relyanceai

Achieve Trust with Confidence

How your privacy team can answer the 3 most challenging privacy questions:

- Where is all of our PI and sensitive enterprise data?
- How do I know we're compliant?
- How can we proactively identify new risks?

Introduction

The growth in the volume of data generated and collected has been staggering, with some studies suggesting the volume of data generated globally doubles every two years. Reinforcing this forecast, by 2025, it's estimated there will be more than 75 billion connected IoT devices worldwide, generating massive amounts of data from sensors, smart devices, and industrial equipment. Add in new AI initiatives, and it's estimated that we'll be generating 463 million zettabytes of data every day! Against this backdrop, safeguarding sensitive information and respecting individuals' privacy rights have become a strategic imperative for organizations across all industry sectors.

A robust privacy program goes beyond mandated compliance, serving as a beacon of trust that fosters stronger customer relationships, attracts new clients, and cultivates a culture of transparency and accountability within an organization. By prioritizing privacy compliance and data protection, companies can mitigate the risk of data breaches, regulatory penalties, and reputational damage from loss of consumer trust, while also unlocking opportunities for innovation and differentiation.

Where is all our PI data?

463

Million zettabytes created daily by 2025

Raconteur, 2023

Am I compliant?

$1.32B

Privacy lawsuits in 2023

Relyance internal assessment

What about new risks?

85%

Execs plan to use AI heavily in business

2023 KPMG AI Risk Survey

The primary challenge most financial leaders have today is knowing if they are meeting their obligations to customers and regulators. So, in this guide, we provide a step-by-step playbook to building a privacy compliance framework on top of a foundation of verified trust and compliance.

This guide will cover:

- Three essential questions every privacy team must answer with confidence:
  - Where is all of our PI and sensitive enterprise data?
  - How do we know we're compliant?
  - How can we proactively identify new risks?
- Today, first-generation privacy tools are exceedingly manual, which leads to poor data map quality, which leads to challenges to proving compliance, which leads to being reactive to new risks. Exactly the opposite of what we need!
- The solution is to build trust into a privacy program's foundation, ensuring that the PI data that is actually flowing through your systems meets the obligations you have to auditors and customers, 100% of the time.
- Upon this foundation, we can ensure that we have accurate compliance workflows in place, ROPAs, DSRs, and other processes.
- And when new vendors are brought on board or changes are made to the code and applications in use, we need to know what to prioritize and take action.
- With this level of automation and risk management in place, we can focus all our time on business impact – ensuring privacy by design in the products your company is building, customer trust, and complete data governance over your company's most important data.

Three Questions Every Privacy Team Needs to Confidently Answer

Cementing the foundation of any privacy program – whether a program in its infancy or a mature program keeping pace with the growth of data – requires answering three questions:

Where's My Data?

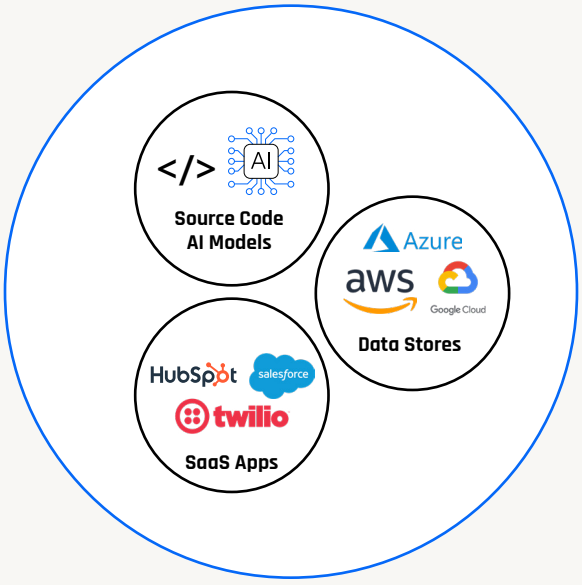
This fundamental question lies at the core of any robust privacy strategy. Privacy teams need to have a comprehensive understanding of the data lifecycle within their organization, including its creation, storage, transmission, and deletion. They must meticulously map out the flow of data across systems, networks, and applications to understand its exact locations and who has access to it at each stage.

