WHITE PAPER

Developing a Data Retention Policy to Meet Privacy Data Minimization Requirements

Abstract

Organizations need to meet both privacy data minimization rules as well as legal and regulatory recordkeeping requirements. As opposed to creating a separate data retention policy and record retention schedule, it is better to create a single data retention policy containing all requirements. This unified approach is more compliant and drives more consistent execution.

contoural

Developing a Data Retention Policy to Meet Privacy Data Minimization Requirements

New and existing privacy regulations require that personal information be retained only as long as necessary for legitimate business need. To comply, organizations are developing data retention and disposition policies. While this might at first appear to be a straightforward endeavor, organizations are learning that determining what to keep—and for how long, and what can and should be deleted—involves much more than privacy.

To avoid conflicts and comply with non-privacy regulatory requirements, retention and disposition decisions must take into account records retention requirements and the business need. Finally, it is not enough to simply have a data retention policy; the policy must be executed with care and diligence.

Privacy Requirements Drive Data Minimization

Nearly all organizations create and retain personal information about individuals. New and emerging privacy regulations restrict the retention of this personal information to "no longer than necessary" for a legitimate business need. Additionally, under most privacy compliance regimes, individuals have the right to request that their information be deleted or erased.

Despite having been active for several years, many of these data retention and disposition regulations have not been meaningfully enforced. This is quickly changing. In Europe, companies are facing fines for over-retention of personal information. Many companies are getting ready for California's enforcement as its privacy rules come into effect, and Illinois is stepping up its enforcement of retention of biometric data. Furthermore, the U.S. Federal Trade Commission has long encouraged or required, through both recommendations and enforcement activity, a data minimization focus for organizations.

Figure 1. Regulators have seemed slow to enforce personal information requirements, but now many are stepping up enforcement.

When these laws first came out, many companies took a "wait and see" approach. That is quickly coming to an end. Enforcement of data minimization principles is driving new looks at existing processes. Organizations can appropriately manage the personal information lifecycle using the same tools as other information. What personal information to save, and for how long, should be addressed through the organization's existing data retention policies, both to demonstrate good faith efforts to comply with rules and to provide guidance to IT and other groups on what they can save.

At the outset, creating a data retention and deletion policy seems like a straightforward task. However, it often gets bogged down through endless inputs from multiple stakeholders and lack of consensus. The root cause of getting stuck is that many data retention policies focus too narrowly on personal information disposition requirements that are not in sync with records retention compliance or business needs. Sometimes, organizations effectively punt on the issue by creating vague, watered-down, or ill-defined policies or retention rules. This provides little guidance to employees regarding what to save and not save.

Records retention laws and regulations often require companies to retain records for a certain number of years. These requirements may override consumer deletion requests even if the record in question contains personal information.

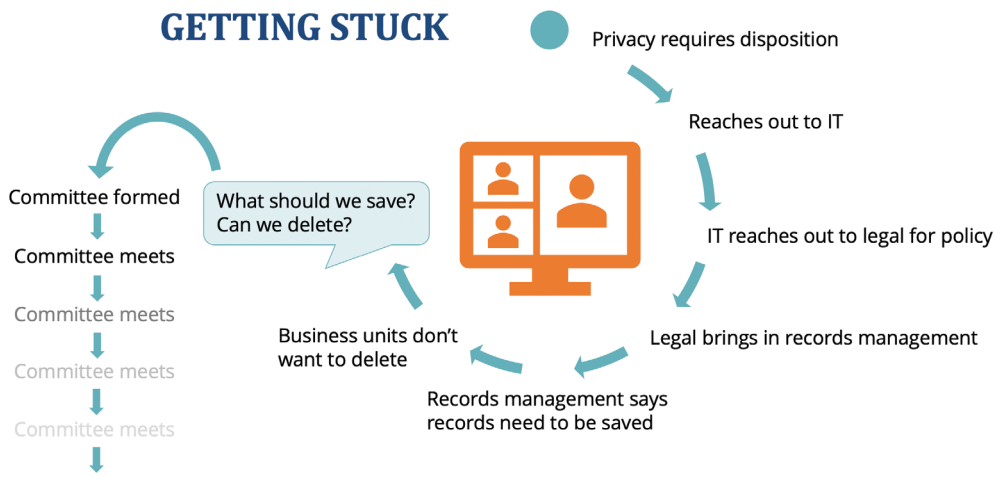

Figure 2. It is common for data retention policy creation to stall out. The root cause of this getting stuck is most often focusing narrowly on privacy requirements and not incorporating other compliance or business drivers.

