

Ebook

The ROI of Privacy Management

Driving Innovation and Growth
Across the Business

osano

Contents



Data Privacy Is a Strategic Investment



Privacy Builds Trust with Customers



Privacy Improves Marketing Effectiveness



Data Privacy Programs Improve Operational Efficiency



Privacy Management Identifies and Mitigates Risk



Transform Compliance into a Business Advantage



About Osano



Endnotes

INTRODUCTION

Data Privacy Is a Strategic Investment

In many organizations, data privacy is seen as a necessary expense—a box to check to avoid penalties and ensure compliance with regulations. It's easy to see it as just another cost center, with benefits that only serve to reduce litigation risks or avoid regulatory fines.

Yes, a robust privacy program does do those things. But that narrow perspective doesn't encompass data privacy's broad strategic value for the business, which far outweighs the cost. Data privacy isn't just a defensive measure: It can be a powerful catalyst for business success. In fact, some organizations report a **1.6× return on investment¹** for their privacy program expenditures, while others realize as much as **\$2.70 for every dollar spent²** on privacy.

But how can your business achieve these impressive financial returns?

This guide delves into the tangible business benefits of a well-executed privacy program—not just for compliance teams, but for the entire organization. We'll explore how data privacy initiatives can enhance operational efficiency, boost customer trust, drive marketing effectiveness, reduce churn, and create competitive differentiation.

Regardless of your role or responsibility for privacy compliance, this guide will equip you with the insights needed to understand and communicate the true value of prioritizing data privacy. Learn how embracing a robust privacy program can be a win for everyone and how Osano's technology and expertise can help you realize these benefits.

SECTION 1

Privacy Builds Trust with Customers

You've no doubt heard the saying, "Data is the new oil." Data, like oil, is a valuable resource that, when refined and applied in the right way, can fuel business growth, innovation, and revenue.

However, unlike oil, external data doesn't flow freely and can't be claimed by people who discover it. The flow of data in a business relies on consumers who provide it and sanction its use. And increasingly, they are reluctant to give companies access to their personal information and have legitimate questions about how we use it. Consumers reward businesses they trust with their data, and that trust is earned with ethical data stewardship. In this business climate, strong data privacy practices are not just a compliance necessity: They are a competitive advantage.

No Trust? No Customer.

A staggering 94%¹ of organizations report that customers won't buy from them if they fail to protect data properly, and 81%² believe that the risks from data collection outweigh the benefits. But crucially, only 29% of participants in a recent IAPP survey³ found it easy to understand how well a company protects their data, while 64% agreed that clear and understandable privacy policies enhance trust. The adoption of AI by businesses doesn't help: 57%⁴ of global consumers view the use of AI in collecting and processing personal data as a significant threat to privacy.

The market shift around the necessity and value of data and increasing customer concern about company data practices require that businesses adopt customer-centric privacy practices. By adopting ethical data-handling practices and being transparent about those practices with customers, businesses can build trust and translate it into powerful business benefits:



More revenue: One study found that 60%⁵ of consumers are willing to spend more with brands they trust to protect their data.



Stronger brand: Google⁶ found that a positive privacy experience can increase the share of brand preference by 49%.



Customer retention: McKinsey reports that 71%⁷ of consumers surveyed would stop doing business with a company if it mishandled their sensitive data, and 52%⁸ of consumers in a Pew Research Center Survey said they already stopped buying from a company due to privacy concerns.

Building Consumer Trust with Osano

Osano's privacy platform enables comprehensive, transparent consent management for privacy and marketing teams:

- › Use templates to create and update privacy policies and cookie disclosures without the need for a development team with **Osano's Trust Center**.
- › Give consumers control over not only what you collect about them, but also how you communicate with them with meaningful, easy-to-exercise choices in **Osano's Unified Consent & Preference Hub** ("Unified Consent").
- › Ensure that consent and subject rights are always up to date and easy for consumers to understand with language and rights localization.
- › Create disclosures with confidence: **Osano's Data Mapping and Assessments** modules help you accurately disclose what you're collecting, where, why you're processing it, how long you retain that information, and whether personal information feeds into AI models and decision-making technology.

