

# Data Mapping Best Practices

Data mapping for data privacy can be a bit of a mystery – what needs to go into a data map? What do you need to avoid? How do you ensure that your organization is keeping track of all of the risk associated with your collection of personal information? In this checklist, we've gathered some of the top tips and best practices you should keep in mind:

## **Make It One of Your Privacy Professional's Core Responsibilities**

Like compliance itself, data mapping is an ongoing process; not a one-and-done task. That means data mapping isn't an appropriate task to assign to, say, your IT personnel, who have a slew of other responsibilities to attend to and will be therefore more inclined to treat it as a special project.

Data mapping is best handled by a dedicated privacy professional whose sole responsibilities are compliance activities like data mapping.

## **Prioritize Mapping Systems With the Riskiest Data**

If you're aware of systems that collect, process, and/or store sensitive data or particularly large quantities of data, that's where you should begin your data mapping work. Odds are, there will be downstream flows that need to be accounted for, opportunities to reduce unnecessary data collection, or additional security measures you can employ.

## **Acknowledge Unknown Unknowns**

You may not know exactly what privacy risks exist in your organization's various systems, but you at least know where to look to find out—right?

In reality, you'll almost never have a complete picture of all the systems and PI collection points at play in your organization. It's important to acknowledge this reality and make plans to discover where unknown stores of PI may exist.

## **Avoid the Data Science Bottleneck**

There's a major drawback to leveraging business intelligence and data science in mapping your organization's PI landscape: If your organization has these resources in place, it's generally because they're needed for a multitude of tasks. Data privacy compliance, unfortunately, will likely fall low on the list of data science priorities. Even when privacy-focused data mapping's turn comes up, the data science team likely won't have the same understanding of requirements as a privacy professional would.

## Use an Automated, Privacy-Focused Data Mapping Tool

As a consequence, it's best to secure a privacy-focused, automated data mapping tool that your privacy professionals can use without being reliant on external teams and processes.

If they don't want to wait on data science resources, of course, your privacy team could just open up a spreadsheet and get to mapping—but this approach is prohibitively tedious. By the time you finish mapping your data with a spreadsheet, it'll already be out of date anyhow!

Consider automated data mapping tools instead. These make it easy to find, record, and work with PI, data stores, and data flows across multiple systems.

## Need Help Establishing and Maintaining Your Data Map?

Osano Data Mapping is an automated data mapping solution that enables you to quickly gain insight and audibility and sets the stage for downstream compliance activities. Schedule a demo to find out how.

[Schedule a Demo](#)

**osano**



@osano



[linkedin.com/company/osano](https://www.linkedin.com/company/osano)



[http://facebook.com/osanoatx](https://www.facebook.com/osanoatx)



[osano.com](https://www.osano.com)

### About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 website to capture consent for more than 2.5 billion monthly visitors.