WHITE PAPER

Creating a Data Retention Policy to Meet Privacy Requirements

contoural

READY. COMPLIANT. IN CONTROL.

Creating a Data Retention Policy to Meet Privacy 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. However, in what at first appears 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. Records retention requirements and the business need also must be factored into retention and disposition decisions, to avoid conflicts as well as comply with non-privacy regulatory requirements. Finally, more important than simply having a data retention policy, care and diligence need to be put into actually executing these policies.

A. Privacy Requirements Drive Data Minimization

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

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.

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

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 use existing processes to 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 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.

B. Data Retention Policy Creation Often Gets Stuck

1. Privacy requires disposition
2. Reaches out to IT
2. IT reaches out to legal for policy
3. Legal brings in records management
4. Records management says records need to be saved
5. Business units don't want to delete
6. What should we save? Can we delete?
7. Committee formed
8. Committee meets
9. Committee meets
10. Committee meets…
11. Committee meets…

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.

Creating a data retention and deletion policy at the outset appears to be a straightforward task. However, the effort often gets bogged down through endless inputs from and lack of consensus with multiple stakeholders. 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. Sometime organizations effectively "punt" on the issue by creating vague, non-prescriptive, watered-down, or ill-defined policies that may simply list hazy, non-prescriptive retention rules. Avoid this, as it will do little provide guidance to employees regarding what to save and not save.

Furthermore, there is sometimes a tendency by privacy, legal, or compliance teams to "go it alone" and create a retention policy by themselves with little input or collaboration, and then hand it off to IT or business units to execute. There may be a policy, but it is unlikely it will be or can be followed, and the gap between what the organization says it will do in its policy and its lack of execution creates more risk than not having a retention policy at all.

C. Data Retention Policy vs. Records Retention Schedule Requirements

A policy is, at its core, simply a statement of what the organization does. Therefore, most organizations already have data retention policies in their records retention schedules. 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 may require companies to retain records for a certain number of years, driven by literally thousands of record retention regulations. 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 to delete their personal information after they close their account, but recordkeeping rules require

that this account information be retained at least seven years in most states. Figure 3 details, for example, California's record retention requirements around employment information.

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.

Figure 3 above lists California's record retention requirements for retaining employee records. Figure 4 lists California's CPRA requirement for retaining personal information for no longer than is reasonably necessary. How to handle the conflict? In many cases, the company's business need for information is longer than the legally-mandated retention period – that is, the business utility of that information lasts longer than the legal utility. Because of such conflicts, the work to create a data retention and deletion policy often gets stuck. These examples are based on California law, but most privacy laws have similar requirements, resulting in similar potential conflicts with record retention requirements.

Data retention and disposition policies and strategies need to be synchronized with records retention requirements. Conflicts between the two can create non-compliance. As such, the most compliant, 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.

Of less concern is what the document is called. Some companies call it a data retention policy; others call it a records retention schedule. It is not important. What matters is that data retention policies are records-enabled, and records retention schedules are privacy-enabled.

Finally, as is best practice, the end result should not focus exclusively on legal and regulatory requirements. Rather, these policies also need to address business need and value. Good retention policies serve not only 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 having this agreement. Failing to build this consensus at the beginning will force companies to revisit it every time they try and delete information.

D. Creating a Personal Information Retention Justification Process

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 Dockets, Board of Director Conflict of Interest Records, Annual Reports, 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 relations as part of the disclosure) • Shareholder Records (contains names of 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.

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.

E. Attributes of a Privacy-enabled Records Retention Schedule (or Records-enabled Data Retention Policy)

Many organizations are updating their retention policies to address a larger set of requirements. To build a good retention policy and schedule:

Include an Inventory of All Information Types – A first step is identifying all 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, etc. as well as paper documents.

Apply Legal and Regulatory Retention Requirements – From the larger inventory, based on the content and independent of media – determine the legal and regulatory requirements. This can include national, state/provincial, local, as well as industry-specific regulations. For organizations that operate across multiple countries these requirements must be identified for each country. In general, where possible create global retention categories and define local exceptions where necessary. Also 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.

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. Polices should acknowledge this responsibility.

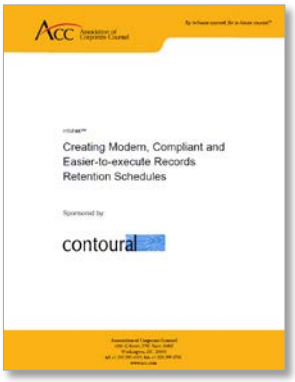
Obtain Consensus with the Business – Finally, continue to socialize the policy, business value and retention requirements with business units and other key stakeholders, seeking to achieve reasonable retention periods.

F. Conclusion

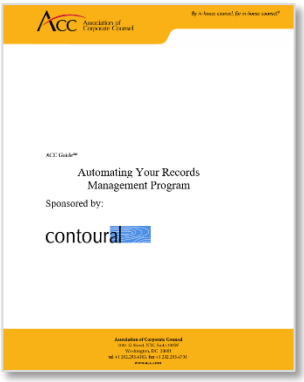
Meeting privacy data minimization requirements creates an additional complication on top of existing and often challenging records retention requirements. Avoid the temptation to create separate policies and go it alone. Engage other stakeholders as well as business units. Keep these policies up to date. Developing compliant, balanced approaches in modern, easier-to-execute polices may take a little more effort at the beginning, but well-crafted policies make execution much easier, reduce downstream conflicts, and reduce or avoid disposition resistance from business units and employees. It is worth the effort to do it right.

Additional Materials Available

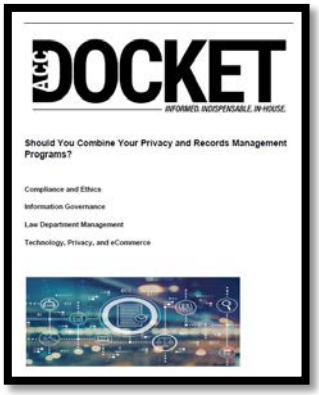
More in-depth information on this topic is available. Additional content is available at www.contoural.com or email us at info@contoural.com



Guide: *Creating Modern, Compliant and Easier-to-Execute Records Retention Schedules*



Guide: *Automating Your Records Management Program*



Article: *Should You Combine Your Privacy and Records Management Program*

Guide: *Deleting Emails and Files Quickly and Defensibly*

About Contoural

Contoural is the largest independent provider of strategic privacy and Information Governance consulting services. Serving more than 30% of the Fortune 500, many small and mid-sized companies, public sector organizations, and non-profits, we reduce risk, ensure compliance, lower costs, and drive employee productivity. As an independent provider we sell no products, provide no “reactive” eDiscovery services, store no documents, nor receive referral fees. Contoural is recognized as the market leader in strategic privacy and Information Governance consulting services.

Our Strategic Consulting Services

Data Retention/Records Retention Schedule Development

Assessment and Roadmap

Personal Information Inventory

Risk Tolerance Review and Targeted Program Maturity

Risk-driven Policies and Notices

Privacy-enabled Incident Response

Privacy Subject Access and Deletion Request Process

Privacy Training and Awareness

Data Placement Strategy and Rollout for Unstructured Files and Semi-structured Email Data

Structured Data Retention and Remediation Strategy

Organizational, Disposition and Monitoring Services

Organizational Privacy Roles and Responsibilities

Employee Behavior Change Management and Training

Fractional Privacy and Records Manager

contoural

READY. COMPLIANT. IN CONTROL.

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