By answering this question definitively, privacy teams can effectively implement controls and safeguards to protect sensitive information, ensuring it remains secure and compliant with applicable regulations.

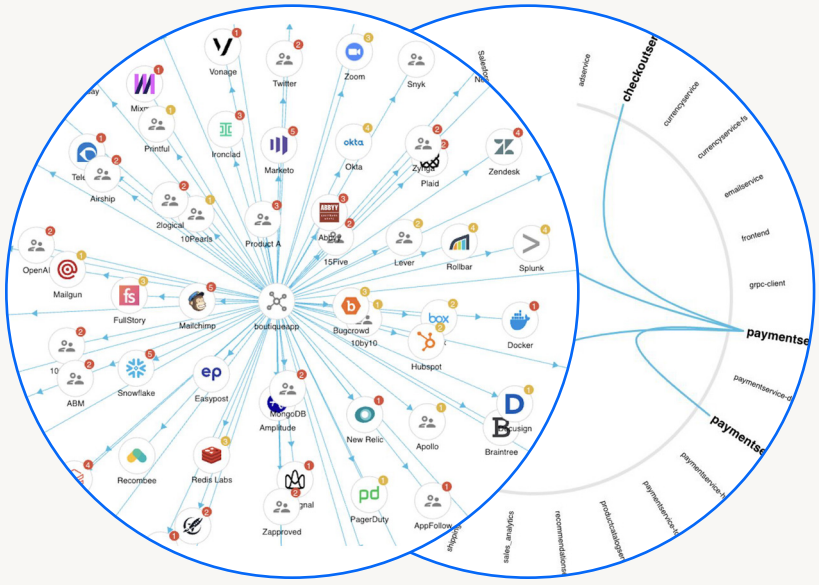
Where is all of our PI and sensitive enterprise data?

Source code, SaaS Apps, AI models, multi-cloud data stores

At rest



In motion



Am I Compliant?

Ensuring compliance with relevant laws, regulations, and industry standards is the responsibility of every privacy team. They must continuously assess and evaluate their organization's practices against the evolving legal landscape to determine whether they are meeting their obligations.

This involves conducting thorough audits, gap analyses, and risk assessments to identify areas of non-compliance and take corrective action promptly. Confidence in compliance not only safeguards against regulatory fines and penalties, but also fosters trust among customers and stakeholders, affirming the organization's commitment to ethical data handling practices.

Where is My Risk?

Understanding and managing risk is essential for maintaining a resilient privacy program. Privacy teams need to proactively identify and assess potential threats and vulnerabilities that could compromise the security and privacy of data, conducting regular risk assessments, analyzing data flows, and evaluating the effectiveness of existing controls.

By identifying areas of heightened risk, privacy teams can prioritize resources and implement targeted mitigation strategies to fortify their defenses against data breaches, cyber-attacks, and regulatory enforcement actions. Adopting a proactive posture in risk management contributes to ongoing compliance and strengthens the organization's overall resilience in the face of evolving threats.

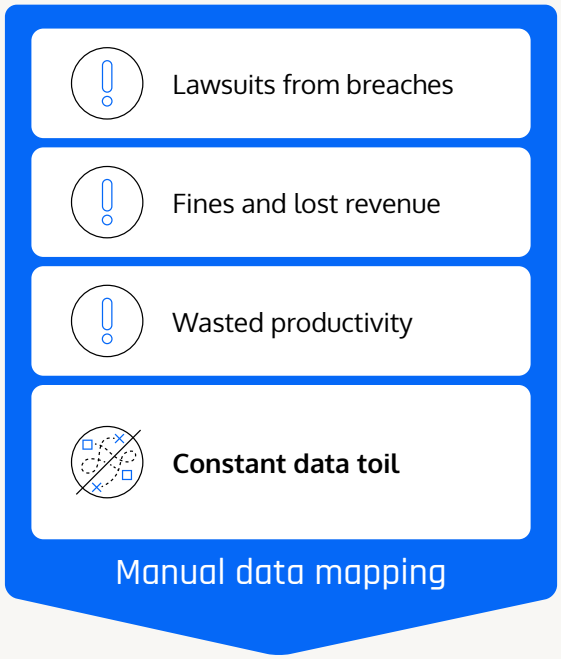
Two Approaches to Answering These Questions

