never designed to address.

Maintaining Visibility Across Digital Experiences Remains Challenging

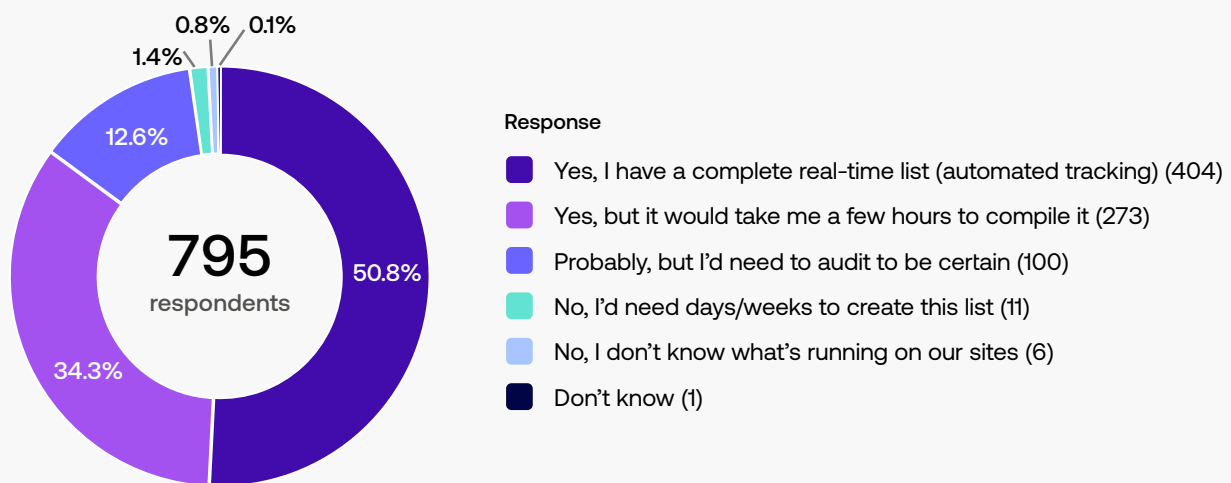
While organizations increasingly recognize the importance of maintaining a complete inventory of third-party technologies, many continue to rely on processes that are difficult to maintain as digital environments grow more complex.

When asked how quickly they could produce a complete inventory of technologies operating across their websites, only half of respondents reported having immediate visibility into their digital environment.

FIGURE 2

Real-Time Visibility Into Third-Party Technologies Remains Limited

Survey Question: *Could you list, right now, ALL third-party scripts currently collecting data on your organisation's websites*



Base: All respondents (n = 795)
 **. "Conduct an audit" refers to performing a manual or technical review to identify and inventory technologies that are not already tracked through a continuously maintained inventory.

While these findings suggest that many organizations have invested in inventory management processes, they also reveal that nearly half of organizations cannot immediately identify every technology operating within their digital environment.

This visibility gap presents a significant challenge for privacy teams. Marketing teams launch campaigns, vendors update scripts, agencies deploy new technologies, and developers release new functionality on a continuous basis. Maintaining an accurate inventory through periodic reviews or manual processes becomes increasingly difficult as digital ecosystems grow more dynamic.

The challenge is not necessarily a lack of governance effort. Rather, it reflects the reality that digital environments often evolve faster than traditional governance processes can adapt.

Unauthorized Script Activity Has Become a Routine Operational Challenge

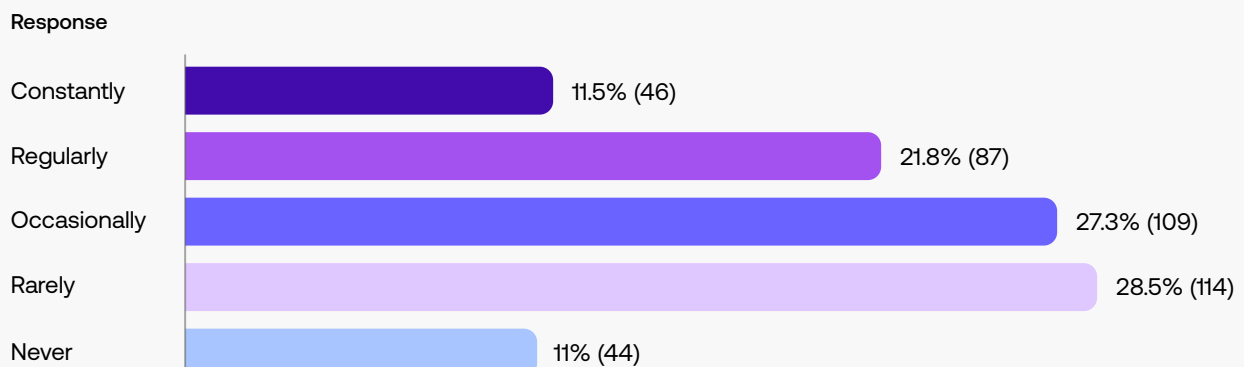
The complexity of modern digital experiences means that unauthorized or unrecognized technologies are no longer rare occurrences.

Our research found that unauthorized script activity is a routine operational reality for most organizations. Most organizations reported discovering unauthorized technologies operating within their digital environments, with 60.6% experiencing such discoveries at least occasionally.

FIGURE 3

Unauthorized Script Discovery Is a Frequent Occurrence

Survey question: How often, if ever, do you discover unauthorised or undocumented tracking scripts ALREADY running on your websites?



Base: Persona 1 respondents (n = 400). Percentages may not total exactly 100% due to rounding.

Combined, 60.6% of organizations discover unauthorized technologies either occasionally, regularly, or constantly, suggesting that unexpected data collection activity has become an expected operational condition rather than an isolated compliance failure.

Unauthorized technologies can appear for many reasons. Vendors may modify existing services, marketing teams may deploy new tools, agencies may introduce tracking technologies, or development teams may implement new functionality without triggering formal privacy review processes.

For privacy leaders, the challenge is increasingly not whether governance policies exist, but whether those policies continue to be followed after technologies have been deployed.



Key Insight

Unauthorized script discovery should not be viewed as evidence of isolated compliance failures. Rather, it reflects the growing operational complexity of governing continuously changing digital environments.

Organizations Continue to Discover Compliance Issues Reactively

Perhaps the most important finding in this chapter is not how often organizations discover unauthorized technologies, but how those discoveries occur.

Many organizations continue to rely on manual reviews, periodic assessments, external notifications, and reactive investigations to identify unauthorized data collection activity. Relatively few organizations employ continuous monitoring approaches capable of identifying issues as they emerge.

This creates a significant gap between organizational accountability and operational visibility.

In an ideal environment, organizations would identify unauthorized technologies internally, investigate root causes, and remediate issues before they impact customers or attract regulatory attention. Instead, many organizations remain dependent on reactive discovery methods that identify problems only after they have already occurred.

The implications extend beyond privacy compliance. Delayed visibility increases operational burden, extends remediation timelines, and reduces organizations' ability to demonstrate proactive governance during regulatory inquiries.



Why This Matters

Organizations that discover unauthorized data collection activity only after it has occurred lose the opportunity to proactively mitigate compliance risk. As digital ecosystems become increasingly dynamic, continuous visibility is becoming a foundational requirement for privacy governance.

Regional Spotlight: United States

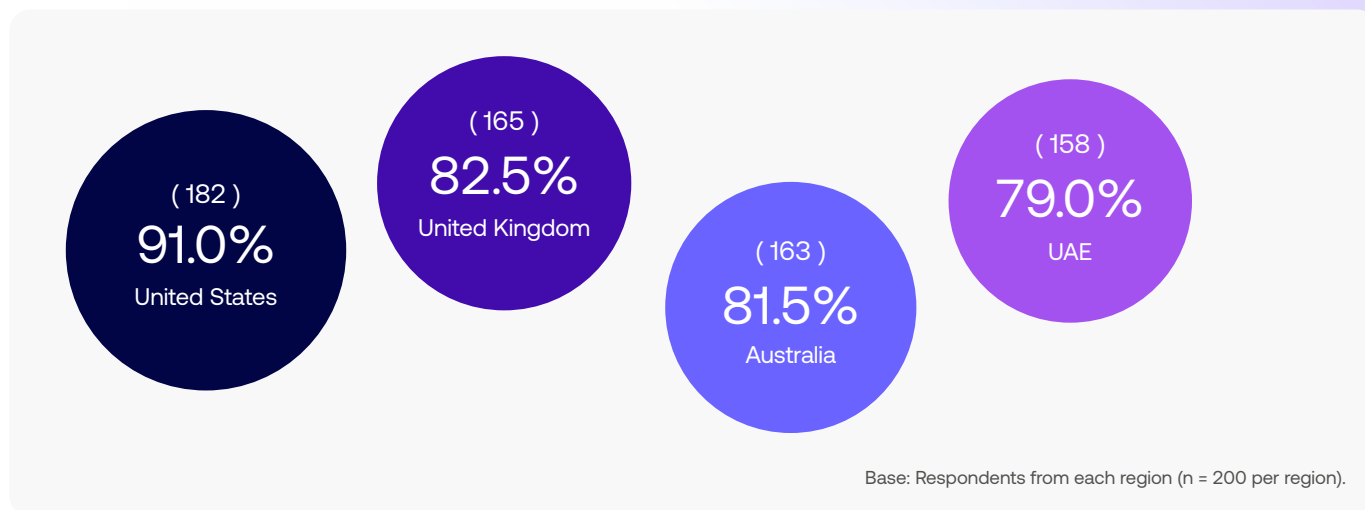
Organizations Across All Regions Manage Complex Third-Party Ecosystems

While organizations across all regions surveyed reported managing increasingly complex digital environments, respondents in the United States were most likely to report operating more than ten third-party technologies across their websites and digital properties (91.0%). Organizations in the United Kingdom (82.5%), Australia (81.5%), and the UAE (79.0%) also reported high levels of digital ecosystem complexity.

These findings suggest that the challenge of maintaining visibility into third-party technologies is not limited to a specific geography or regulatory framework. Rather, it reflects the broader reality that modern digital experiences increasingly rely on large and continuously evolving ecosystems of vendors, scripts, and embedded services.

FIGURE 4

Organizations Operating More Than Ten Third-Party Technologies



What These Findings Mean

The findings in this chapter suggest that the challenge facing privacy teams is no longer understanding regulatory requirements or establishing governance policies. Rather, the challenge is maintaining continuous visibility into digital environments that evolve every day.

Organizations continue to add technologies faster than traditional governance processes can inventory, validate, and monitor them. As a result, many organizations operate in environments where unauthorized data collection activity is not an exception—it is an expected operational condition.

Perhaps most importantly, the data reveals a growing gap between internal visibility and external accountability. While organizations remain legally responsible for the behavior of technologies operating on their websites and applications, many continue to rely on periodic assessments and reactive discovery methods to identify compliance issues.

As digital experiences continue to grow in complexity, visibility itself is becoming a foundational requirement for privacy compliance.



