Access

Whitepaper

# Data Privacy for the Information Professional

Data privacy is no longer a niche concern delegated to legal teams and IT departments. It's a core responsibility and an organizational mindset. Whether you're tasked with managing records, overseeing compliance, or advising business units, privacy considerations are now a constant thread throughout every part of the organization.

This shift demands more than updated policies or annual audits. It calls for a strategic, organizational-wide approach that embeds privacy into the entire information lifecycle. That includes traditional information governance (IG) tasks like managing retention schedules, but increasingly extends to setting limits on data use, obtaining consent, and justifying why personal data is collected in the first place.

The challenge is heightened by the fragmented and fast-evolving landscape of U.S. privacy law. While California's CCPA and CPRA receive much attention, many states have enacted or are pursuing their own laws. And each state or law has its own unique definitions, rights, and compliance obligations. Unlike Europe's GDPR, there is no single U.S. standard. This creates a moving target that can't be addressed with static checklists or a "set it and forget it" approach.

Instead, privacy must become a guiding principle that informs decision-making across departments. When treated this way, privacy evolves beyond just a legal requirement into a sustainable, long-term practice that builds trust and resilience.

This whitepaper outlines how to make that shift. In the following pages, you'll learn the principles of Privacy by Design, how to build a flexible and strategic privacy framework, and the records retention considerations that follow suit. After reading, you'll see a clear path for your organization to transition from reactive solutions to a proactive, privacy-first culture.

# Privacy by Design

"Privacy by Design" is more than just a best practice. It's a mindset and operational framework that embeds privacy principles into the core of business processes, systems, and technologies from the outset.

At its core, Privacy by Design asserts that privacy values—along with legal requirements, ethical standards, and data control mechanisms—must be integrated at the earliest stages of product or process development. Whether you're designing a new system, onboarding a vendor, or updating a data collection workflow, privacy must be foundational, not supplemental.

**Operationalizing privacy requires close collaboration between Records, IT, Legal, Compliance, HR, and even Marketing. Each department collects and handles personal data differently, so successful privacy frameworks depend on shared ownership and aligned governance.**

You can start collaborating with these teams by organizing a cross-functional working group or privacy task force. Invite key stakeholders from each department to align on data handling practices, surface potential risks, and agree on shared responsibilities. Regular meetings and open documentation can help build a consistent, organizational-wide understanding of privacy expectations. This strategy also ensures that policies aren't developed in a vacuum.

## The Seven Principles of Privacy by Design

Before your organization can operationalize privacy, you must first understand its underlying principles—the "why" behind the "what." This means shifting from reactive compliance to proactive governance. Whether you're managing structured records or sprawling unstructured data, the foundation of every privacy program rests on a few universal concepts. These core principles cut across jurisdictional lines, from the broad mandates of the GDPR to the evolving patchwork of U.S. state laws, and offers a lens through which to evaluate your organization's data practices.

**Privacy by Design has seven core foundational principles that drive its outcomes:**

1. **Proactive, not reactive; preventive, not remedial**
   Build controls to prevent privacy issues before they arise.
2. **Privacy embedded into design**
   Make privacy a default feature of the system or process rather than an afterthought.
3. **Privacy as the default setting**
   Collect only what is necessary; users shouldn't have to opt out to protect their data.
4. **End-to-end security – full lifecycle protection**
   Safeguard personal data from the point of collection to secure destruction.
5. **Full functionality – positive-sum, not zero-sum**
   Design systems that meet both privacy and business goals without tradeoffs.
6. **Visibility and transparency – keep it open**
   Be clear and open about data practices internally and externally.
7. **Respect for user privacy – keep it user-centric**
   Empower individuals with control and understanding of their data.

These principles are high-level, but they provide the philosophical foundation for how systems and processes should be built to respect privacy rights and comply with applicable laws.

