Shumaker

APRIL 2, 2026 | PUBLICATION

Data Inventories: A First Step for Practical Privacy Compliance

What data do you have?

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Brian C. Focht

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Where do you keep it?

You should repeat these two questions dozens, if not hundreds, of times while you're setting up your privacy compliance program.

A company cannot build an effective privacy compliance program without first understanding what personal data it collects, where that data resides, how it is used, with whom it is shared, and how long it is retained.

That is the role of a data inventory. While it may sound like a back-office exercise or a task left to entry-level workers, a data inventory is one of the most important operational tools in a privacy program. It gives a company the factual foundation it needs to comply with privacy laws and apply privacy controls in a meaningful way.

For organizations subject to U.S. privacy laws, the General Data Protection Regulation (GDPR), or both, maintaining a data inventory distinguishes a functional privacy program from one that exists only on paper. It supports legal compliance, improves governance, and aligns privacy notices, contracts, retention policies, and rights-response procedures with actual practices. It guides decision-making and supports informed compliance and risk management.

What a data inventory is

A data inventory is a well-organized record of the personal data a company collects and uses throughout its operations. It reflects the company's real-world practices, not just its written policies or assumptions. A data inventory should help answer key questions: what personal data is collected, where it comes from, why it is processed, where it is stored, who has access to it, with whom it is shared, and when it is deleted.

In practice, a data inventory acts as the core support for your privacy compliance efforts. A company cannot accurately describe its processing activities in a privacy notice, fully respond to a deletion request, judge whether its retention practices are reasonable, or evaluate vendor-related risks without a clear understanding of its own data flows and systems.

Why a data inventory matters

This one is pretty simple: a data inventory matters because privacy compliance depends on knowing your data.

Under EU privacy law, that principle is especially clear. The GDPR's accountability requirements, records of processing obligations, data minimization rules, storage limitation principle, and privacy by design expectations all assume that a company knows—and, more importantly, has documented—its relevant data processing activities.

Without that foundation, companies have a much more difficult time fulfilling their legal obligations.

Although less centralized and far from universal, the same is true under U.S. privacy laws. State privacy laws generally require businesses to disclose categories of personal information collected, the purposes for which it is used, the categories of third parties to whom it is disclosed, and the rights consumers may exercise regarding that data. Those obligations are hard to satisfy accurately without an accurate, up-to-date record of what data you actually have. A company that does not know where personal data is stored or how it moves through the organization is much more likely to issue incomplete notices, omit relevant information in responses to requests, or overlook risky data uses and disclosures.

A good data inventory also supports more than legal compliance. It helps reduce operational friction by giving different departments and divisions a common understanding of how personal data is handled. An accurate data inventory will also improve incident response, improve vendor diligence, and make it easier to identify unnecessary or outdated data collection practices.

Widely used privacy and governance frameworks, including the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), reflect the same basic idea: managing your privacy risks requires first understanding your data.

What a data inventory should contain

Too often, when I inquire about data inventories, I am directed to an asset management record that has been reused without any changes as a system inventory for privacy compliance.

"That's not a *data* inventory, though," you might say. "It's right there in the name! And an *inventory* of your *data!"* I agree. Yet, it's still something I often see, even from privacy consultants. It's not entirely useless, but it's not complete, and it's not going to do much for your company when it comes to privacy compliance.

While the level of detail will vary with the organization's size and complexity, several categories of information are commonly important.

1. Identify the Data

First, the inventory should identify the business process, function, application, or system involved. It should also specify the relevant categories of data subjects, such as customers, employees, applicants, website visitors, patients, or business contacts, as well as the types of personal data processed in connection with each activity.

If data collection includes sensitive data (under any applicable data privacy law), biometrics, or is used for automated decision making or to train or fine-tune artificial intelligence (AI), you will likely want to increase the detail of your inventory, the frequency with which it is updated, and the regularity with which it is

audited.

2. Method of Collection and Purpose of Processing

Second, the inventory should document where the data comes from and why it is processed. That usually includes the source of the data, the business purpose for collection or use, and any related legal or compliance justification. For companies operating in Europe or dealing with EU data, this may also include the lawful basis for processing. For U.S. compliance purposes, this information supports notice disclosures and internal governance of data use.

While not technically part of your data inventory, this is also an ideal place to address any necessary notices or consent issues related to your collection practices. Since you're taking an inventory of your data, include where you store your records of notice and consent for the data you collect.

3. Where it's Kept and Who Has Access

Third, the inventory should identify where the data is stored, which teams or roles have access to it, and which vendors, service providers, partners, affiliates, or other third parties receive it. This is an opportunity to ensure that your "least privilege" cybersecurity controls are properly configured and that your data classification guidelines are working effectively.

If data is transferred internationally, that should also be documented. Retention periods, deletion procedures, and relevant security or classification designations should also be included wherever possible.

Depending on the company's risk profile, it may also be useful to note whether the data is used for analytics, profiling, targeted advertising, automated decision-making, AI-related uses, or other activities that may create heightened legal or reputational risk.