Key Takeaway

Privacy begins with visibility. Organizations cannot govern what they cannot continuously see.

Consent Doesn't End with a Banner



Deploying a Consent Management Platform Does Not Guarantee Compliance

Over the past decade, consent management platforms (CMPs) have become foundational components of digital privacy programs.

Driven by regulations such as GDPR, CCPA/CPRA, and an increasing number of global privacy laws, organizations have invested heavily in technologies designed to collect, manage, and communicate user consent preferences. For many organizations, implementing a CMP has become synonymous with implementing digital privacy controls.

However, collecting consent and enforcing consent are fundamentally different challenges.

While consent management platforms play an important role in modern privacy programs, they operate within increasingly complex digital ecosystems containing dozens of third-party technologies, embedded services, marketing platforms, and external vendors. As these ecosystems grow more dynamic, ensuring that every technology consistently honors user consent preferences becomes significantly more difficult.

The findings from this research suggest that organizations have largely solved the challenge of collecting consent. The next challenge is continuously verifying that consent choices are actually being enforced.

Consent Management Platforms Have Become Standard Privacy Infrastructure

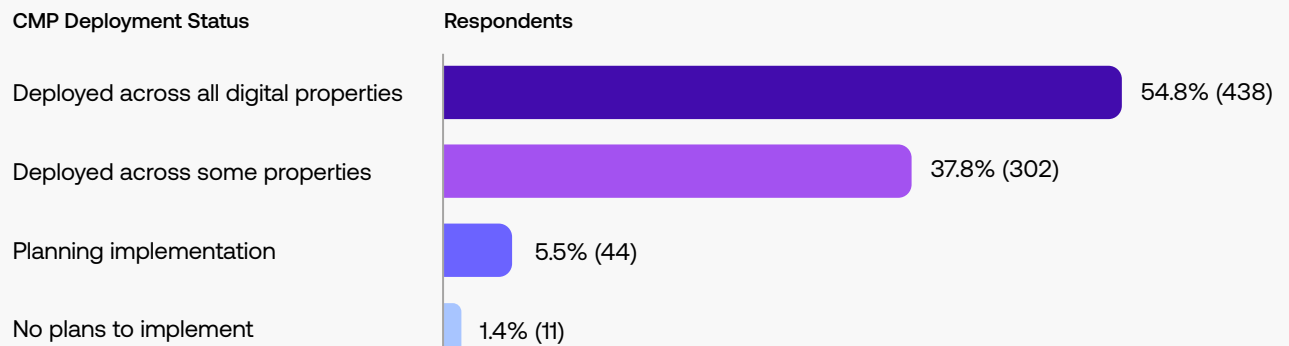
Consent management platforms have achieved near-universal adoption among organizations managing digital experiences.

Our research found that more than nine out of ten organizations have deployed a consent management platform across at least some portion of their digital properties. However, implementation maturity varies significantly, with many organizations continuing to operate hybrid environments where consent controls are applied inconsistently.

FIGURE 5

Consent Management Platforms Have Achieved Widespread Adoption

Survey question: Does your organization use a cookie consent management platform (CMP)?



Base: All respondents (n = 800).

In total, 98.1% of organizations have or plan to implement consent management technology, highlighting the extent to which consent management has become standard privacy infrastructure.

These findings suggest that the challenge facing organizations is no longer whether to deploy consent management technologies. Rather, the challenge is ensuring those technologies continue to function as intended within increasingly dynamic digital environments.



Key Takeaway

The question is no longer whether organizations have implemented consent management. The question is whether they can prove that consent preferences are being enforced.

Verification of Consent Enforcement Remains Limited

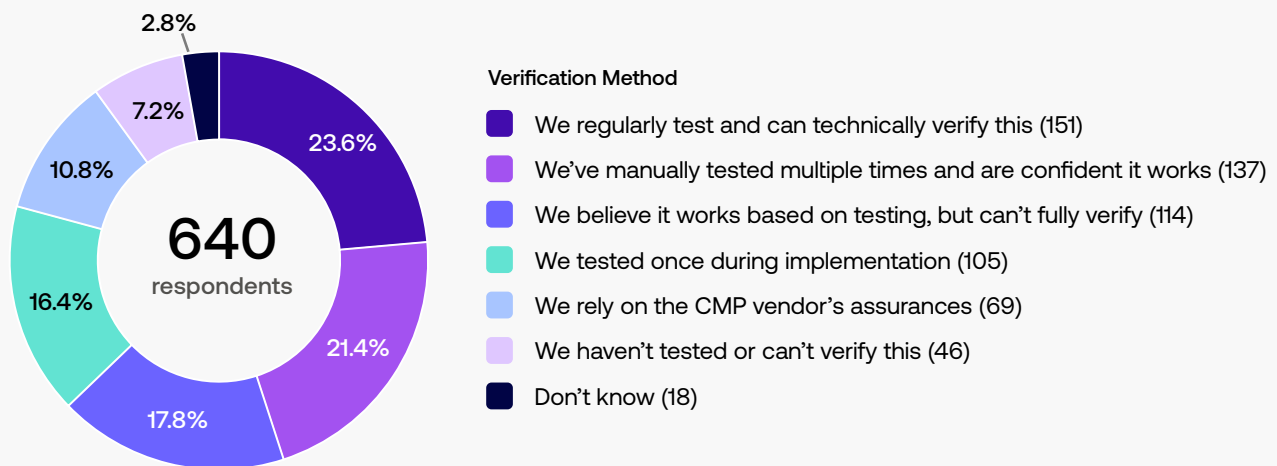
Despite widespread CMP adoption, relatively few organizations continuously verify that their consent configurations operate as intended.

When asked how they validate consent enforcement, fewer than one-quarter of respondents reported that they regularly test and technically verify consent behavior in production environments.

FIGURE 6

Few Organizations Continuously Verify Consent Enforcement

Survey question: Which of the following, if any, best describes whether you have tested and can verify that your cookie consent setup actually prevents tracking (e.g. when a user clicks “Reject All”)?



Base: Persona 1 and Persona 2 respondents (n = 640).

These findings reveal an important gap between confidence and verification.

While many organizations believe their consent controls function correctly, fewer than one in four continuously validate consent enforcement through technical testing. Others rely on one-time implementation testing, vendor assurances, or assumptions that consent mechanisms continue to operate as originally configured.

As digital environments evolve, however, assumptions can quickly become outdated.

Third-party vendors release updates, website functionality changes, marketing technologies are added, and execution sequences are modified. Each change creates the potential for consent behavior to drift from the organization's original intent.



Key Takeaway

Consent collection is a point-in-time event.
Consent enforcement is a continuous operational process.

Many Organizations Continue to Rely on Manual Consent Enforcement

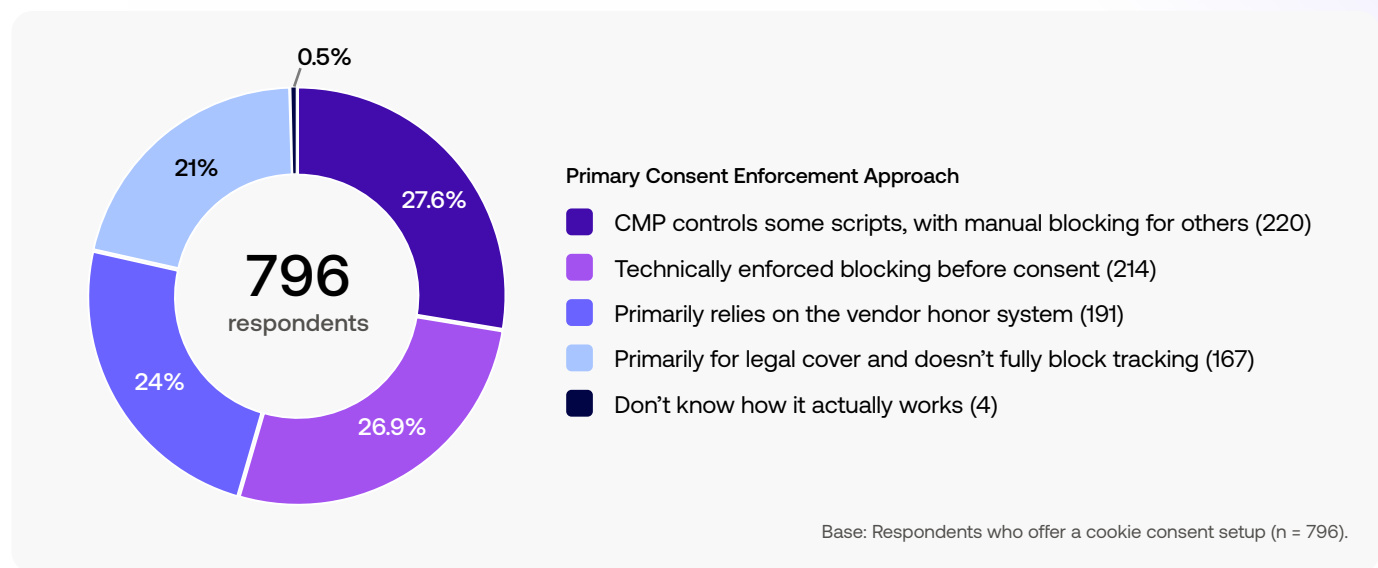
The survey also found that many organizations rely on operational processes that are difficult to maintain as digital ecosystems become more complex.

Only approximately one-quarter of organizations reported implementing technical controls that actively prevent data collection before consent is granted. Many others rely on manual processes, vendor cooperation, or consent frameworks that do not fully enforce user preferences.

FIGURE 7

Consent Enforcement Often Depends on Manual Processes

Survey question: What best describes your cookie consent implementation?



These findings suggest that consent enforcement remains heavily dependent on operational processes rather than technical verification.

For organizations managing dozens of third-party technologies, maintaining manual enforcement processes can become increasingly difficult as vendors update technologies, new services are deployed, and digital experiences evolve.

This creates an environment where organizations may believe they are compliant while lacking the visibility required to independently validate that assumption.