Osano's status as a B-Corp and certified public benefit corporation further enhances the perception of your company as a privacy-forward brand that's focused on building trust and loyalty among customers.

SECTION 2

Privacy Improves Marketing Effectiveness

Across the business, there's often a perception that data privacy compliance hinders the ability of marketing to personalize campaigns and segment audiences—which, therefore, hinders innovation, effectiveness, and the ability to drive revenue. Marketers often fall prey to this concern. However, there's evidence that this is simply not the case. In fact, embracing privacy compliance programs and using privacy-oriented technology like Osano can improve marketing and sales effectiveness, drive efficiency, and more.

Research shows that employing personalization in digital marketing improves both open rates and the value of each dollar spent:

- › 80%¹ of people are more likely to make a purchase from a personalized email.
- › Personalized emails have transaction rates that are six times² higher than non-personalized ones.
- › Automated flows such as abandoned-cart or post-purchase emails generate up to 30 times³ more revenue per recipient.

Customers Want Personalization but Only with Consent

Customers want a personalized and consistent experience across channels, and 61%⁴ expect brands to tailor experiences based on their preferences. Do privacy-friendly practices change that? No, but there's a catch: 69%⁵ of customers say they appreciate personalization IF it's based on data they've shared with the business directly.

91%⁶
of consumers

say they're more likely to shop with brands that recognize, remember, and provide relevant offers and recommendations.

69%⁷
of consumers

say they appreciate personalization, so long as it's based on data they've shared with a business directly.

Privacy-Forward Personalization Can Drive Better Results

While privacy laws like the GDPR and CCPA may limit opt-in rates and cookie-based data collection, this doesn't mean marketing will become less effective or more costly. Marketers who adapt by focusing on first-party data can achieve the same results while spending 10% to 20%⁸ less.

And, contrary to popular assumption, embracing data privacy can make marketing more efficient:

- › Ads personalized with data willingly shared by users are 7%⁹ more relevant than those based on cookies.
- › Customers who feel in control of their data when interacting with your company are twice¹⁰ as likely to find advertising relevant.
- › Those customers are also three times¹¹ more likely to react positively to advertising.

In fact, 31%¹² of customers say that understanding how data sharing works with your company makes them more likely to agree that data sharing in return for more relevant ads represents a fair value exchange.

Ads personalized with data willingly shared by users are

7%⁹
more relevant
than those based on cookies.

How Osano Helps Improve Marketing Effectiveness

With Osano's privacy platform, marketing teams can balance personalization and compliance, building trust with consumers, increasing the likelihood of consent, and leveraging data as a powerful tool for success.

› Increase consumer trust and engagement and simplify their ability to control how their data is used:

- **Unified Consent** gathers data directly from users and centralizes it, helping ensure that data used to tailor campaigns and ads is willingly shared.

› Enable effective personalization through a compliance lens:

- With **Unified Consent**, compliantly collect and manage not just cookie data, but also sensitive data, communication preferences, and other personal identifiers to meet global privacy requirements.
- With **Unified Consent** and **Cookie Consent** banners, give consumers a sense of control over their data and increase their willingness to share information by offering multiple ways to set preferences—opt-in/opt-out, communications, or revoking consent if needed.
- **Osano's Subject Rights Management** simplifies how users can exercise their rights. Forms and templated communications localized to each user allow them to easily understand what data companies have on them, request its deletion, or limit its use, further reinforcing trust and control over their data.

With the Osano platform and its approach to compliance-friendly data collection, marketers can increase engagement and the likelihood of data sharing, which can improve the impact of marketing expenditures and optimize return on investment.

