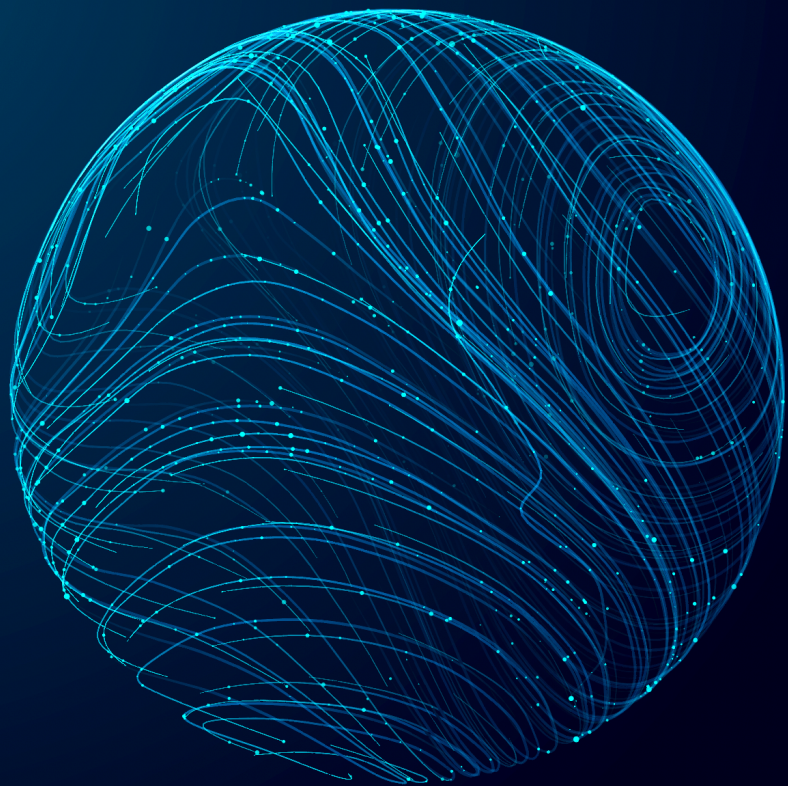


RELYANCE AI

Using Data Inventory and Mapping to Navigate a Complex Regulatory Environment

A sustainable data protection program is critical infrastructure for building and maintaining trust with users, customers, partners, and regulators. Just like a house, a program built on a weak foundation will crumble under stress. Manual data inventory and mapping practices can't maintain pace with the speed and volume of real-time data flows, and any pillars built on this data quicksand will sink when tested. Learn how a full understanding of data inventories and data flows can allow you to create a seismic-proof, yet lean, privacy program.



Background

The dramatic growth in data-driven technologies across every sector of the economy has spurred a worldwide push for more rigorous data protection legislation. The GDPR,¹ CCPA,² LGPD,³ PDPA,⁴ and other data protection regulations with extra-territorial reach are poised to test the ability of countless organizations to develop and maintain an adequate data protection and privacy program. Failure to meet the standards set out in these regulations can be disastrous. 2020 and 2021 have seen some of the largest fines ever issued by Data Protection Authorities in the EU, such as the \$746,000,000 and \$50,000,000 fines issued to Amazon and Google respectively, for failures to comply with the GDPR. It's not hard to see how the fines add up: failure to comply with some of the basic requirements established in the GDPR may result in fines equaling up to 4% of annual turnover.

As both international and domestic organizations react to the current regulatory environment and anticipate further developments in the data protection space, many legal, privacy, and data security teams find themselves stuck in a reactionary cycle that causes them to spend an inordinate amount of their resources on privacy compliance. On top of devoting significant resources to developing and implementing the finer points of a compliance program in response to every new regulation and development, many organizations spend major portions of their budget on outside counsel fees.

1 General Data Protection Regulation 2016/679 in the European Union.




2 California Consumer Privacy Act.

3 General Personal Data Protection Law 13709/2018 (LGPD) in Brazil.

4 Personal Data Protection Act 2012 in Singapore.

This landscape leaves many in-house privacy teams feeling overwhelmed and in a position where they need additional resources to maintain operational compliance, all the while having their budget requests heavily scrutinized and often rejected by their business colleagues. However, your privacy team will be able to respond to privacy developments more nimbly and effectively—even in a lean state—if you are able to develop a full understanding of your organization’s data inventory and data flows.

Still, many organizations struggle to devote the time and resources necessary to manually create a data inventory and map, or rely on the assistance of outside counsel to do so, leaving them with significant blindspots about their processing activities and data flows. While the subject matter expertise offered by internal experts and outside counsel remains important for most organizations, smart privacy teams can significantly reduce their resource spend by distilling their compliance and data strategy down to three fundamental questions, which encompass the foundational principles of data governance:

-  What personal data does your organization possess?
-  Who has access to that data?
-  How is that data collected and used?