Consent Enforcement Gaps Are Common

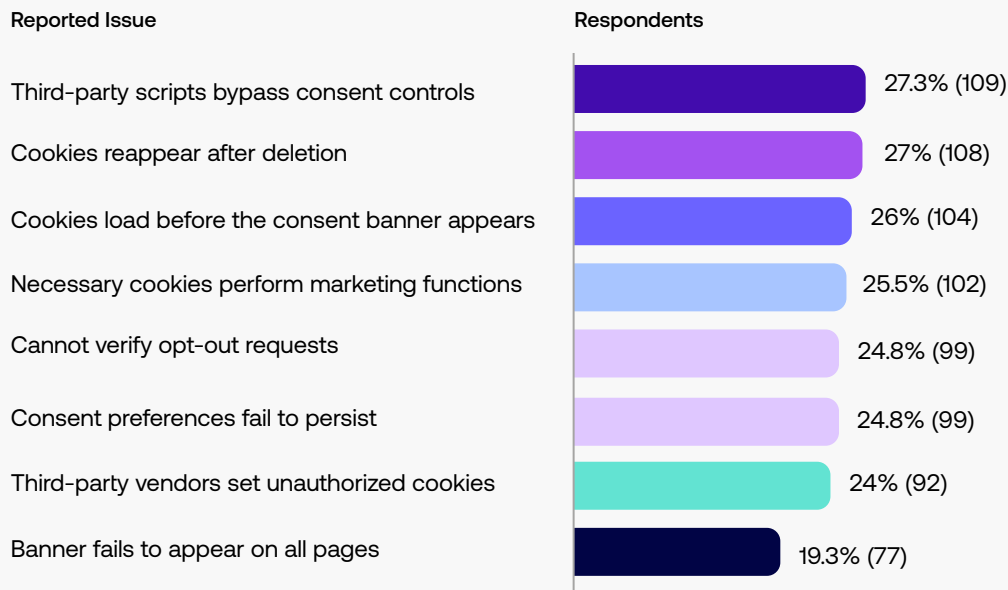
The complexity of modern digital ecosystems means that consent enforcement failures are not uncommon.

Respondents reported experiencing a wide range of issues that resulted in data collection occurring outside intended consent controls.

FIGURE 8

Organizations Report a Wide Range of Consent Enforcement Failures

Survey question: Which of the following cookie consent issues, if any, have you ever experienced? (Select all that apply)



Base: Persona 1 respondents (n = 400). Multiple responses permitted.

These findings suggest that consent failures are not necessarily the result of poor privacy programs. Rather, they reflect the operational challenge of governing highly dynamic environments where technologies continuously change.

Consent failures can occur for many reasons:

- Third-party vendors update existing technologies.
- Website changes alter script execution order.
- New technologies are deployed without privacy review.
- Marketing tools bypass existing controls.

Consent preferences are not consistently propagated across systems.

The challenge for organizations is therefore not simply obtaining consent—it is continuously validating that consent remains effective over time.



Why This Matters

Regulators do not evaluate whether organizations intended to honor consent preferences. They evaluate whether consent preferences were actually honored.

Regional Spotlight

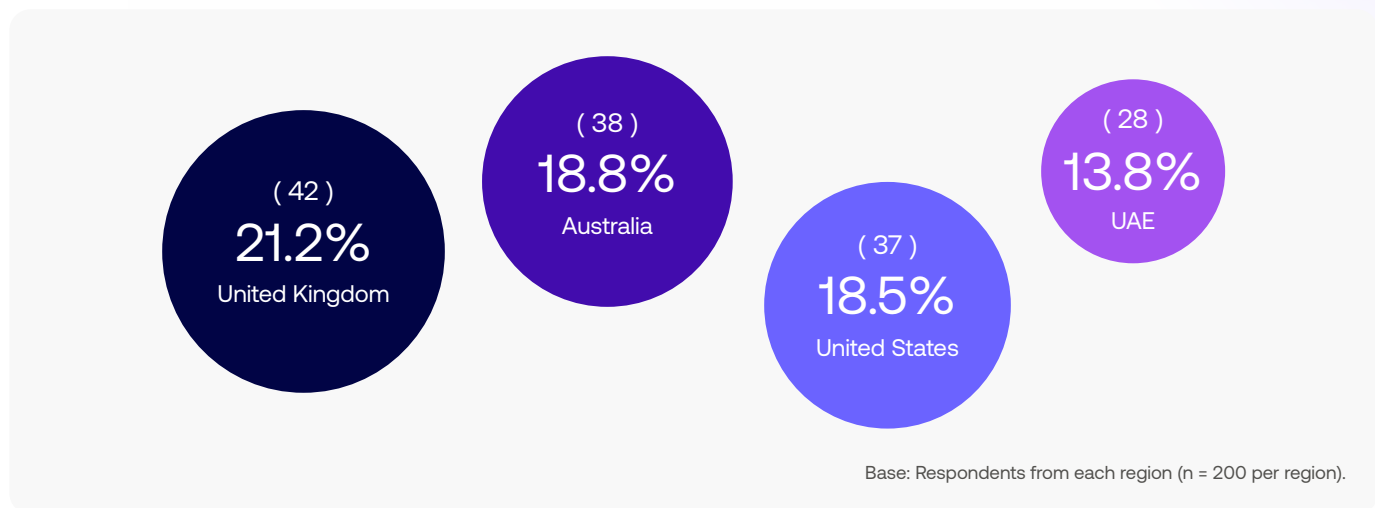
Continuous Consent Verification Remains Limited Across Regions

While consent management technologies have achieved broad adoption globally, relatively few organizations regularly test and technically verify that consent preferences are enforced as intended. Organizations in the United Kingdom reported the highest rates of continuous consent verification (21.2%), followed by Australia (18.8%) and the United States (18.5%). Respondents in the UAE reported the lowest rate of continuous verification (13.8%).

These findings suggest that, regardless of geography or regulatory framework, organizations continue to face challenges validating consent enforcement across increasingly complex and continuously evolving digital environments.

FIGURE 9

Organizations That Regularly Test and Technically Verify Consent Enforcement by Region



What These Findings Mean

The findings in this chapter reveal an important evolution in digital privacy compliance.

For many years, organizations approached consent management primarily as a deployment challenge: implement a consent banner, configure user preferences, maintain records, and document policies.

Today's digital environments require a different approach.

As digital ecosystems become increasingly dynamic, organizations can no longer assume that consent preferences continue to function as originally designed. Instead, they must continuously validate that technologies operating within production environments behave as intended.

The future of consent management will likely depend less on collecting consent and more on continuously verifying that consent choices remain effective across the Digital Experience Layer.



Key Takeaway

Consent doesn't end with a banner. It requires continuous verification.

CHAPTER 03

The Vendor Accountability Gap



Organizations Remain Responsible for Behaviors They Cannot Always Observe

Modern digital experiences depend on trust.

Organizations trust analytics providers to collect data appropriately. They trust advertising technologies to honor consent preferences. They trust payment providers to protect sensitive information. They trust customer support platforms, embedded services, content delivery networks, and software vendors to operate within approved privacy and security requirements.

However, trust alone does not guarantee compliance.

As digital ecosystems become increasingly dependent on third-party technologies, organizations face a growing challenge: maintaining accountability for technologies and vendors they do not directly manage. Vendors release updates, marketing teams deploy new tools, agencies introduce tracking technologies, and software providers modify functionality—all of which can alter how customer information is collected, processed, and shared.

Importantly, these changes often occur without the direct involvement—or awareness—of privacy, security, and compliance teams.

The findings from this research suggest that organizations have largely established vendor governance frameworks. The challenge is maintaining confidence that vendor behavior continues to align with those frameworks over time.

Organizations Have Established Formal Vendor Governance Processes

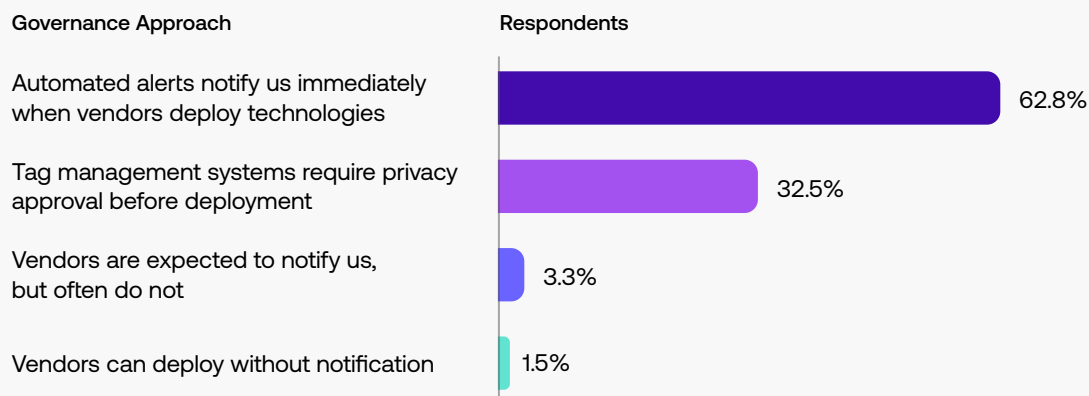
The good news is that most organizations have implemented formal processes designed to govern how third-party technologies are introduced into their digital environments.

Our research found that nearly all organizations have established approval workflows, monitoring controls, or governance requirements intended to prevent vendors from deploying technologies without appropriate oversight.

FIGURE 10

Most Organizations Have Established Vendor Governance Controls

Survey question: Do you receive notifications when your marketing team deploy a new tracking script?



Base: Persona 1 respondents (n = 400).

In total, **95.3% of organizations report having implemented formal governance controls designed to manage vendor deployments.**

These findings suggest that privacy teams are not failing to establish governance processes. Rather, organizations have invested significant effort in creating policies, approval workflows, and oversight mechanisms intended to reduce compliance risk.

However, establishing governance controls and continuously validating their effectiveness are fundamentally different challenges.



Key Insight

Organizations have largely solved vendor governance on paper. The challenge is continuously validating that governance controls remain effective as digital ecosystems evolve.

Continuous Verification of Vendor Behavior Remains Limited

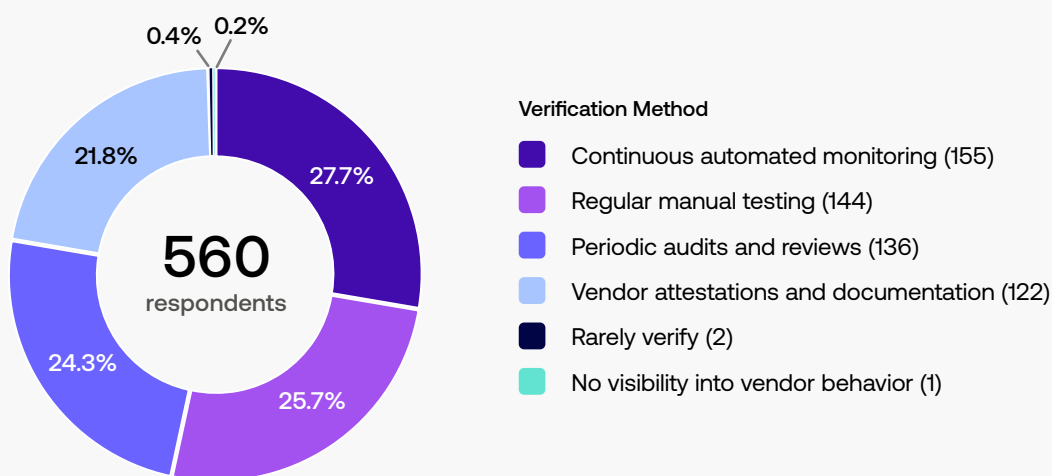
While most organizations have implemented governance frameworks, relatively few continuously monitor whether vendor behavior remains consistent with approved policies and consent requirements.