**Personally identifiable information, or PII, is any data that can be used to identify a specific person.**

Examples: full name, Social Security number, driver's license number, bank account number, passport number, phone number, mailing or e-mail address, IP address, date or place of birth, race, and gender.

## Translating Principles into Practice

The challenge lies in operationalizing these principles within your organization's unique regulatory and business context. That means:

- Analyzing the principles in the context of your operations, industry, and jurisdictions.
- Interpreting their application across technology systems, data flows, and business functions.
- Ensuring alignment with records retention schedules, policies, and procedures.

Successfully implementing Privacy by Design requires an ongoing process and technology design mandate. It necessitates alignment across various business units and leadership to ensure that your systems don't just claim to protect privacy—they actually do.

## Privacy Best Practices

Now that you understand the principles at a high level, let's get a bit more specific on how you can apply them. By implementing the following best practices, you can build systems that protect individuals, minimize risk, and align privacy with organizational strategy.

- **If it can be traced to someone, it's considered personal information.** Some privacy laws provide detailed lists of what counts as personal data; others, such as the CCPA and GDPR, have broader and more general definitions. Therefore, never assume that data capable of identifying someone isn't classified as personal information.
- **Less is more, and regarding privacy, less is better.** If you don't need a piece of personal information, don't collect it. If you did need it and it's no longer necessary, get rid of it. This notion of data minimization, or keeping the least personal information in your possession, is a core principle of all privacy laws. Establishing and enforcing a records retention schedule ensures you dispose of unnecessary or outdated information to minimize risk and meet compliance guidelines.
- **When in doubt, disclose and ask for clarity.** You don't always need to disclose why you're collecting personal information, and you don't always need permission. However, if permission is required and you don't obtain it, you could make a costly mistake. It never hurts to ask for confirmation.
- **If they don't need to see it, they shouldn't.** Privacy laws ensure that sensitive information is safeguarded, including how data is stored, protected, and shared. To protect individuals' privacy and rights, clear guidelines should be established for how data can be accessed and by whom.
- **Don't overlook third-party data processors.** Your organization is accountable for how vendors collect, use, and retain personal data on your behalf. Review contracts for privacy clauses, ensure vendors have robust security policies and processes, and check in with them regularly.

Implementing these data privacy best practices can seem overwhelming, but a good place to start is by reviewing your organization's existing processes and evaluating how they prioritize privacy. From there, identify gaps or weaknesses and prioritize those areas to ensure compliance and meet privacy standards.

## The Compliance Paradox

Privacy laws say: "*Keep as little personal data as possible, for as short a time as possible.*"

But those same laws require proof that you followed the rules, which means creating and storing new records that may also contain personal data.

**That's the paradox.**

You disclose how data will be used. You get consent. But to demonstrate compliance, you need evidence: time-stamped opt-ins, copies of disclosure language, and audit trails. All of which must be stored and managed, oftentimes longer than the data they relate to.

Here's an example: A healthcare clinic launches a patient intake portal where individuals can fill out digital forms before their visit. To meet HIPAA requirements, the clinic must inform patients how their information will be used and get their consent. But to prove compliance later, they must retain data showing when the patient submitted the form, what language was shown, and which boxes were checked. That proof, which may contain PII, becomes its own record and is subject to retention and security rules.

The result? Even when you're trying to reduce what you store, compliance forces you to create new data. Multiply that by thousands of interactions and manual tracking becomes impossible.

# The Impact of Privacy Laws on Records Retention

The expansion of privacy laws across the globe has made maintaining or updating a retention schedule more complex than ever.

Privacy laws demand that businesses take a more sophisticated and defensible approach to records retention. The potential for discovery requests, legal action, investigations, and audits means that organizations must be prepared to justify their retention decisions at any time. Having a defensible retention schedule that can be referenced in case a record was (or wasn't) destroyed is a necessity.

Another key aspect to consider is the underlying premise of many privacy laws. The concept that individuals own their personal data and, as such, have the legal right to control how it is collected, used, and retained. This shift in philosophy requires organizations to continually update their retention policies to ensure compliance.