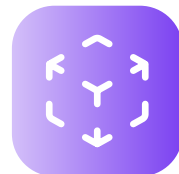
SECTION 3

Data Privacy Programs Improve Operational Efficiency

Operational efficiency is critical to maintaining a competitive edge. But that efficiency is elusive in many businesses.



Data silos are killing productivity: In a report from Cornell University's Ellis Idea Lab¹, 58% of employees stated that different departments often use separate applications, which creates barriers to finding and sharing information. Employees wasted an average of 59 minutes per day searching for information across multiple systems. And respondents estimated that 21% of the mistakes they made resulted from difficulties in accessing information on their company's online tools and communication platforms.



Shadow IT further aggravates fragmentation and increases risk: One report found that 56%² of applications used within companies are not owned or sanctioned by IT. While these tools might solve short-term issues, they create long-term inefficiencies and complicate data governance.



And manual work is costly in more ways than one:

- › Wastes time
- › Introduces error
- › Costs money out of pocket
- › Puts organizations at risk for noncompliance and breach

The High Cost of Manual Subject Rights Management

Handling subject rights requests (SRRs) can be a painfully resource-intensive project. The financial burden of processing these requests averages \$1,524³ per manually handled SRR (often involving HR, legal, IT, and compliance teams), leading to inefficiencies and higher costs.

And the bad news? It gets worse as SRR volumes increase. In fact, 60%⁴ of businesses report an increase in SRRs over the past year, with some handling over 500⁵ requests weekly. It adds up, as does the time spent on this manual work. Many organizations find they can't process the requests fast enough to be in line with regulations, raising their risk of non-compliance.

Subject Rights Management Without Tears

During the first year of the California Consumer Privacy Act (CCPA), organizations in the IT sector had to process nearly 900,000 SRRs. Given that the average cost of manually processing an SRR is \$1,524, that works out to a total cost of nearly \$1.3 billion. A 10% reduction in cost from process efficiency could have saved \$130 million; a 30% improvement could have saved approximately \$390 million.

McKinsey⁶ estimated that automation could raise global productivity growth by 0.8% to 1.4% annually. A privacy program that automates SRR processes and workflows to help teams to handle more requests, faster, is a solid investment that delivers both compliance and cost savings.

Integrate, Deduplicate, and Automate Your Way to Operational Excellence

A robust data privacy program can automate processes, map data, and assess systems, information, and processes in departments across the business to not only support compliance but also directly enhance a company's operational capabilities across non-privacy functions.

Data privacy programs streamline processes across departments, reducing friction and improving workflows.



Increased Efficiency

In a Cisco study, 78%⁷ of organizations report that their data privacy initiatives drive operational efficiency. By properly managing and securing personal and sensitive data, businesses avoid costly errors, redundancies, and inefficiencies, ultimately boosting productivity and allowing organizations to reallocate resources toward innovation and growth.



Faster Sales Cycles

Privacy programs also optimize the sales cycle; 73%⁸ of companies found that investing in privacy reduced delays. With clear policies, well-documented privacy compliance practices, and a well-organized data infrastructure, sales teams can access vital information without bottlenecks, accelerating deal closures and improving customer satisfaction.

How to Drive Operational Efficiency with Osano

By automating key workflows, enhancing data visibility, and fostering collaboration between departments, Osano helps organizations optimize operations while staying compliant with privacy regulations.