When asked how they verify vendor activity after deployment, only approximately one-quarter of respondents reported using continuous automated monitoring.

FIGURE 11

Most Organizations Continue to Verify Vendor Behavior Through Periodic Processes

Survey question: *How, if at all, do you monitor and verify that vendors' scripts behave as expected and don't change data collection without your knowledge?*



Base: Persona 1 and Persona 3 respondents (n = 560).

These findings reveal an important operational gap.

While organizations have established governance frameworks, many continue to rely on manual testing, periodic reviews, or vendor assurances to determine whether third-party technologies continue to behave as intended.

This approach may have been sufficient when websites contained relatively few third-party technologies. However, modern digital experiences evolve continuously. Vendors release updates, add integrations, modify data collection practices, and change functionality on an ongoing basis.

As a result, verification methods that occur monthly, quarterly, or annually may no longer provide sufficient visibility into rapidly changing digital environments.



Key Insight

Governance frameworks establish expectations. Continuous monitoring validates that those expectations continue to be met.

Vendor Data Collection Practices Frequently Change Without Notification

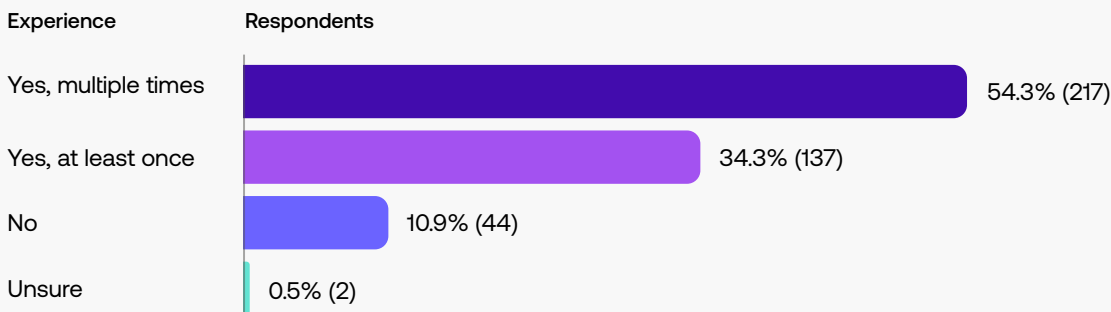
Perhaps the most significant finding in this chapter is the frequency with which organizations experience changes to vendor behavior without prior notification.

Our research found that nearly nine out of ten organizations have experienced vendors changing how customer data is collected, processed, or shared without informing privacy or compliance teams.

FIGURE 12

Undocumented Vendor Behavior Changes Are Common

Survey question: *Has a marketing vendor ever changed their data collection practices without notifying your privacy team?*



Base: Persona 1 respondents (n = 400).

In total, **88.6% of organizations reported experiencing undocumented changes to vendor data collection practices.**

This finding highlights one of the defining challenges of privacy compliance across the Digital Experience Layer.

Organizations remain legally and operationally accountable for vendor behavior, yet many lack the operational visibility necessary to identify when that behavior changes.

Examples of undocumented changes can include:

- Vendors collecting additional data elements.
- Changes to cookie and tracking behavior.
- New third-party integrations.
- Modifications to consent handling.
- Additional data sharing with downstream providers.
- Changes to software development kits (SDKs) or embedded services.

While these changes may be operationally routine from the vendor perspective, they can introduce significant compliance, privacy, and security implications for organizations responsible for governing them.



Key Insight

Vendor accountability cannot be assumed. It must be continuously verified.

Governance and Operational Reality Often Diverge

One of the most important themes emerging from this research is the distinction between governance intent and operational reality.

Organizations have invested heavily in privacy programs, vendor management frameworks, approval processes, and compliance controls. These investments have created mature governance structures designed to reduce risk and improve accountability.

However, maintaining confidence that those controls continue to operate effectively after deployment remains a significant challenge.

The findings from Chapters 1 and 2 demonstrated that organizations frequently discover unauthorized technologies and consent failures after they occur. This chapter reveals a similar pattern in vendor governance: organizations establish policies and controls, but often lack the continuous operational visibility necessary to verify that those controls remain effective over time.

This gap between governance and operational reality represents one of the defining challenges of privacy compliance across the Digital Experience Layer.

Regional Spotlight

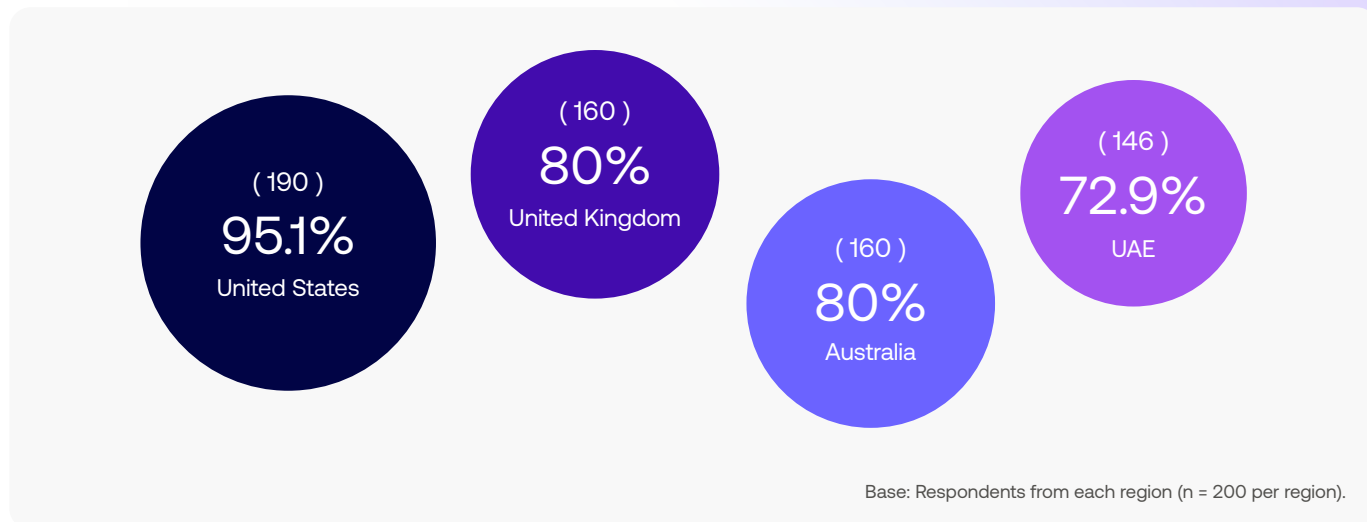
Vendor Governance Challenges Are Global

While organizations in different regions employ varying governance models and operate under different regulatory frameworks, the challenge of maintaining visibility into changing vendor behavior remains remarkably consistent. Respondents in the United States reported the highest incidence of vendors changing data collection practices without notification (95.1%), followed by organizations in the United Kingdom and Australia (both 80.0%). Organizations in the UAE reported lower rates (72.9%), though nearly three-quarters still experienced undocumented changes to vendor behavior.

These findings suggest that the challenge of maintaining accountability for third-party technologies is not driven by geography or regulation, but by the increasingly dynamic nature of modern digital ecosystems.

FIGURE 13

Organizations That Experienced Undocumented Vendor Changes



What These Findings Mean

The findings in this chapter suggest that the challenge facing organizations is no longer establishing vendor governance frameworks. Rather, it is maintaining confidence that those frameworks continue to operate effectively as digital environments evolve.

Organizations remain responsible for technologies they do not directly control. Yet vendors, technologies, and digital experiences continue to change faster than traditional governance processes can monitor them.

As digital ecosystems become increasingly dynamic, organizations can no longer rely solely on trust, contracts, or periodic reviews to manage vendor risk.

Instead, maintaining accountability across the Digital Experience Layer increasingly depends on continuous visibility and ongoing verification.



Key Takeaway

Vendor accountability cannot be assumed. It must be continuously verified.

CHAPTER 04

When Compliance Becomes Evidence



Privacy Compliance Is Increasingly Measured by What Organizations Can Prove

For many years, organizations approached privacy compliance primarily as a documentation exercise.

Organizations developed privacy policies, implemented consent management platforms, negotiated vendor agreements, conducted assessments, and established governance frameworks designed to satisfy regulatory requirements. These efforts remain essential components of modern privacy programs.

However, regulatory expectations continue to evolve.

Increasingly, regulators are focused not only on whether organizations have implemented privacy controls, but also on whether organizations can demonstrate that those controls functioned as intended within production environments. Questions surrounding consent enforcement, third-party data collection, vendor accountability, and data sharing practices increasingly require organizations to provide operational evidence rather than policy documentation alone.

This shift represents an important evolution in privacy compliance.

The challenge is no longer simply establishing controls. The challenge is demonstrating that those controls continue to operate effectively as digital environments evolve.

The findings from this research suggest that many organizations are already experiencing this transition firsthand.

Regulatory Readiness Depends on Operational Visibility

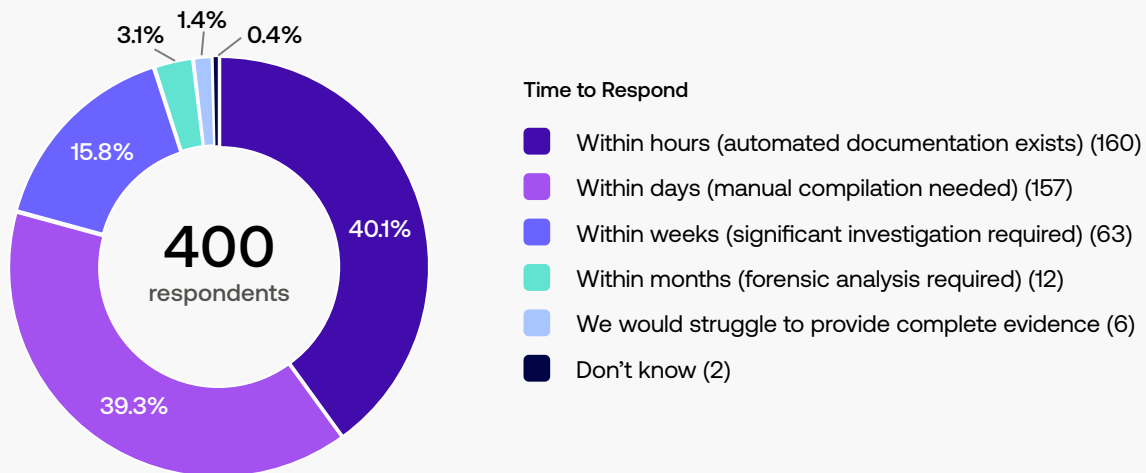
Privacy enforcement related to websites, digital experiences, and online data collection practices has become an operational reality for many organizations.

Our research found that approximately half of all organizations surveyed have received a regulatory inquiry related to digital experience privacy practices.