Global Compliance, Risk Management and Data Strategy Centered Around These Foundational Principles

Data inventories and maps not only form the bedrock of successful privacy programs, but they are also required in order to maintain compliance with certain data protection regulations. Both the GDPR⁵ and LGPD⁶ require organizations that process personal data to maintain records of their processing activities, also known as “ROPAs.” Privacy professionals also expect ROPAs to become required by regulations issued by the California Privacy Protection Agency pursuant to the CCPA⁷. Among a number of other items, organizations are generally required to include in their ROPAs information about the categories of data subjects involved in the processing, and the nature of their personal information being processed. In addition, these organizations must also keep records of their data transmissions, including the identity of any recipients of that personal data and any transfers of that data over some international borders.

While they bring a great deal of value to organizations that create them beyond being merely a compliance tool, ROPAs are one of the most onerous data governance requirements for organizations to meet, regardless of whether they are a controller or processor⁸ of personal data. However, the heavy lifting involved in surveying each department’s data repositories within an organization, and developing an understanding of how and where that data is transmitted, is virtually impossible unless an organization already has developed a data inventory and map, which together provide virtually all the insights needed to generate compliant and instructive ROPAs.

Even where not required by law, data inventories and maps are still important foundational tools in data governance as they allow organizations to survey their data repositories, understand what data is in and out of the scope of relevant data protection laws, and take a strategic view towards data governance and compliance.

5 GDPR Article 30.

6 LGPD Article 37.

7 The California Consumer Privacy Act of 2018, recently amended and expanded by the California Privacy Rights Act.

8 Under GDPR Article 4, a “controller” is “a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means” of its data processing operations. A “processor”, on the other hand, is a “natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”. The definitions of each under the LGPD are similar.

Often, organizations that process personal data tend to focus primarily on data protection regulations that are commonly reported on in the media or trade publications such as the GDPR, or that apply in their home jurisdiction, like the CCPA in the case of California-based companies. However, the GDPR⁹, CCPA¹⁰, and most other major data protection regulations can apply to organizations outside of their own jurisdiction, based on the nature of the personal information those organizations possess. By maintaining up-to-date data inventories and maps, organizations can determine which data protection regulations apply to them relatively easily and cheaply, as their internal privacy teams and/or outside counsel will not have to complete the data discovery process while analyzing the organization's regulatory exposure and performing a gap analysis to identify and close compliance oversights.

Data inventories and maps also serve strategic purposes. In addition to providing insights as to what data protection regulations may apply to your organization, data inventory management and mapping can help an organization create and execute on their data strategy, by generating deep insights into the nature of its processing operations, and identifying the potential for new regulations to apply due to changes in processing activities or the ingestion of new data. With these insights at hand, organizational management can more effectively weigh the commercial benefits of a potential data strategy against the compliance-related costs to be incurred in creating a new data governance program, or adding any additional features to your existing program based on the application of new laws.

Lastly, data inventory and mapping allow organizations to reduce risk in what is arguably one of the most vulnerable areas of data protection: vendor management. Here, inventories and maps can answer two of the foundational questions proposed above: who can access your data, and how is it being collected and used? By identifying who the recipients of your organization's personal data are, privacy and information security teams can ensure that their vendors' data governance and protected practices are thoroughly vetted, thereby reducing the risk of a data breach or other security incident due to a vendor having faulty or insufficient security controls in place.

9 Under Article 3(2) of the GDPR, the law applies to any processing of personal data of data subjects in the EU, regardless of the location of the controller or processor, if the processing activities relate to the sale of goods or services into the EU, or the monitoring of data subject behavior within the EU.

10 Section 1798.140 of the CCPA provides that any organization that processes personal information of California residents may become subject to the law if they meet one of three threshold requirements.

Manual Data Inventory and Mapping Practices Are Costly, Time-Consuming, and May Increase Risk for Your Organization

Manual data inventory and mapping practices can't maintain pace with the speed and volume of real-time data flows, engineering teams, and business processes, and any data governance built on them is likely to fail. As mentioned above, privacy and security teams have to date spent an inordinate amount of time and resources developing and updating their understanding of (i) what information their organization possesses, (ii) who has access to that data, and (iii) how that data is collected and used. However, due to the size and complexity of many organizations' processing activities and data inventories, the inventory and maps the privacy team painstakingly create are often outdated by the time they are finalized.