A crucial part of this process is the assignment of appropriate privacy classifications to records. To stay in compliance, record owners must be proactive in reviewing and updating classifications during annual reviews or whenever new data types emerge. This ensures that records are aligned with current privacy laws and helps mitigate the risks associated with outdated or improperly classified data.

## Establishing a "Reasonable" Retention Period

**The question always comes up:**

*How long should we keep personal data?*

**The answer is:**

*A reasonable period. But what exactly does that mean?*

A "reasonable" retention period is dictated by legal standards, industry best practices, and the needs of the business.

In general, data should only be kept as long as necessary for the original purpose it was collected for. If there is no clear legal requirement to retain it for longer, or if the data is no longer needed for business purposes, it should be securely disposed of.

However, there may be valid scenarios where retaining data beyond the legal requirement is in the organization's best interest. For example, extended retention might support audits, long-term analysis, or internal operational needs. In these cases, the decision to keep data longer must be intentional and fully documented.

Retention becomes even more complex for organizations operating across multiple states or countries, where privacy and data protection laws may conflict. For instance, one jurisdiction may require data to be retained for five years, while another may mandate its deletion after just one. In these cases, it's often most effective to maintain a centralized global retention schedule that reflects a common baseline, while clearly documenting exceptions where shorter or stricter requirements apply.

**A Tip from the Access Information Governance Team:**

Balancing privacy regulations with records management processes is an ongoing and often time-consuming project. Additionally, there's a lot of variation across individual state legislations that require someone who's highly specialized in that field to recognize how those privacy regulations apply to your business operations. Information professionals should work with their privacy, compliance, or legal departments when making changes in retention schedules, as necessary.

Rather than creating separate schedules for each region, a unified schedule with jurisdiction-specific carveouts strikes a balance between manageability and compliance.

Any deviation from standard retention periods—whether due to business needs or jurisdictional differences—should be supported by thorough documentation. This includes:

- A clearly defined justification
- Legal review and approval, if applicable
- Documentation of the decision and scope
- Updates to the retention schedule or policy

This documentation ensures that retention decisions remain defensible during audits, investigations, or litigation, and it helps demonstrate consistency and intent; the two critical components of a mature privacy and governance program.

Failure to document these choices can expose the organization to unnecessary risk. Holding onto personal data without a valid, well-recorded justification may lead to non-compliance with privacy laws or complicate your legal defense in the event of discovery.

**In short, "keep it longer" should never be a casual decision. When retention periods vary by region, document the "why," define the "how," and revisit the "when" as laws and operational needs continue to evolve.**

## Conclusion: Privacy is a Practice, Not a Project

As privacy regulations continue to evolve, so too must the way organizations manage information. Compliance can no longer be reactive or siloed. It requires an intentional, strategic effort that spans policies, technologies, and people.

For information professionals, this means stepping into a leadership role: designing sustainable retention frameworks, translating legal expectations into operational practices, and championing privacy as a core business value.

The path forward isn't always simple—but it is clear: Treat privacy as a continuous practice. Lead with transparency. And document everything.

With the right frameworks and mindset, your organization can not only stay compliant but build lasting trust and resilience in the face of constant change.

If your team needs guidance navigating today's privacy landscape, especially as it relates to records retention and policy development, the experts at Access can help.

**Learn more about our Information Governance Policy Services or contact us today to start building a program that aligns privacy compliance with long-term business goals.**

Access

### About Access

Access is the largest privately held records and information management services provider worldwide, with operations across the United States, Canada, Central and South America. Access provides transformative services, expertise, and technologies to make organizations more efficient and more compliant. Access helps companies manage and activate their critical business information through offsite storage and information governance services, scanning and digital transformation solutions, document management software, and secure destruction services. Access has been named twelve times to the Inc. 5000, the ranking of fastest-growing private companies in the U.S.