FIGURE 14

Organizations Differ Significantly in Their Ability to Respond to Regulatory Requests

Survey question: *If a state Attorney General asked you to prove what data your website collects RIGHT NOW, how fast, if at all, could you respond?*



Base: Persona 1 respondents (n = 400).

These findings demonstrate that while many organizations believe they could respond quickly to a regulatory request, others would require additional investigation or manual analysis before providing an accurate answer. As digital environments become more complex and technologies change more frequently, the ability to respond quickly increasingly depends on maintaining continuous visibility rather than reconstructing historical activity after the fact.



Key Takeaway

Regulatory readiness begins with operational visibility. Organizations cannot demonstrate compliance if they cannot accurately identify what is happening across their digital properties today.

Confidence Does Not Always Equal Continuous Evidence

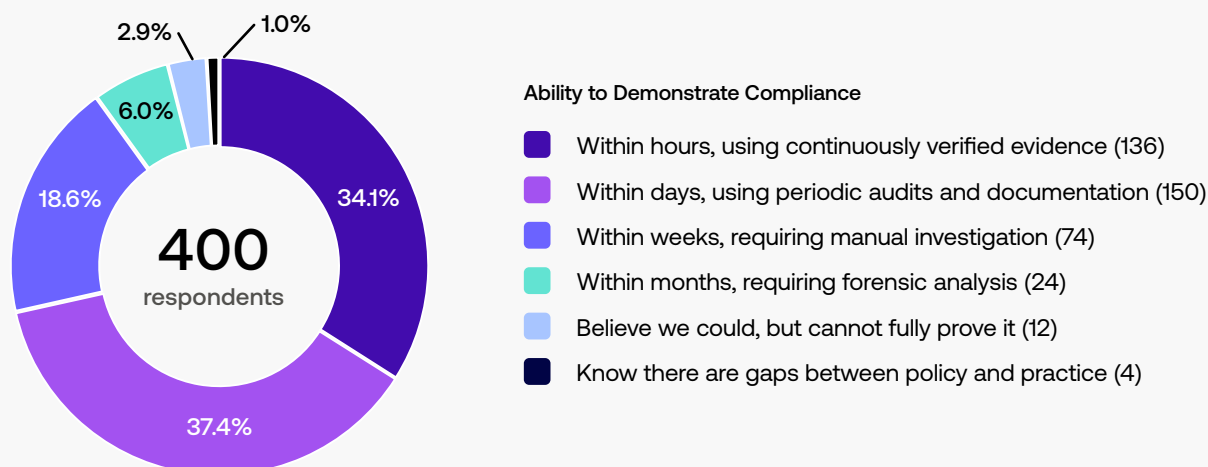
The research also explored how organizations would demonstrate that website behavior aligns with their published privacy commitments if requested by a regulator.

While a majority of respondents reported they could produce evidence within hours or days, the methods used to generate that evidence varied significantly.

FIGURE 15

Organizations Can Produce Evidence, But Continuous Verification Remains Limited

Survey question: *How quickly, if at all, could you prove that your website's actual data collection matches your privacy policy (e.g., if requested by a regulator)?*



Base: Persona 1 respondents (n = 400).

Although 71.5% of respondents indicated they could produce evidence within hours or days, only 34.1% reported maintaining continuously verified evidence. Most organizations continue to rely on periodic audits, historical documentation, or manual investigations to demonstrate compliance.

These findings highlight an important distinction between responding to a regulatory request and continuously maintaining evidence that privacy controls are functioning as intended. Reconstructing historical website behavior after the fact becomes increasingly difficult as third-party technologies, consent configurations, and vendor implementations evolve over time.



Key Insight

The challenge is no longer whether organizations can eventually produce evidence. The challenge is maintaining evidence continuously as digital environments evolve.

Privacy Compliance Is Becoming Operational

Taken together, these findings suggest that privacy compliance is evolving beyond documentation toward operational verification.

Historically, organizations demonstrated compliance through policies, consent records, vendor agreements, and audit reports. While these remain essential, they provide only a snapshot of governance at a particular point in time. They do not necessarily demonstrate what technologies were operating in production, what data was collected, or whether privacy controls continued to function as intended after deployment.

As digital ecosystems become more dynamic, operational evidence is becoming an increasingly important complement to traditional governance documentation. Organizations that maintain ongoing visibility into third-party technologies, consent enforcement, and vendor behavior are better positioned to respond confidently to regulatory requests and demonstrate that their privacy commitments are reflected in day-to-day operations.

What These Findings Mean

Privacy compliance is no longer measured solely by the existence of policies and documented processes. Increasingly, organizations are expected to demonstrate—quickly and accurately—how privacy controls operate across live digital environments.

Regional Spotlight

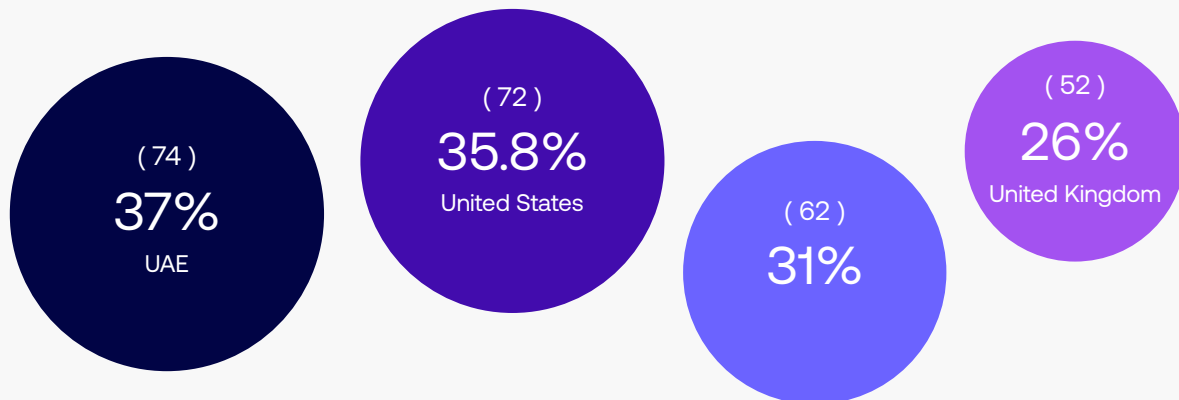
Evidence-Based Privacy Compliance Is Becoming a Global Expectation

The ability to produce operational evidence quickly varied across the regions surveyed, though respondents in every market reported growing confidence in their ability to demonstrate compliance. **Organizations in the UAE were most likely to report that they could produce continuously verified evidence within hours (37.0%), followed by the United States (35.8%), Australia (31.0%), and the United Kingdom (26.0%).**

While the level of operational readiness differs somewhat by region, the overall trend is consistent: organizations increasingly recognize that demonstrating compliance requires more than policies and documentation alone. Across all markets, privacy leaders are investing in capabilities that improve visibility, strengthen operational verification, and accelerate their ability to respond to regulatory requests.

FIGURE 16

Organizations Able to Produce Continuously Verified Compliance Evidence Within Hours



Base: Respondents from each region (n = 200 per region).

What These Findings Mean

The findings in this chapter suggest that privacy compliance is evolving from a documentation exercise into an operational discipline.

Organizations can no longer rely solely on policies, contracts, and periodic assessments to demonstrate compliance across rapidly changing digital environments. Instead, the ability to produce timely, accurate, and verifiable evidence is becoming a key indicator of privacy program maturity.

As the Digital Experience Layer grows in complexity, organizations that maintain continuous visibility into website behavior, third-party technologies, and consent enforcement will be better positioned to respond to regulatory scrutiny and adapt to evolving compliance expectations.



Key Takeaway

Privacy compliance is increasingly measured by evidence, not intent.

The Operational Maturity Gap



Mature Privacy Programs Still Face Significant Execution Challenges

Privacy programs have advanced substantially over the past decade. Organizations have implemented consent management platforms, formalized vendor review processes, established governance frameworks, and developed greater regulatory expertise.

The survey reflects this progress. Most respondents characterize their organizations' client-side privacy maturity as either advanced or developing, indicating that formal programs and documented processes are now widespread.

However, program maturity does not eliminate operational friction.

Privacy teams must oversee digital environments in which scripts, cookies, vendors, consent configurations, and data flows change frequently. Even organizations with established governance structures can struggle to maintain accurate policies, verify consent enforcement, process requests across multiple vendors, and detect changes in third-party behavior.

The data reveals a gap not between awareness and intent, but between program maturity and the resources, automation, and visibility required to execute privacy governance consistently at scale.

Many Privacy Teams Remain Under-Resourced

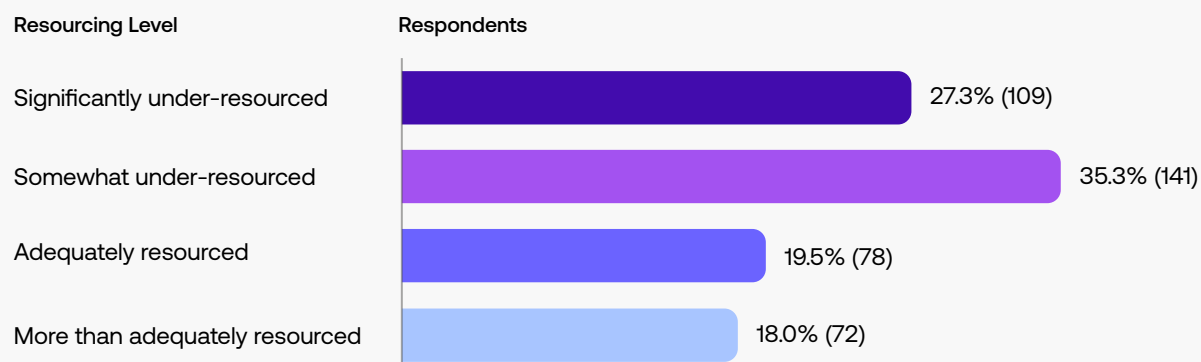
The survey asked privacy professionals directly whether they have sufficient resources to manage client-side privacy.

Nearly two-thirds of applicable respondents described their teams as either significantly or somewhat under-resourced.

FIGURE 17

Nearly Two-Thirds of Privacy Teams Report Resource Constraints

Survey question: How would you describe your resourcing for client-side privacy?



Base: Persona 1 respondents (n = 400).

In total, 62.6% of respondents reported that their client-side privacy function is under-resourced.

Resource constraints can affect more than workload. Limited budget, headcount, or technical expertise can force teams to prioritize immediate compliance needs over proactive monitoring and long-term program improvement. This can leave even mature privacy programs dependent on periodic reviews and manual investigation.



Key Insight

Privacy teams may have established governance processes without having sufficient resources to operate those processes continuously.