There can also be a tendency among privacy, legal, or compliance teams to "go it alone" and create a retention policy with little outside input or collaboration, then hand it off to IT or business units to execute. Such a policy is unlikely to be followed, and the gap between what the policy says and its actual execution creates more risk than not having a retention policy at all.

Data Retention Policy vs. Records Retention Schedule Requirements

At its core, a policy is simply a statement of what the organization does. As such, most organizations' records retention schedules already contain data retention policies. Policies (high-level statements) and schedules (detailed requirements) may be driven by different compliance targets, but both fundamentally seek to define what information should be saved for how long.

Records retention laws and regulations often require companies to retain records for a certain number of years. These requirements may override consumer deletion requests even if the record in question contains personal information. For example, a customer

of a financial services company may request that their personal information be deleted after closing their account, but most states' recordkeeping rules require that this account information be retained for at least seven years.

Take, for example, California's record retention requirements for retaining employee records (Figure 3, below) compared with California's CPRA requirement for retaining personal information for no longer than is reasonably necessary (Figure 4). How should an organization handle this conflict?

CITATION	RECORDS TO BE KEPT	RETENTION/ LIMITATION PERIOD	COMPANY RETENTION
Cal. Gov't Code § 12946	Any and all applications, personnel, membership, or employment referral records and files; personnel files of applicants or terminated employees.	4 years after the records/ files are initially created/ received, or 4 years after the date the employment action was taken.	End of employment + 6 years

Figure 3. An example of California's requirement for saving employment records.

CITATION	RECORDS TO BE KEPT	RETENTION/ LIMITATION PERIOD	COMPANY RETENTION
Cal. Bus. and Comm. Code § 1798.100	Personal information, sensitive personal information.	No longer than is reasonably necessary for [the] disclosed purpose.	?

Figure 4. California's CPRA requirements for retaining personal information, including employment records, for no longer than is reasonably necessary seem to conflict with other California law.

In many cases, the company's business need for information is longer than the legally-mandated retention period—that is, the business utility of the information lasts longer than the legal utility. Because of such conflicts, the work to create a data retention and deletion policy often gets stuck. While these examples are based on California law, most privacy laws have similar requirements, resulting in potential conflicts with record retention requirements.

Since conflicts between the two can create non-compliance, data retention and disposition policies and strategies need to be synchronized with records retention requirements. The easiest and smartest approach is to incorporate both into a single policy. Both sets of requirements aim to detail what information needs to be saved for how long; putting them in a single document makes it easier.

Finally, the end result should not focus exclusively on legal and regulatory requirements. Rather, these policies also need to address business need and value. Good data retention policies do not only serve as legal statements but also seek to achieve a reasonable consensus with business units and other stakeholders regarding what information needs to be maintained to run the business and what can and should be deleted (and when). Any deletion exercise depends on this agreement. Failure to build consensus at the beginning forces companies to revisit these questions every time they try to delete information.

What's In a Name?

Some companies call it a data retention policy; others call it a records retention schedule. What the document is called is of less concern; what matters is that data retention policies are records-enabled, and records retention schedules are privacy-enabled.

Creating a Personal Information Retention Justification Process

Most privacy laws require a business justification for retaining personal information. Unfortunately, there is no "bright line" rule or existing case law clearly indicating what constitutes a legitimate business need.

Organizations should develop a process for determining and documenting business need. For non- prescriptive rules such as business justification, following a documented, good-faith process demonstrates compliance and provides defensibility.