- › **Osano Subject Rights Management** streamlines SRR processing by automating key tasks (including identity verification and assigning work), detecting duplicates, and using geofencing and localization to serve up the correct forms by jurisdiction.
- › Use **Osano's Data Mapping** and **Subject Rights Management** tools together to automatically delete and summarize data from designated systems. This reduces manual coordination, speeds up response times, and lowers the cost of responding to requests.
- › Easily communicate your data privacy practices to sales prospects using **Osano's Trust Center**. A transparent approach to privacy reduces delays caused by compliance concerns, speeding up the sales cycle.
- › **Osano Data Mapping** identifies how data is processed and stored across applications, allowing privacy teams to easily spot duplicate systems, data, and processes. This transparency enables better communication around the organization's tech stack, reduces data silos and shadow IT, helps optimize data processes, and promotes good compliance practices like data minimization.
- › Use **Osano Data Mapping** and **Assessments** together to foster a better understanding of each department's processes and technology.
 - Conduct assessments directly with individual departments to gain insight into specific tools and how they are used; workflows and preferences; and risks that can impact efficiency and compliance, like duplicate work, fragmentation, and sensitive data in shadow IT.
 - Drive better engagement and more accurate answers on repeat assessments by pre-populating repeat assessments with previously discovered system information, enabling the team to focus on updates rather than rework.

SECTION 4

Privacy Management Identifies and Mitigates Risk

Security and risk mitigation are top priorities, whether you're a CISO focused on strengthening security, a compliance officer managing risk, or a CFO safeguarding the company's financial interests. But many organizations carry excessive risk, especially related to sensitive data and access:

- › In one global risk report, the average company found 534,465¹ sensitive files; 17% of all sensitive files were accessible to every employee.
- › 53%² of companies found over 1,000 sensitive files that were accessible to every employee.
- › IDC found that 83%³ of companies have had at least one access-related cloud data breach.
- › 60%⁴ of companies cite insufficient visibility and access controls as a major security threat.
- › 37%⁵ of consumers surveyed received notification that their personal data had been compromised in at least one account in 2023.

Often the scope of data vulnerability is so large that companies don't know where to begin.

Risks Are Compounding

The figures above are just the risks that we know of currently. The explosion of data, combined with the increasing use of cloud services, shadow IT, and artificial intelligence, means that companies are dealing with more risks than ever before.

Since 2021:

85%⁶ of companies
have experienced some kind of a breach.

11%⁷ of those breaches
could be traced back to shadow IT.

By this year, it's estimated that:

60%⁸ of malware attacks
will originate from SaaS applications.

48%⁹ of organizations
are entering non-public company
information into GenAI applications.

Companies need to not only mitigate the risks they know exist in the business now, but also future-proof the business against threats that are quickly evolving.

Data Privacy Management: Your Head Start in Minimizing Risk

You can't protect what you can't see. Identifying and safeguarding personal sensitive data through a robust privacy program mitigates risk throughout an organization.

- If you clearly understand where your data resides and how it's being used, you know where to implement stronger security and access controls and minimize data.
- By simplifying the process of mapping data and enhancing the ability of IT and risk teams to bring unauthorized software under management, teams can reduce inefficiencies, eliminate redundant services, and ensure that every tool meets the organization's security and compliance standards.
- As AI proliferates across the organization, a comprehensive data privacy program equips privacy, IT, and risk teams with the insights and controls necessary to mitigate risks, ensuring that AI can be integrated into your operations without compromising consumer trust or regulatory compliance.

Privacy controls and data management can help IT and security teams quickly and accurately pinpoint which systems need heightened protection, enabling them to set priorities and craft a comprehensive plan to protect the whole organization against threats.

The High Cost of Privacy Risk

Companies have faced multi-million-dollar settlements or fines in multiple cases of privacy regulation enforcement. For example, a hospital system received a fine¹⁰ of \$4.75 million after failing to protect systems with protected health information, allowing an employee to access and sell patient information as part of an identity scheme. In another case, a commercial security camera provider failed to restrict employees and contractors from accessing customer videos and used them to train algorithms without user consent, resulting in a \$5.8 million settlement¹¹ with regulators.

A New Threat: Lack of Cyber Insurability

With data leaks, ransomware, malware, and even outright employee theft, cyber insurance is essential to any company's risk mitigation strategy. But what would happen if you went to file a claim for the costs associated with a data breach, and an insurer denied your claim because you couldn't demonstrate that the breached data was lawfully consented to for collection and processing? This is an increasingly likely scenario, with 31%¹² of insurance underwriters viewing privacy violations as their primary concern for 2024. Insurers may limit coverage for wrongful/nonconsensual data collection, increasing risk amidst data privacy lawsuits.