Most Client-Side Privacy Work Remains Manual

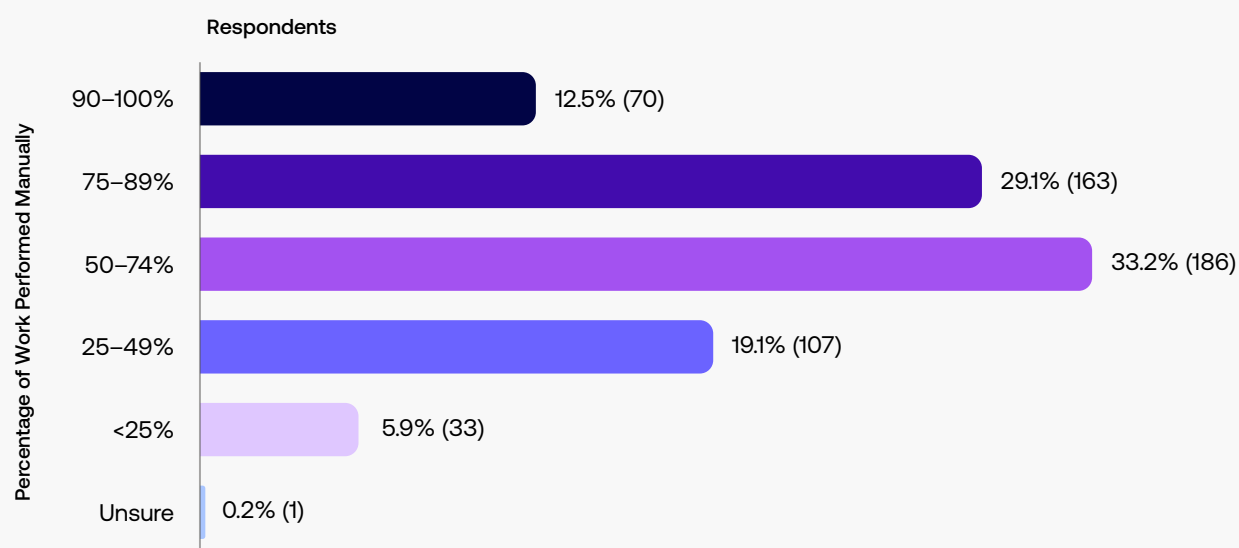
Resource pressure is compounded by the amount of privacy work that still depends on manual processes.

Respondents estimated that an average of 64.3% of their client-side privacy work is performed manually rather than through automation. Nearly three-quarters reported that at least half of their work remains manual.

FIGURE 18

Client-Side Privacy Work Remains Predominantly Manual

Survey question: *What percentage, if any, of your client-side privacy work is manual (vs. automated)?*



Base: All respondents (n = 560)

Combined, **74.8% of respondents** said that at least half of their client-side privacy work is manual, including 41.6% who reported that three-quarters or more is handled manually.

Manual processes remain valuable for activities requiring legal judgment, contextual analysis, or business consultation. However, relying on them for routine discovery, validation, monitoring, and evidence collection can limit a team's ability to keep pace with changes across large digital environments.



Key Insight

The operational burden on privacy teams is driven not only by the volume of work, but by how much of that work still requires manual intervention.

Privacy Challenges Span Policy, Operations, and Technology

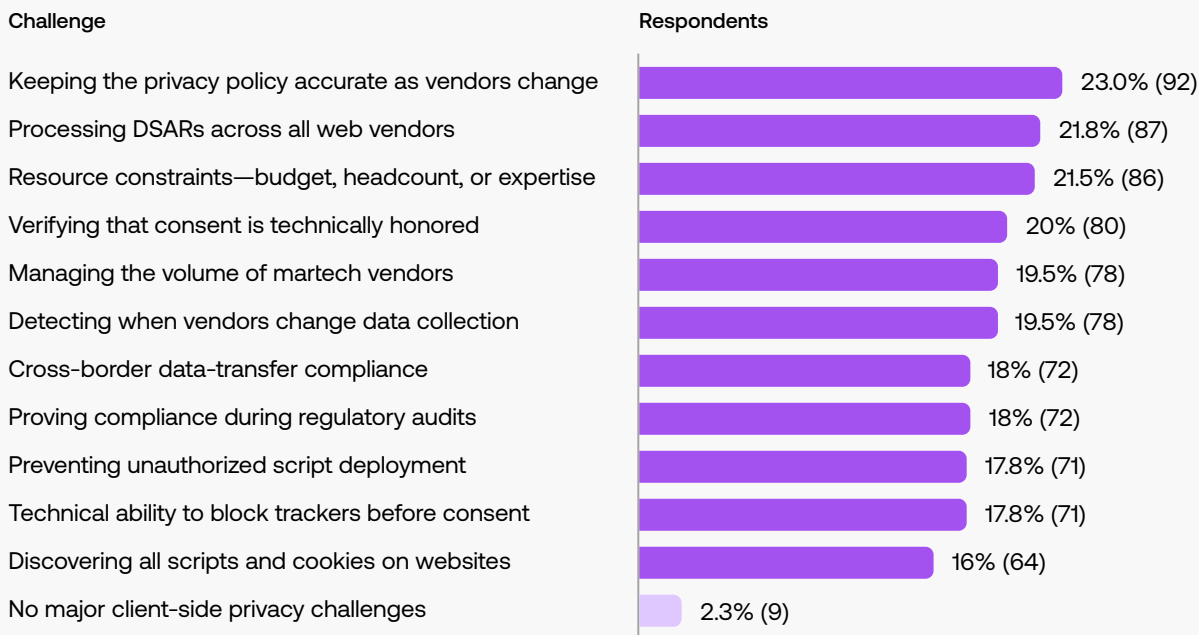
When asked to identify their biggest client-side privacy challenges, respondents did not point to a single dominant problem. Instead, the results reflect the interconnected nature of privacy operations.

Maintaining an accurate privacy policy as vendors change was the most frequently selected challenge, followed closely by processing data subject access requests across web vendors, resource constraints, technical consent verification, vendor volume, and detecting changes in data collection practices.

FIGURE 19

Client-Side Privacy Challenges Extend Across the Entire Operating Model

Survey question: What, if anything, are your biggest client-side privacy challenges? (Select up to 3)



Base: Applicable respondents, n=400. Multiple responses permitted.

The relatively even distribution across these challenges is itself significant. It indicates that client-side privacy is not a single-process problem. Policy management, request fulfillment, resourcing, consent, vendor oversight, technical enforcement, and evidence generation are all connected.

Solving one area in isolation may improve part of the program without addressing the broader operational burden.



Key Insight

Client-side privacy maturity depends on coordinating legal, governance, technical, and operational capabilities—not optimizing a single control.

Most Organizations Report Meaningful Privacy Maturity

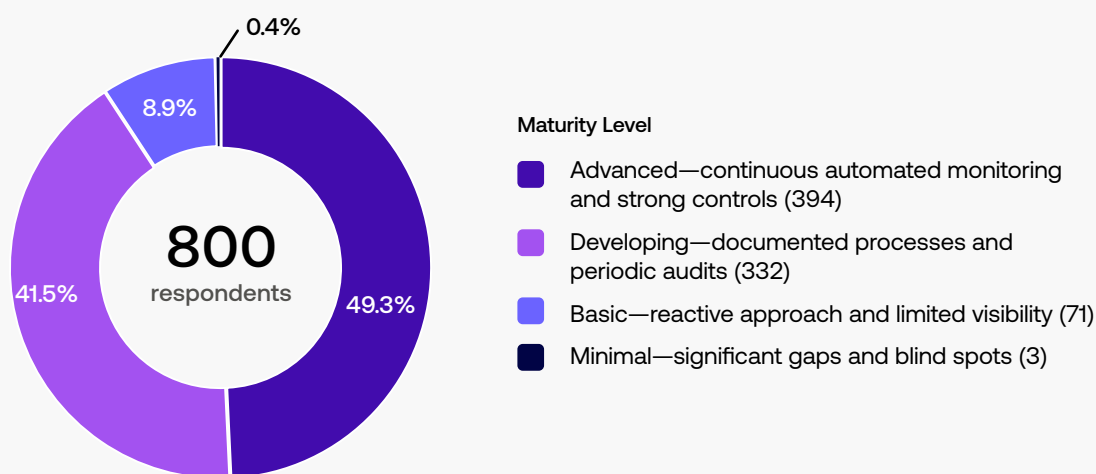
Although privacy teams face resource and execution challenges, respondents generally view their organizations' client-side privacy programs as mature.

Nearly half rated their organization as advanced, while another 41.5% described it as developing.

FIGURE 20

Most Organizations Rate Their Client-Side Privacy Maturity as Advanced or Developing

Survey question: *How would you rate your organisation's client-side privacy maturity?*



Base: All respondents, n=800.

In total, 90.8% of respondents rated their programs as advanced or developing. Only 9.3% described their maturity as basic or minimal.

This finding changes how the operational maturity gap should be understood. The survey does not indicate that most organizations lack privacy programs or operate only reactively. Instead, it shows that organizations can possess documented processes and strong controls while still experiencing high levels of manual work, resource pressure, and difficulty managing dynamic digital environments.

The gap is therefore not simply between mature and immature organizations. It exists between the maturity organizations have achieved and the operational efficiency they need to sustain it.



Key Insight

Program maturity does not automatically translate into scalable execution. Mature organizations can still face significant resource, visibility, and automation constraints.

Organizations Want Better Integration and Real-Time Control

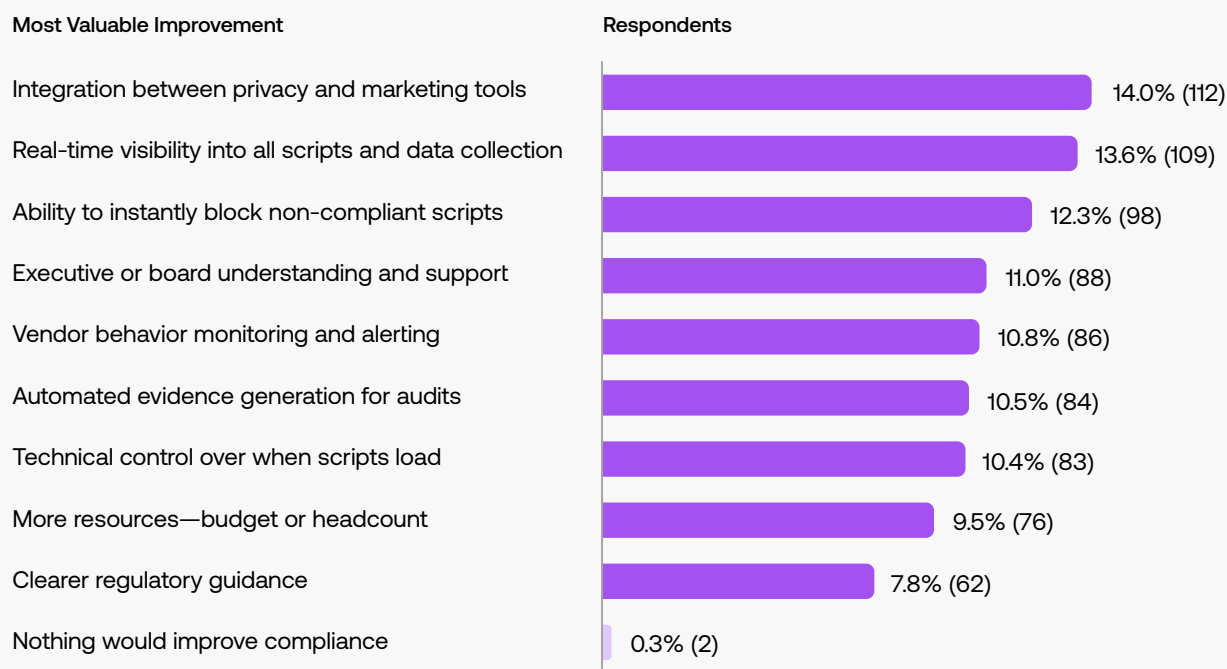
Respondents were also asked to identify the single improvement that would have the greatest effect on client-side privacy compliance.