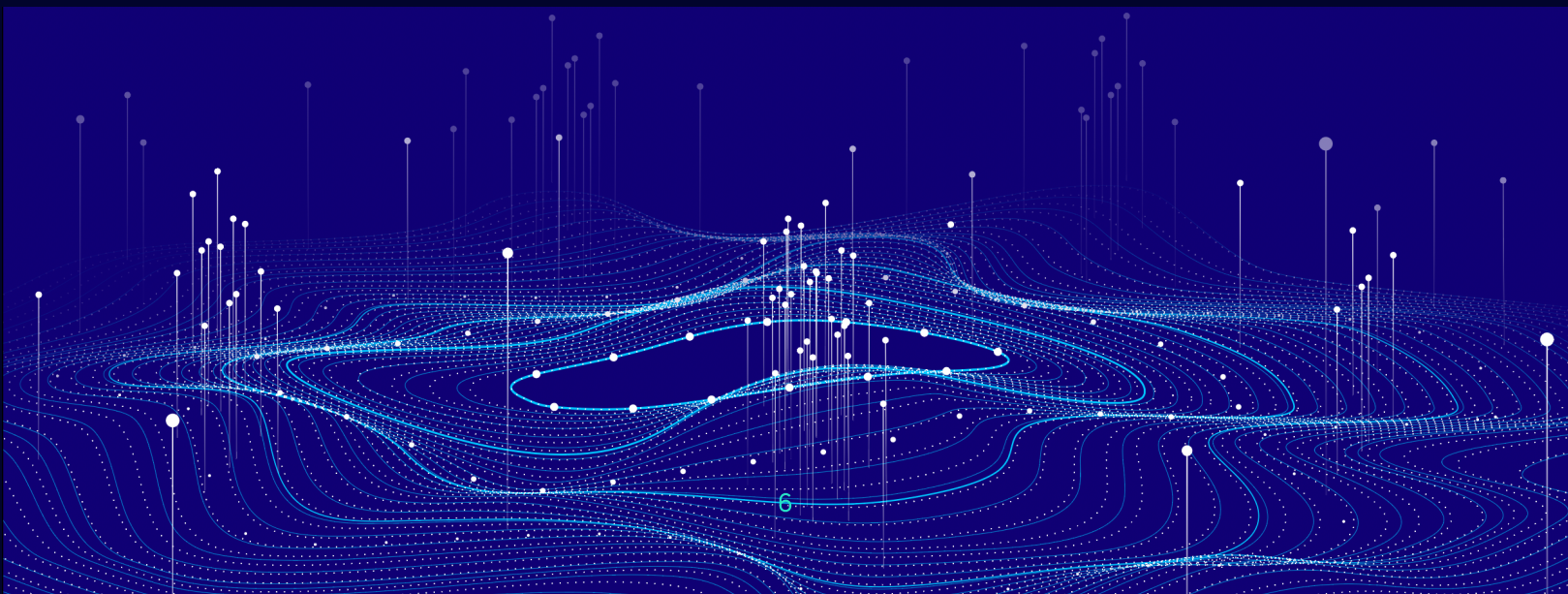
Any privacy program built on such an out-of-date understanding of an organization's data will struggle and likely fail to meet even the most basic requirements that exist in most data protection regulations: the creation of ROPAs, evaluation of data processor vendors, and management of data subjects exercising their rights to control their own data, commonly through requests referred to as Data Subject Access Requests, or DSARs. Failure to meet those requirements, particularly the efficient management of DSARs, will leave organizations exposed to potential penalties including fines and other regulatory enforcement.

There are a few tools on the market that are advertised as "automated" solutions. However, these tools often merely shift the pain of manual workflows onto your browser, essentially providing an organizational tool where most of the relevant information about your organization's processing activities and data inventory must be entered manually. Even tools that feature more automated workflows, once installed on your network or machine, create an entirely new problem: increased privacy and security risks. Onboarding a new privacy and data protection tool should not produce vulnerabilities, but should instead play a role in your overall data protection strategy, leaving your data in its safest state—untouched. Most critically, any solution that does not rely on a live data inventory and data map will open up all compliance efforts to oversight, unintentional mistakes, and doubt.

Live Data Inventory and Mapping to the Rescue

The Relyance AI Platform leverages a number of low-touch integrations to create a fully automated, live, and continuously monitored and managed data inventory and map as your privacy program's blueprint, freeing up resources for your privacy team and reducing your spend on outside counsel and consultants.

Our comprehensive data protection and privacy platform uses proprietary machine learning and intelligent instrumentation to automate data discovery, analysis, inventorying, and mapping, while reducing resource waste, all without requiring access to your organization's underlying personal data. Our cross-functional and centralized platform is the robust and scalable foundation that gives every team visibility into current data flows, preventing unwanted data incidents, promoting cooperation within and between teams, and creating a trickle-up effect of confidence across your organization.





The information provided on this paper does not, and is not intended to, constitute legal advice; instead, all information, content, and materials in this paper are for general informational purposes only. The information provided in this paper may not constitute the most up-to-date legal or other information. Readers should contact an attorney to obtain advice with respect to any particular legal matter.