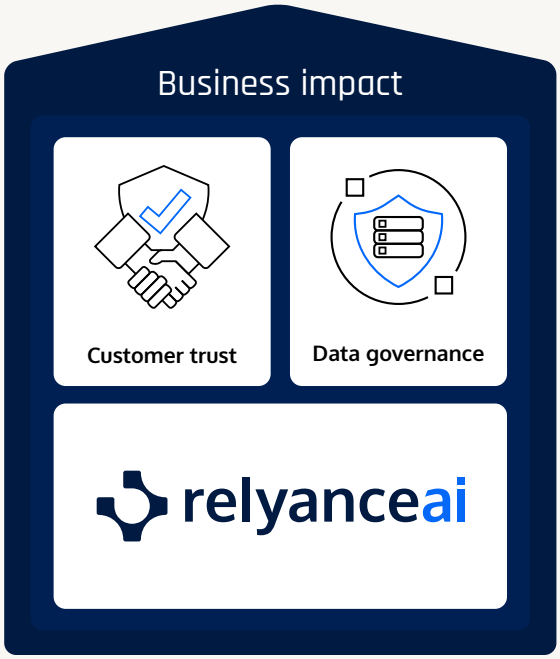
2016 is largely considered the year when privacy regulation forced organizations to understand their responsibilities around data. In April 2016, the European Union adopted the groundbreaking General Data Protection Regulation (GDPR), the first comprehensive set of privacy regulations, although the law didn't take effect for another two years.At the time, there were no vendors offering privacy management software or platforms, so a privacy program was, by necessity, built on manual methods rather than an in-the-code approach.

First-Generation Data Mapping

Some organizations in the early stages of building privacy programs and today continue to rely on manual methods, at least as a starting point. But a privacy program based on manual methods relies heavily on human intervention and procedural controls to manage data privacy and protection. A manual approach, by definition, builds in wasted time. This method produces poor data map quality, rapidly outdated results, and creates challenges for privacy teams to prove compliance. The end result is broken trust among all stakeholders, including an organization's leadership as well as customers and regulators.

A foundational decision with business impact





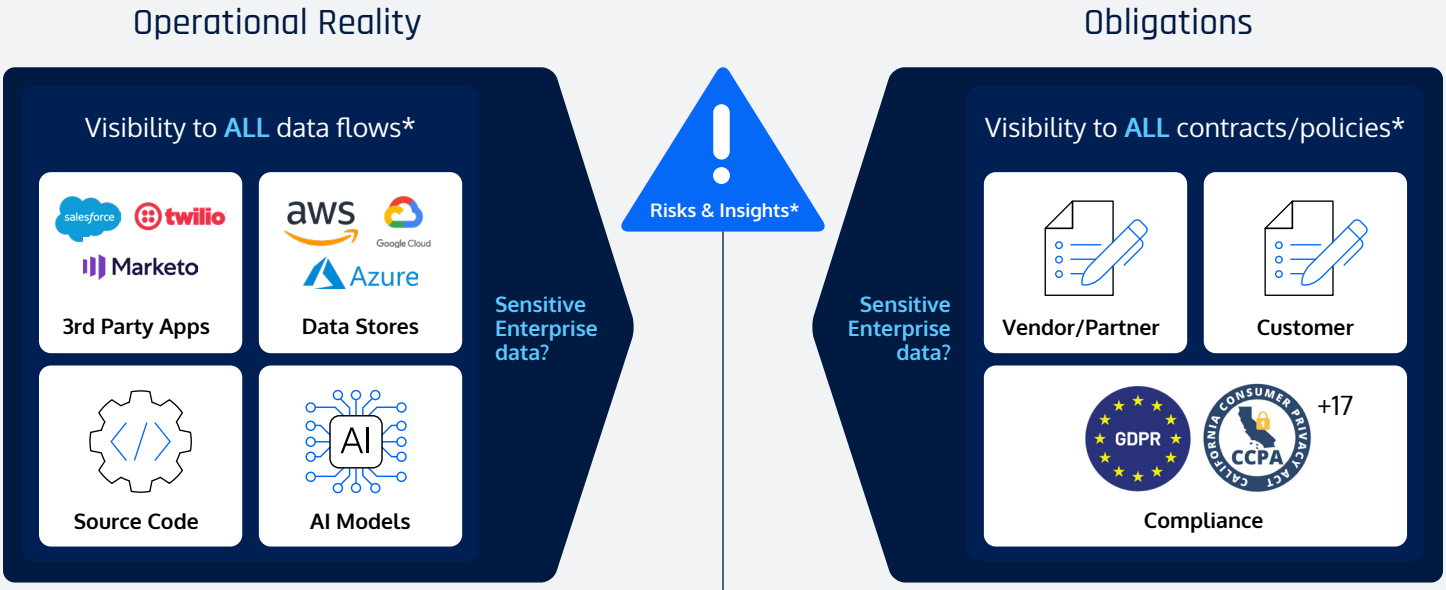
Building Privacy Using an In-the-Code™ Approach