No single answer dominated, but the leading responses centered on connecting privacy with marketing operations, obtaining real-time visibility, controlling non-compliant scripts, strengthening organizational support, monitoring vendor behavior, and automating evidence generation.

FIGURE 21

Organizations Prioritize Integration, Visibility, and Technical Control

Survey question: *What, if anything, would MOST improve your client-side privacy compliance?*



Base: All respondents, n=800.

The responses show that organizations are looking for more than additional headcount or regulatory guidance. Many of the highest-priority improvements involve connecting organizational processes with real-time technical visibility and control.

This reinforces the broader pattern identified throughout the report: privacy teams have built governance foundations, but need stronger operational capabilities to apply those frameworks across live digital environments.

Regional Spotlight

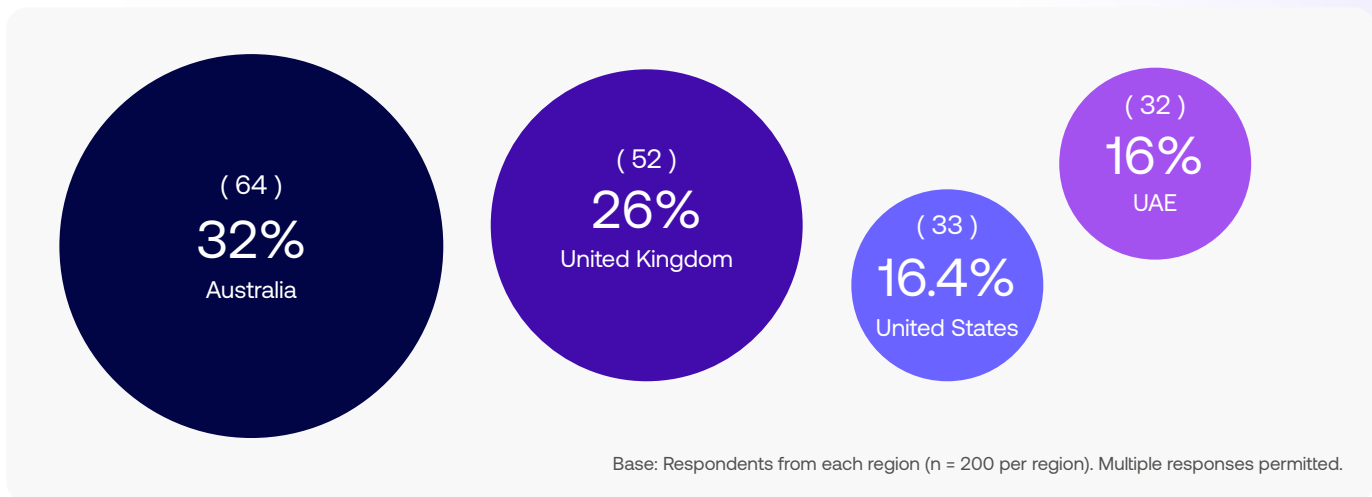
Detecting Vendor Changes Presents Different Challenges by Market

The difficulty of identifying changes in vendor data collection varied across the regions surveyed. Respondents in Australia were the most likely to name this as one of their biggest client-side privacy challenges, at 32.0%, followed by the United Kingdom at 26.0%. The issue was selected by 16.4% of respondents in the United States and 16.0% in the UAE.

FIGURE 22

Detecting Changes in Vendor Data Collection Remains a Cross-Market Challenge

Survey question: *What, if anything, are your biggest client-side privacy challenges? (Select up to 3)*



The variation suggests that operational priorities differ by market, but the underlying governance issue is shared: organizations need reliable ways to identify when third-party behavior changes after approval or deployment.

What These Findings Mean

The data presents a balanced picture of privacy maturity.

Most organizations have moved beyond minimal or purely reactive programs. They have documented processes, established controls, and, in many cases, adopted continuous monitoring. Yet these gains coexist with substantial resource constraints and a heavy reliance on manual work.

This creates an operational maturity gap. Privacy programs may be strategically mature while remaining difficult to execute efficiently across websites, applications, vendors, and data flows that change frequently.

Closing that gap will require more than additional policies. Organizations need better integration between teams and systems, real-time visibility into client-side activity, stronger technical controls, and automation for repeatable monitoring, validation, and evidence collection.



Key Takeaway

Privacy programs have matured, but scalable execution remains a challenge. The next stage of maturity will depend on reducing manual work and strengthening real-time operational capabilities.

The Shift to Continuous Compliance



Organizations Are Redefining How Privacy Compliance Is Managed

The findings throughout this report reveal a consistent theme: organizations increasingly recognize that traditional approaches to digital privacy compliance are struggling to keep pace with modern digital environments.

Organizations have invested heavily in privacy programs, consent management platforms, governance frameworks, vendor oversight processes, and regulatory expertise. Yet many continue to face challenges maintaining visibility, validating consent enforcement, governing third-party technologies, and demonstrating compliance across rapidly changing digital ecosystems.

Importantly, organizations appear to recognize that these challenges are not temporary.

The findings from this research suggest that privacy leaders increasingly understand that maintaining compliance across the Digital Experience Layer requires new operational capabilities designed to provide continuous visibility, validation, and assurance.

This shift represents more than a technology trend.

It represents a fundamental change in how organizations approach digital privacy compliance.

Organizations Expect Privacy Investment to Continue Increasing

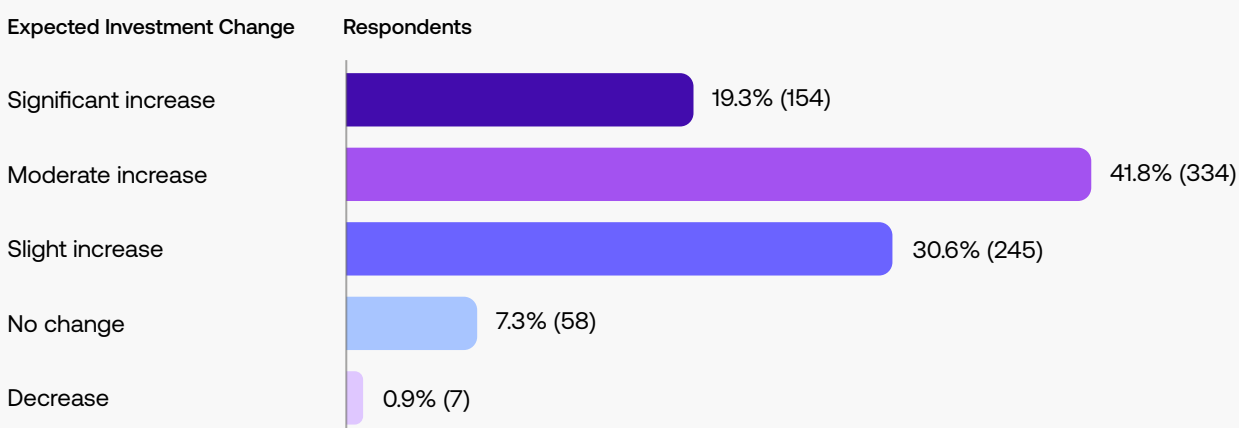
Our research found overwhelming agreement that investment in digital privacy compliance will continue to grow over the coming years.

More than nine out of ten organizations surveyed expect their investments in digital privacy technologies, processes, and operational capabilities to increase.

FIGURE 23

Organizations Expect Continued Growth in Privacy Investment

Survey question: Over the next 12 months, will your investment in client-side privacy increase or decrease?



Base: All respondents (n = 800). Percentages may not total exactly 100% due to rounding.

In total, 91.7% of organizations expect investment in digital privacy capabilities to increase.

These findings suggest that organizations increasingly view digital privacy not solely as a regulatory obligation, but as an operational capability requiring sustained investment.

Several factors are contributing to this trend, including:

- Increasing regulatory scrutiny
- Growing third-party ecosystems
- Expanding vendor relationships
- Greater consumer privacy expectations
- Increased operational complexity
- The emergence of AI-powered digital experiences

As digital environments continue to evolve, organizations recognize that maintaining privacy compliance requires ongoing investment in both governance and operational capabilities.



Key Insight

Organizations no longer view digital privacy as a one-time compliance initiative. They increasingly view it as a continuously evolving operational function..

Organizations Are Actively Evaluating Privacy Automation

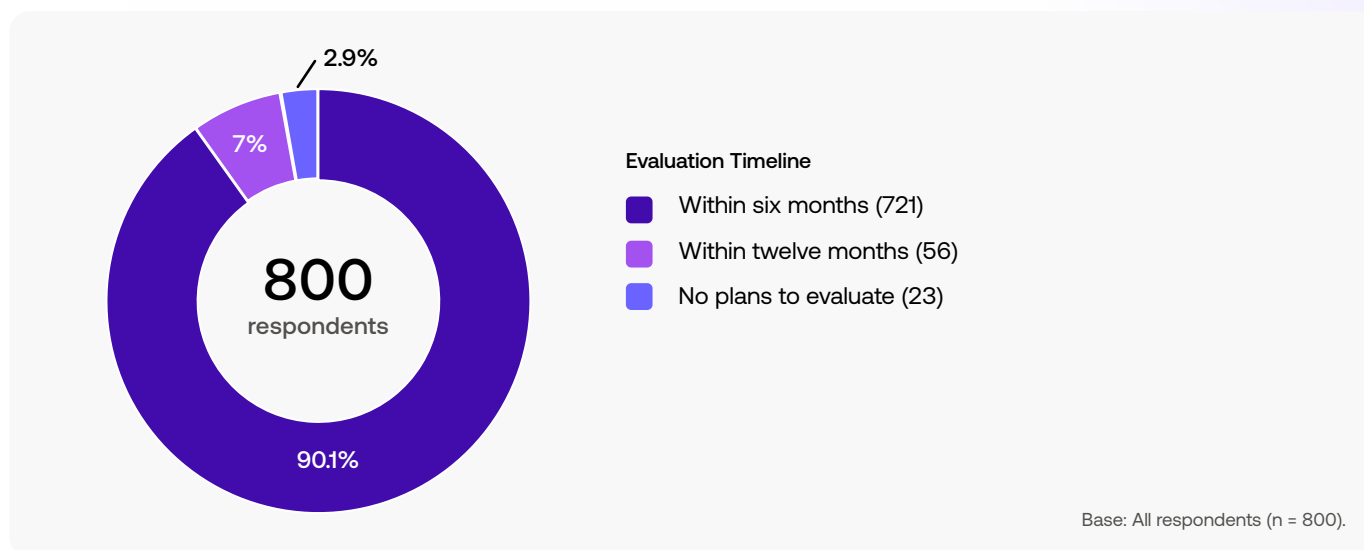
Perhaps the strongest indicator of this shift is the near-universal interest in privacy automation technologies.