How companies can do it right

Even a quick review of the previous section should make it painfully obvious that a data inventory is neither a one-time thing nor does it exist in isolation.

Legal and privacy teams may be responsible for structuring the exercise, but the substance of the inventory usually comes from the business, technical, and operational teams that work with data every day. That means the process should involve input from IT, information security, HR, procurement, marketing, product, operations, and relevant business owners. While it may also seem that the heavy lifting for this type of project will be performed by entry-level personnel, the real value of a proper data inventory lies in having everyone in the organization involved.

Additionally, a data inventory has a much smaller impact on an organization that lacks robust, integrated data management and security policies. Conducting a data inventory without, for example, connecting it to your data classification policy and document retention/destruction policy is a missed opportunity. The more comprehensive your policies are, the better they work together and the more value your organization will gain from these efforts.

For many companies, the best starting point is to identify the systems and processes that matter most. That often includes HR systems, customer relationship management (CRM) platforms, customer support tools, website technologies, marketing platforms, analytics tools, finance systems, and major vendors. From there, the company can document the categories of personal data involved, the purposes of processing, the data flows, and the retention and sharing practices associated with those systems.

It is also important to assign ownership. Each major system or business process should have a responsible owner who can confirm how data is used and help validate future changes. Without ownership, inventories tend to become stale quickly and inconsistently across business units, depending solely on the enthusiasm of those in charge.

The inventory should also be designed to be practical. It will never capture absolutely everything and will not be perfect on day one. Companies should not delay action because they cannot document every corner of the business at once. It is better to start with the highest-risk or most important systems and build a workable structure. From there, you expand and refine the inventory over time.

Common mistakes companies make

Check the box, move on to the next. One common mistake is treating the data inventory as a document created only to satisfy a legal requirement or complete a compliance checklist. When that happens, the inventory is often too abstract to be useful, too stale to be reliable after a short period, and almost never truly complete or accurate. A data inventory should be a working operational record, managed in tandem with your overall data management process, that helps inform real decisions, not just a static artifact prepared for a file.

Map the network, call it a day. Another frequent mistake, one that I mentioned earlier, is confusing a system inventory with a data inventory. A list of applications or assets may show what tools the company uses, but it does not necessarily explain what personal data is processed, why it is used, who receives it, or how long it is retained. Those privacy-specific details are what make the inventory valuable (and are the things you need to know when it comes to compliance).

Assume the lawyers and managers have all the answers. Companies also often make the mistake of limiting the exercise to legal or compliance personnel. That approach can overlook how data is actually handled in practice. In my experience, you can't always rely on marketing people to know what data the advertising team is collecting or using. Your process needs to include talking to the individuals who actually perform tasks like collecting data, obtaining consent, storing data, and transmitting data, along with everything else involved in the data lifecycle. Those who configure tools, onboard vendors, launch products, run marketing campaigns, manage personnel records, or oversee business operations often have information that never appears in contracts or policy documents.

Buying a new car instead of getting an oil change. Another problem is overengineering the initial effort. If the inventory process is too complicated, too time-consuming, or too disconnected from existing workflows, it becomes difficult to maintain. A more practical, phased approach is usually more sustainable.

Operating a business based on one unchanging dataset. Finally, many companies fail to establish a process to keep inventory current. That is a serious weakness because business practices, tools, and data uses change constantly. An outdated inventory may create false confidence while leaving important gaps unaddressed.

How to keep a data inventory current

A data inventory is only useful if it remains current enough to reflect the company's actual practices. That means it needs to be created with change in mind, both in how the data will be kept up to date and in how the inventory itself can respond to changes in the business or industry. Updates should be triggered by events such as onboarding a new vendor, launching a new product or feature, adopting a new marketing tool, changing an HR process, expanding analytics practices, or modifying retention rules.

Periodic reviews are also important. Regular check-ins with system owners, annual privacy assessments, procurement reviews, and coordination with IT and security can all help confirm whether processing activities have changed. Incorporate data inventory updates into vendor review, change management, or internal audit processes so that the inventory evolves alongside the business.

Most importantly, make sure that the people responsible for keeping the inventory up to date do so regularly and consistently across business units. A data inventory can quickly become unreliable if half the organization updates regularly, while the other half updates only at irregular intervals, if at all.

The goal is to treat the data inventory as a living compliance and governance tool rather than something that is completed once and then forgotten.

Conclusion

A data inventory is one of the most important foundations of an effective privacy program. It helps a company understand what personal data it processes, how that data moves through the organization, and what obligations attach to it. That understanding is essential for both U.S. and EU privacy compliance and is consistent with widely recognized privacy and governance standards, including NIST and ISO.

Without a reliable data inventory, your privacy notices may be incomplete, your data subject access responses may miss responsive data, your retention practices may be inconsistent, and your vendor oversight may lack critical details. By contrast, a well-built and well-maintained data inventory gives companies the visibility they need to turn privacy compliance into something operational, practical, and defensible.

So, what data do you have? And where do you keep it?

Please contact Brian Focht or another member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line if you have any questions.

Shumaker