How Can Osano Help Identify and Mitigate Risk?

Osano plays a critical role in identifying and mitigating risk, enabling organizations to proactively address potential compliance gaps, reduce exposure to privacy violations, and manage data responsibly. Osano not only helps ensure compliance with evolving privacy regulations but also enhances security and financial risk mitigation, allowing teams to be part of a more holistic and collaborative approach to risk management and enforce a strong privacy posture across the organization.

- › **Osano Data Mapping** provides a comprehensive view of your data ecosystem and the actual flow of data across the organization, helping you meet compliance requirements, assess risk, and support data minimization.
- › **Osano's Vendor Privacy Risk Management** helps identify, track, and mitigate potential third-party data privacy risks in your vendor ecosystem by analyzing hundreds of data points in vendor security and privacy documentation.
- › Together, **Osano's Cookie Consent** and **Unified Consent & Preference Hub** ensure user data is consented to, properly recorded, and easily auditable, bolstering the value of your data and meeting evolving obligations, such as those related to cybersecurity insurance.
- › Identify, quantify, manage, and communicate privacy and data risks to the organization with **Osano Assessments**, its collaboration functionality, and integrations with **Osano's Data Mapping** and **Vendor Privacy Risk**.
- › With **Osano Data Mapping**, unlock a complete view of personal and sensitive information—its storage, movement, and ownership—to help organizations better minimize data collection and limit potential exposure of data in the event of compromise.
- › Automate both SRRs and consent management, reducing the risk of human error and non-compliance, including the ability to notify sub-processors of data when subject rights requests are received. This helps reduce the likelihood of fines, penalties, and reputational harm to the organization.
- › Evaluate the risk of processing personal information in AI systems with **Osano's AI Assessment Template**.

SECTION 5

Transform Compliance into a Business Advantage

A robust privacy program not only safeguards your business from regulatory penalties but also enhances key business functions, leading to measurable improvements across the organization. Use this guide to initiate conversations within your teams and align your strategy around the significant business benefits of a robust privacy program, positioning your company for long-term success.

(For concrete advice on using the insights from this guide to gain buy-in for privacy program enhancements, download our companion guide, [Building the Business Case for Data Privacy](#).)

By building trust with customers, driving more effective and consent-based marketing, streamlining operations, and proactively identifying risks, privacy programs create a ripple effect of benefits. These advantages extend beyond the legal and compliance teams to marketing, IT, security, and leadership, transforming privacy into a key driver of growth and innovation.

Whether your organization is just beginning its privacy journey or looking to enhance its existing program, Osano's expertise and technology can help you achieve these outcomes. Investing in privacy is not just about avoiding risks—it's about unlocking opportunities that drive long-term success.

SECTION 6

About Osano

Navigating the complexities of privacy compliance can be daunting, but Osano turns complexity into clarity. As global regulations continue to evolve, Osano provides a unified, scalable platform designed to meet your organization's most critical privacy needs. Osano not only mitigates the risk of non-compliance but also drives operational efficiency and strengthens customer trust.

Osano simplifies essential tasks like data mapping, subject rights management, and vendor risk evaluations, giving you greater visibility and control over your data. By automating these processes, Osano reduces the burden on privacy teams, minimizes the risk of human error, and ensures that privacy management is both efficient and effective. With seamless integration into existing systems, Osano enhances your workflows without causing disruption, allowing your organization to maintain compliance as it grows and regulatory demands change.

With Osano, privacy compliance becomes a strategic advantage, empowering your organization to protect trust, reduce risk, and thrive in a complex digital landscape.