Trust begins with understanding an organization's reality, and then aligning it to the regulatory obligations. An in-the-code approach delivers that alignment, because the code includes all the information needed for an organization to meet its privacy obligations to customers and regulators. An in-the-code platform integrates privacy controls directly into the software and systems architecture, embedding privacy by design principles and protections at the foundational level of the technology stack. With this type of data privacy management platform, an organization has visibility to all its data flows, as well as visibility to the requirements outlined in its contracts and policies with third-party vendors.

By continuously scanning the data flows and comparing the results against the contract requirements, the platform produces valuable proactive risk insights, such as data misalignments, weak security controls, missing or unsigned contracts, and the need for new assessments – all of which are flagged for the privacy team for immediate action. Overall, this approach fosters a culture of privacy by design by making data protection an inherent aspect of the technology infrastructure, rather than relying solely on manual oversight and enforcement.

Holistic customer trust and data protection requirements

All operational reality meets all obligations



*Unique to Relyance

- Data misuse or data leak
- 3rd party PI/sensitive data flow
- End-to-end application flow and lineage
- Supply chain risk analysis
- Data residency violations
- New risk assessment needed
- Shadow IT/weak security controls
- Contractual obligations violation
- Keep up with compliance frameworks

Privacy automation is the key to building privacy using an in-the-code approach, leveraging technology and streamlined processes to ensure efficient compliance with privacy regulations and safeguarding sensitive information. This approach begins with a solid foundation built through data inventory and mapping, and then implementing and automating other privacy best practices and compliance processes includingcomprehensive data inventory and mapping, Privacy Impact Assessments (PIAs), Records of Processing Activities (ROPAs), vendor management, automated Data Subject Requests, and data minimization strategies.

The goal is to enable organizations to manage privacy programs proactively, aligning security measures with privacy obligations, conducting regular privacy audits, and building a process for continuous improvement and adaptation to the evolving privacy landscape and regulatory environment. By employing automation tools, integrating workflows, and fostering collaboration across legal, compliance, and privacy teams, organizations can establish a robust privacy management system, mitigate risks, and build trust with customers and regulators while navigating the complexities of modern privacy requirements.

Answering the 3 Privacy Questions Through an In-the-Code™ Approach

Solving 'Where's My Data?' with Automated Data Inventory and Data Mapping

Automated Data Inventory

A data inventory is a comprehensive record or catalog that documents all the types of data collected, stored, and processed by an organization. This inventory typically includes details such as the types of data, its sources, purposes for collection, storage locations, and any third parties with which the data is shared.

An automated data privacy management platform builds a data inventory by employing software tools and algorithms to systematically scan, collect, and categorize data across all systems and databases within an organization – including source code, SaaS apps, AI models, and multi-cloud data stores. These automated processes identify and document the types of data collected, their sources, storage locations, and associated metadata. In addition, automation enables continuous monitoring and updating of the data inventory as new data is generated or existing data sources change, ensuring its accuracy and relevance over time.

Automated Data Mapping

A data map is a systematic depiction of how data in the inventory exists and flows that identifies and categorizes all data within an organization, and any associated relationships, enabling a comprehensive understanding and management of sensitive information.