Our research found that virtually all organizations surveyed plan to evaluate technologies designed to automate privacy monitoring, validation, and compliance activities.

FIGURE 24

Organizations Are Actively Evaluating Privacy Automation Technologies

Survey question: Are you currently evaluating or planning to evaluate client-side privacy automation tools?



In total, 97.1% of organizations plan to evaluate privacy automation capabilities.

These findings suggest that organizations increasingly recognize the limitations of traditional manual governance approaches within highly dynamic digital environments.

Automation is no longer viewed simply as a way to reduce operational burden. Instead, it is increasingly viewed as a capability that can help organizations maintain visibility, validate controls, and support ongoing compliance activities at scale.

Organizations evaluating privacy automation technologies are seeking capabilities such as:

- Continuous monitoring
- Consent validation
- Vendor behavior verification
- Third-party technology inventory management
- Runtime visibility
- Evidence collection
- Automated compliance reporting
- Risk identification and prioritization



Key Insight

Privacy automation is rapidly becoming a foundational component of modern privacy operations.

Organizations Are Moving Toward Continuous Operational Privacy

One of the clearest themes emerging from this research is the growing recognition that digital privacy compliance requires ongoing operational management.

Historically, organizations managed privacy compliance through:

- Periodic audits
- Annual assessments
- Vendor questionnaires
- Policy reviews
- Manual testing
- Documentation exercises

While these activities remain important, they were designed for environments that changed relatively slowly.

Today's digital ecosystems operate differently.

Third-party technologies update consistently. Vendors change behavior. Consent mechanisms evolve. New services are deployed. AI-powered experiences emerge. Data collection practices shift in real time.

As a result, organizations increasingly recognize the need for capabilities that support:

- Continuous visibility
- Continuous validation
- Continuous monitoring
- Continuous evidence collection
- Continuous governance

This transition from periodic assessment to continuous operational oversight represents one of the most significant shifts occurring within digital privacy compliance today.

Regional Spotlight

Investment in Operational Privacy Capabilities Is Increasing Globally

Organizations across all regions surveyed reported plans to increase investment in privacy technologies and operational capabilities. While investment priorities vary by geography, respondents consistently indicated that digital privacy will require additional resources, technologies, and operational capabilities in the years ahead.

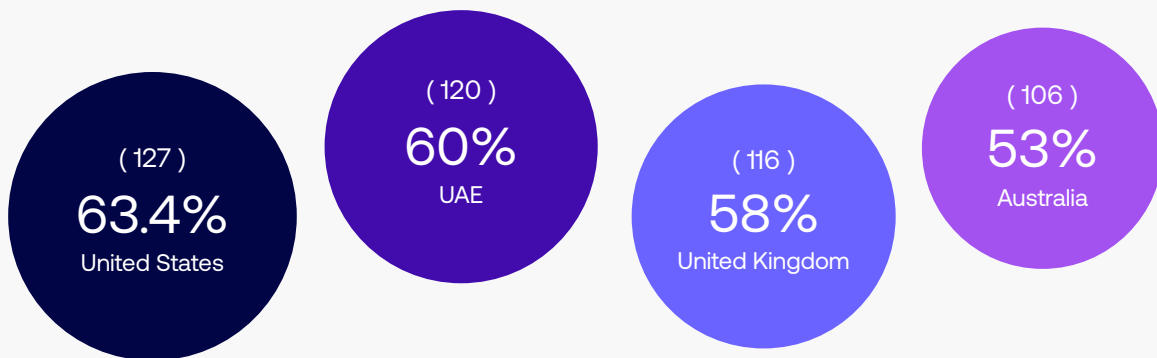
Respondents in the United States reported the highest expectations for increased investment, with **63.4% anticipating moderate or significant growth in digital privacy spending**. Organizations in the UAE (60.0%) and the United Kingdom (58.0%) reported similarly strong expectations, while respondents in Australia (53.0%) also indicated substantial planned investment increases.

These findings suggest that the transition toward operational privacy management is not limited to a single regulatory framework or region, but represents a broader global trend.

FIGURE 25

Organizations Expecting Moderate or Significant Growth in Digital Privacy Investment

Survey question: Over the next 12 months, will your investment in client-side privacy increase or decrease?



Base: Respondents from each region (n = 200 per region).

What These Findings Mean

The findings in this chapter suggest that organizations increasingly recognize privacy compliance as an ongoing responsibility rather than a periodic exercise.

As digital ecosystems grow more complex, organizations are investing in technologies and processes that provide greater visibility, validation, and assurance across their environments.

This reflects a broader evolution in privacy management, moving from static compliance programs toward more adaptive models that can keep pace with changing digital experiences.



Key Takeaway

Organizations increasingly recognize that effective privacy compliance requires continuous operational visibility, validation, and governance.

The Next Era of Privacy Compliance

The findings presented throughout this research reveal an industry at an important inflection point.

Over the past decade, organizations have invested heavily in privacy programs, consent management technologies, governance frameworks, vendor oversight processes, and regulatory expertise. These investments have transformed privacy from a legal and compliance obligation into a strategic business function responsible for protecting both organizations and the individuals they serve.

At the same time, digital experiences have evolved faster than traditional privacy governance models were designed to accommodate.

Modern websites and applications are no longer static environments governed through periodic assessments and manual review processes. They are dynamic ecosystems composed of dozens of third-party technologies, embedded services, software vendors, AI-powered experiences, and continuously evolving data flows.

The findings from this research suggest that organizations increasingly recognize this challenge. Throughout this report, respondents consistently identified many of the same operational realities: digital ecosystems continue to grow in complexity, visibility into third-party activity remains difficult, consent enforcement cannot be assumed, vendor behavior changes frequently, and regulatory expectations increasingly focus on demonstrable evidence rather than documented intent.

At the same time, privacy leaders clearly understand that traditional approaches to governance are struggling to keep pace. Organizations are investing heavily in

technologies and operational models designed to provide greater visibility, continuous validation, and ongoing assurance across their digital environments.

Taken together, these findings suggest that privacy compliance is entering a new phase of maturity.

The next era of privacy compliance will likely be defined less by policy creation and more by operational execution. Organizations will increasingly require the ability to continuously identify technologies operating within their digital environments, validate consent enforcement, monitor vendor behavior, generate operational evidence, and adapt to rapidly changing technologies and regulatory expectations.

This transition represents more than a technological evolution. It represents a fundamental shift in how organizations govern digital experiences.

The organizations that succeed in this next phase of privacy maturity will not necessarily be those with the largest compliance teams, the most extensive documentation, or the most sophisticated governance frameworks. Rather, they will be the organizations capable of continuously seeing, understanding, validating, and governing what happens across the Digital Experience Layer.

As digital ecosystems continue to evolve, one principle becomes increasingly clear:

Privacy compliance can no longer be measured solely by organizational intent. It must be continuously demonstrated through operational evidence.

Research Objectives

The purpose of this research was to better understand how organizations manage privacy, consent, vendor governance, and regulatory compliance across the **Digital Experience Layer**—the collection of third-party technologies, scripts, embedded services, software development kits (SDKs), APIs, and digital interactions that collect, process, transmit, and govern user data across websites and digital applications.

The study examined how organizations approach digital privacy governance across increasingly complex digital environments, including visibility into third-party technologies, consent management practices, vendor accountability, regulatory readiness, operational maturity, and future investment priorities.

The objective of the research was to identify the operational challenges organizations face as digital ecosystems become more dynamic, interconnected, and continuously evolving.

Survey Methodology

This research was conducted by Censuswide on behalf of Ferroot in the first half of 2026.

Censuswide conducted the research using an online quantitative survey methodology targeting senior professionals responsible for privacy, governance, risk, compliance, and security functions within organizations managing complex digital experiences.

The survey included **800 senior professionals** responsible for privacy, governance, risk, compliance, and security functions across organizations managing complex digital experiences.

Respondents were required to have direct responsibility for one or more of the following functions:

- Privacy and data protection
- Governance, risk, and compliance (GRC)
- Information security and cyber risk
- Digital experience governance
- Consent management
- Vendor risk management
- Regulatory compliance

Respondents were evenly distributed across four geographic markets:



Respondent Profile

The research included organizations across a range of industries and organization sizes to provide a broad perspective on digital privacy compliance practices.

Respondents represented organizations responsible for managing:

- Website and mobile application privacy compliance
- Third-party technology ecosystems
- Consent management platforms
- Vendor governance programs
- Regulatory compliance initiatives
- Digital experience security and privacy controls
- Customer data collection and processing activities

All responses were anonymized and aggregated for analysis.

About the Findings

The findings presented in this report represent the experiences, perspectives, and operational practices of privacy, security, governance, and compliance professionals responsible for managing privacy across increasingly complex digital environments.

The research findings were analyzed to identify broader trends shaping privacy compliance across the Digital Experience Layer, including:

- Visibility into third-party technologies
- Consent enforcement and validation
- Vendor accountability and governance
- Regulatory readiness and evidence generation
- Operational maturity
- Future investment priorities

Percentages may not total exactly 100% due to rounding. Certain survey questions permitted multiple responses.

The findings are intended to provide insight into the current state of privacy compliance across the Digital Experience Layer and the operational challenges organizations face as digital ecosystems continue to evolve.

About Feroot

Feroot helps organizations secure and govern the Digital Experience Layer—the collection of client-side technologies, third-party scripts, embedded services, and APIs that collect, process, and transmit customer data across websites and mobile applications.

Its platform provides continuous visibility into website behavior, enabling organizations to identify unauthorized technologies, validate consent enforcement, monitor vendor activity, and generate operational evidence that supports privacy, security, and compliance programs.

Feroot supports organizations in addressing requirements across more than 50 global privacy, security, and regulatory frameworks, including GDPR, CCPA/CPRA, HIPAA, PCI DSS, DORA, and emerging digital privacy regulations.

Organizations looking to better understand their client-side privacy posture can request a Digital Privacy and Consent Assessment, which provides an independent evaluation of website technologies, consent enforcement, third-party data collection, vendor behavior, and potential compliance risks across live digital environments.

To learn more about Feroot or request an assessment, visit www.feroot.com