Endnotes

Introduction

- 1. [Cisco 2024 Data Privacy Benchmark Study](#).
- 2. [“From Privacy and Trust to ROI,”](#) Robert Waldman, Cisco Security Blog, January 27, 2020.

Section 1: Privacy Builds Trust with Customers

- 1. [Cisco 2024 Data Privacy Benchmark Study](#).
- 2. [“How Americans View Data Privacy,”](#) Pew Research Center, May 2023.
- 3. [IAPP Privacy and Consumer Trust Report, March 2023](#).
- 4. [IAPP Privacy and Consumer Trust Report, March 2023](#).
- 5. [Global Consumer State of Mind Report 2021](#), Truata.
- 6. [“Customers want control over their data – and won’t hesitate to switch brands to get it,”](#) Maria Helena Marinho, Elizabeth Tran, Future of Marketing, Google, February 2023.
- 7. [“The Consumer Data Opportunity and the Privacy Imperative,”](#) Venky Anant, [Lisa Donchak](#), [James Kaplan](#), and [Henning Soller](#), McKinsey, April 27, 2020.
- 8. [Pew Research Center Survey](#), June 2019.

Section 2: Privacy Improves Marketing Effectiveness

- 1. [Forbes Advisor](#), June 2024.
- 2. [Forbes Advisor](#), June 2024.
- 3. [Forbes Advisor](#), June 2024.
- 4. [Google/Greenberg Survey](#), March 2018.
- 5. [The State of Personalization 2021](#), Twilio/Segment.
- 6. [2018 Personalization Pulse Check](#), Accenture.
- 7. [The State of Personalization 2021](#)21, Twilio/Segment.
- 8. [“A customer-centric approach to marketing in a privacy-first world,”](#) [Marc Brodherson](#), [Adam Broitman](#), Jason Cherok, and [Kelsey Robinson](#), McKinsey, May 20, 2021.
- 9. [Privacy By Design Report](#), Google, 2023.
- 10. [Privacy By Design Report](#), Google, 2023.
- 11. [Privacy By Design Report](#), Google, 2023.
- 12. [Privacy By Design Report](#), Google, 2023.

Section 3: Data Privacy Programs Improve Operational Efficiency

- 1. [Workgeist Report 2021](#), Cornell University Idea Lab.
- 2. [“The State of SaaS Sprawl in 2021,”](#) Productiv.
- 3. [“Top Trends in Privacy Driving Your Business Through 2024,”](#) [Nader Henein](#), [Bart Willemsen](#), [Bernard Woo](#), Gartner, May 5, 2022.
- 4. [2023 EY Law Survey](#).
- 5. [Dimensions Data and Truyo Survey](#), May 2020.
- 6. [“A Future that Works: Automation, Employment, and Productivity,”](#) McKinsey Global Institute, January 2017.
- 7. [Cisco 2024 Data Privacy Benchmark Study](#).
- 8. [Cisco 2024 Data Privacy Benchmark Study](#).

Section 4: Privacy Management Identifies and Mitigates Risk

- 1. [2019 Global Data Risk Report](#), Varonis Data Lab.
- 2. [2019 Global Data Risk Report](#), Varonis Data Lab.
- 3. [IDC/Ermetic Survey](#), 2021.
- 4. [IDC/Ermetic Survey](#), 2021.
- 5. [U.S. News and World Report Digital Privacy Survey 2024](#).
- 6. [Infosecurity magazine](#), 2023.
- 7. [Infosecurity magazine](#), 2023.
- 8. [Netskope Cloud and Threat Report](#), 2024.
- 9. [Cisco 2024 Data Privacy Benchmark Study](#).
- 10. [U.S. Department of Health and Human Services](#).
- 11. [“Amazon’s Ring agrees to pay \\$5.8 million to settle FTC spying suit,”](#) Makena Kelly, The Verge, May 31, 2023.
- 12. [Looking Ahead: Cyber Liability Insurance Concerns in 2024](#), Woodruff Sawyer, January 2024.