CODE	CATEGORY	DESCRIPTION	EXAMPLES	RETENTION	PERSONAL INFORMATION	RETENTION JUSTIFICATION
CRP1000	Business Organization	Formal corporate and board of director documentation of the company, as well as records related to shareholder activity and stock ownership in the company.	Includes Articles of Incorporation, Amendments, Bylaws, Corporate Charter, Corporate Meeting Minute Books and Resolutions, Board Meeting Minutes and Materials, Board Committee Meeting Minutes and Materials, Board Docket, Board of Director Conflict of Interest Records, Annual Re-ports, Stock Transfer Records, Shareholder Records, Shareholder Meetings, Shareholder Proxies, Shareholder Dividends	Permanent	Conflict of Interest Forms (contains Board Member and employee names, and may contain names of other relatives as part of the disclosure) Shareholder Records (contains individual shareholders and shares held) Corporate Minutes (may contain personnel names and other employment information) Corporate Resolutions (may contain personnel names)	Laws in Q state, where we are headquartered, require that we keep formal corporate information permanently. Laws in X and Y countries, where we have substantial operations, require that we keep formal corporate information permanently. As a corporation, having a historical record of all decisions made by the Board of Directors is important to our ongoing business.

Figure 5. A sample privacy-enabled records retention schedule that includes business justification for retention of personal information.

Attributes of a Privacy-Enabled Records Retention Schedule

A privacy-enabled records retention schedule (or data retention policy) should capture both records retention requirements and data minimization justifications in a single policy. Many organizations are updating their retention policies to address a larger set of requirements.

To build a good data retention policy/records retention schedule, follow these best practices:

Include an Inventory of All Information Types

Identify all of the types of information across the organization. This inventory should span all media types including structured data in database systems, unstructured file content, semi-structured emails, social media, and others as well as paper documents.

Apply Legal and Regulatory Retention Requirements

From the larger inventory, based on the nature of the content and independent of media type, determine the legal and regulatory requirements. These can include national, state/provincial, local, and industry-specific regulations. For organizations that operate across multiple countries, these requirements must be identified for each country. In general, create global retention categories where possible and define local exceptions as necessary. Consider explicitly calling out non-records.

Determine Business Value

Companies can and should define retention based on business value. In other words, a company can declare something a record because it has business value even if there is no underlying regulatory requirement. Business value can include intellectual property, trade secrets, and operational needs.

Developing compliant, balanced approaches through modern, easier-to-execute polices may take more effort at the beginning, but well-crafted policies ultimately make execution easier, reduce downstream conflicts, and lower disposition resistance.

Address Personal Information

Identify which records and non-records contain personal information and which privacy requirements may apply.

Include Disposition Requirements

If regulations with maximum retention periods exist (e.g., "Destroy after 2 Years"), include these disposition requirements in your retention decision.

Identify Legitimate Business Need

For retention of personal information, include a description of the legitimate business need for the retention as stated.

Consider the Need for Legal Holds

Companies facing or anticipating litigation or regulatory investigations have a duty to preserve that information. This duty to preserve usurps all records expiration or privacy disposition. Policies should acknowledge this responsibility.

Obtain Consensus with the Business

Continue to socialize the policy, business value, and retention requirements with business units and other key stakeholders, seeking to achieve reasonable retention periods.

Conclusion

Privacy data minimization requirements create an additional complication on top of existing and often challenging records retention requirements. Avoid the temptation to create separate policies or go it alone. Engage other stakeholders as well as business units. Keep these policies up to date.

Developing compliant, balanced approaches through modern, easier-to-execute polices may take more effort at the beginning, but well-crafted policies ultimately make execution easier, reduce downstream conflicts, and lower disposition resistance from business units and employees. It is worth the effort to do it right.

Additional Materials Available

Find additional content and in-depth information at www.contoural.com or email us at info@contoural.com.

About Contoural

Contoural is the largest independent provider of information governance, privacy, and AI governance strategic consulting services, including records and information management, governance policies, litigation readiness and control of sensitive information. The company does not sell any products or take referral fees, store any documents, or provide any "reactive" eDiscovery services. Serving as a trusted advisor to more than 30% of the Fortune 500, non-profits, and public sector organizations, Contoural offers a range of record management and information governance services, including:

- Records Retention Schedule/Data Retention Policy Development
- Global Records Citations Research
- Business Justification Process
- Assessment and Roadmap
- Personal Information Inventory
- Privacy Risk-Driven Policies and Notices
- Privacy-Enabled Incident Response
- Data Placement Strategy and Rollout for Unstructured Files and Semi-Structured Email Data
- Structured Data Retention and Remediation Strategy
- Employee Behavior Change Management and Training
- Fractional Privacy Manager
- AI Governance

contoural

READY. COMPLIANT. IN CONTROL.

335 Main Street, Suite B, Los Altos, CA 94022

650.390.0800 | info@contoural.com | www.contoural.com