Similar to the way automation streamlines the development of a data inventory, automation builds a data map by employing specialized software tools and algorithms to scan, analyze, and categorize data across an organization's systems, networks, and applications. An in-the-code data privacy management platform automatically identifies data sources, extracts relevant metadata, and maps relationships between different data elements. Through automated processes, data maps are created quickly and accurately, providing organizations with a comprehensive inventory of their data assets. In addition, an automated platform continuously monitors and updates the data map as new data is generated or existing data sources change, ensuring its accuracy over time.

Challenges

- Months to build data map w/ team of 4
- Static snapshots quickly outdated
- 600+ vendors, 100s changes/week

Building a world-class vendor management program that is:

- **Automated:** Live data map built in hours
- **Accurate:** Validated map and ROPA accuracy
- **Scalable:** 2 hrs/wk to manage exceptions

Samsara is a leading industrial Internet of Things ("IOT") company bringing real-time visibility, analytics, and AI to operations.

Solving 'Am I Compliant?' with Accurate Compliance Workflows and Processes

Records of Processing Activities (ROPAs)

A ROPA, or Record of Processing Activities, is a crucial component of a privacy program, particularly under privacy laws like the EU's General Data Protection Regulation (GDPR). A ROPA serves as a comprehensive register that documents an organization's data processing activities.

Automation ensures the accuracy of ROPAs by systematically collecting and updating data from various sources within an organization, minimizing manual errors and inconsistencies. By employing predefined algorithms and rules, automation can generate ROPAs that are complete and correct to a high degree of accuracy, enabling compliance with privacy regulations. In addition, automation facilitates the customization of ROPAs to meet the requirements of multiple jurisdictions by dynamically adjusting data maps, classifications, and processing activities based on relevant legal frameworks. This adaptable approach allows organizations to generate ROPAs tailored to specific legal contexts, ensuring applicability across diverse regulatory environments while maintaining accuracy and consistency in compliance documentation.

Privacy Impact Assessments (PIAs)

A Privacy Impact Assessment (PIA) is a systematic evaluation process used to identify and assess the potential risks, benefits, and impacts associated with the processing of personal data. PIAs are a critical tool in privacy programs, particularly under regulations like the GDPR and various U.S. state laws, such as the California Consumer Privacy Act (CCPA), as they help organizations proactively identify and mitigate privacy risks.

Automation streamlines the development of PIAs by providing standardized templates and workflows, guiding organizations through the assessment process efficiently. By analyzing data sources and processing activities automatically, automation helps organizations identify when a PIA is needed based on predefined criteria or triggers, assisting with proactive compliance with privacy regulations. Compared with manual methods, automation can save up to 85 percent of the time typically required for conducting PIAs, enabling organizations to allocate resources more effectively and accelerate their compliance efforts.

Vendor Risk Management

Vendor Risk Management focuses on assessing and managing the privacy and data protection risks associated with third-party vendors and service providers that process personal data on behalf of an organization. Organizations should have contractual agreements with third parties that outline specific privacy and security requirements, including data protection obligations, breach notification procedures, and audit rights.

An in-the-code approach significantly improves vendor risk management by automating the assessment and monitoring of vendors' privacy practices and compliance with contractual obligations and regulatory requirements. By leveraging automated processes, organizations can efficiently identify and prioritize vendor risks, ensuring proactive mitigation strategies are implemented to safeguard data privacy.

Data Subject Requests (DSRs)

Data Subject Requests (DSRs) encompass the rights granted to individuals under data protection regulations, including the EU's GDPR and various U.S. state laws, such as the CCPA. DSRs enable individuals to exercise control over their personal data by requesting access, correction, deletion, or restriction of processing.

Automation plays a key role in managing DSRs by efficiently handling request intake, verification, and response processes. By automating workflows and tasks such as data retrieval and redaction, organizations can ensure timely and accurate responses to DSRs, enhancing compliance with privacy regulations. Leveraging automation minimizes manual effort, reduces the risk of errors, and enables scalability to effectively manage a high volume of DSRs.

AI2 Allen Institute for AI

Challenges

- Trillions of pieces of data with PI in AI models
- 1000s of repositories, diversified team
- Privacy team of one! No time, resources
- Non-technical privacy team

Building a World-Class Privacy Program that is:

- **Cross-functional:** "Relyance gives us a common language."
- **Automated:** "1 hour per week to catch issues before they become big."
- **Accurate:** "All personal data is going where it's supposed to go."
- **Confident:** "We've done everything we can to protect privacy in models."

Allen AI is Paul Allen's globally distributed, AI non-profit organization that is researching how AI can help the common good.

Solving 'Where Are My Risks?' with Intelligent Insights

Typical approaches to continuously maintaining compliance involve time-consuming manual review of contracts, new vendors, new partners, and new customer contracts. After this first part of the process is complete, privacy teams then need to compare these new requirements to the data that is actually being shared, which involves more meetings and forms.

AI can automate ongoing verification of trust by alerting you when there's an obligation that isn't being met. When implementing an intelligent platform like Relyance AI, the system immediately generates a number of insights that alert privacy teams to take action, including:

- "Data Protection Impact Assessment not found - Vendor or Product assessment may be required"
- "Privacy Shield detected as a basis of transfer"
- "Former Standard Contractual Clauses (SCCs) detected as a basis of transfer"
- "No Personal Data Types detected in DPA"
- "DPA may not be fully executed"
- "Broad DPA language detected. May require review"
- "Review may be needed: Potential data misalignment"
- "Contract(s) were not identified"

These insights help you identify risks and achieve compliance, making sure all contracts are in place and accurately represent the data flows, the right contracts and data transfer mechanisms are in place, and alert you to the need to conduct any assessments needed based on the personal data processed.

When a privacy program is up and running, the Intelligent Insights module of the Relyance AI platform flags additional issues that may require action to maintain a world-class privacy program, including:

- "Personal Data Type Change Detected in Vendor or Product - Assessment Review Suggested"
- "Personal Activity Change Detected in Vendor or Product - Assessment Review Suggested"
- "New Special Category of Data Detected - Assessment Review Suggested"

In addition, "User Generated Tasks" can be created on the fly and are helpful at all stages of building and maintaining a privacy program because they are completely customizable and configurable by the Relyance AI platform user. These tasks can be created as the privacy team notices issues when verifying the Data Inventory & Map, Universal ROPA, Vendors, and Data Protection Assessments, and later as new data changes are identified or as ad hoc privacy requests are received. User Generated Tasks can also be created as a user goes through an assessment and identifies tasks needed to either complete the assessment or remediate risks identified via the assessment.

PLAID

Challenges

- Goal to get 100% of vendors on standard data protection terms
- Long list of vendors without visibility into data types, language being used
- Manual spreadsheet approach didn't work

Building a world-class vendor management program that is:

- **Automated:** Automatically scan all **vendor contracts**
- **Standardized:** Identify if DPA is sufficient or **what changes need to be made**
- **Scalable:** **Proactively identify new vendors** and ensure compliance

Plaid is in the open banking space and helps customers safely move financial information from one financial service to another financial service.

Building a World-Class Privacy Program on a Foundation of Trust

A well planned and strategically implemented privacy program enables organizations to lay a foundation that prioritizes privacy at every level. From implementing comprehensive data governance frameworks to fostering a culture of data protection and privacy awareness, each step is integral to building a holistic program that not only meets regulatory requirements but also aligns with ethical principles and strengthens customer trust. A world-class privacy program – particularly one built with an in-the-code approach – enables organizations to leverage data responsibly, unlocking insights that drive innovation and fuel business growth.

In addition, the implementation of an automated data privacy management platform offers privacy professionals the opportunity to focus on tasks beyond the realm of privacy management. With routine compliance tasks streamlined through automation, privacy professionals can redirect their time and expertise toward strategic initiatives such as data-driven decision-making, enhancing customer experiences, and driving overall business innovation. By shifting their focus to these value-added activities, privacy professionals can contribute to revenue generation, operational efficiency, and competitive differentiation, demonstrating the broader business value of a comprehensive privacy program. Ultimately, investing in a world-class privacy program is an investment in the long-term success and sustainability of an organization, harnessing the full potential of their privacy teams to mitigate risk while driving tangible business outcomes.