COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2023

Mark Diamond (markdiamond@contoural.com) is President & CEO of Contoural in Los Altos, California, USA.

Creating a data-retention policy for privacy requirements

By Mark Diamond

Nearly all organizations create and retain personal information about individuals. Privacy rules limit how long this information can be retained. In most cases, they stipulate that personal information can be retained "no longer than necessary" for a legitimate business need. Additionally, under most privacy compliance regimes, individuals have the right to request their information be deleted or erased. These new requirements are driving organizations to examine what personal information they store, where they store it, and to impose rules limiting how long they keep it.

Personal information disposition, however, cannot operate in a silo, as other compliance requirements rules come into play. Records-retention legal and regulatory requirements mandate that records be retained for minimum periods, even if these records contain personal information. Relevant information under legal hold must be retained. Furthermore, businesses have a legitimate need to save both personal and other types of information.

These requirements and needs should be synchronized and codified in a data-retention policy. For most organizations, the data-retention policy should enhance their records-retention schedule. A well-crafted policy not only drives compliance but also makes policy execution much easier.

Privacy requirements drive data minimization

While many privacy 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 (see Figure 1). Additionally, many companies are getting ready for California's enforcement as its privacy rules are enacted. Other states have or are expected to adopt similar rules. Furthermore, the U.S. Federal Trade Commission has long encouraged/required a data-minimization focus for organizations through both its recommendations and enforcement activity.

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


European Data Protection Board

edpb

European Data Protection Board

The French SA fines the economic interest group INFOGREFFE EUR 250000

16 September 2022 France

Key Findings

- Failure to comply with the obligation to keep data for a period of time proportionate to the purpose of the processing (Article 5.1.e of the GDPR)

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 life cycle 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 provide guidance to IT and other groups on what they can save.

Companies need to create data-retention policies to comply with these rules. A policy is, at its core, simply a statement of what the organization does. As discussed below, these policies need to be integrated with records retention and other compliance requirements. Different compliance targets may be driven by policies (high-level statements) and schedules (detailed requirements), but both fundamentally seek to define what information should be saved for how long. Effective and compliant data-retention policies should address all information across an enterprise in all formats.

Creating a data-retention policy

A data-retention policy consists of two components: a shorter, overarching policy and a detailed schedule. The policy has three primary purposes: (1) it defines records and nonrecords covered by the data-retention policy, including short-term working documents, and states that records must be kept for the duration of the retention period listed in the records-retention schedule; (2) it states that once a record's and working document's retention period has expired, they must be destroyed; and (3) in the event of a legal hold, the policy and retention schedules are suspended for the records under the hold. Note that we are using the term "record" to describe specific content that may have either minimum or maximum retention requirements.

The retention schedule is a listing of records created and maintained by the organization. A schedule lists the records that must be kept for legal, regulatory, or business purposes; details which documents and data contain personal information; and provides a retention period specifying how long that record must be retained. The schedule may or may not contain citations detailing the specific legal or regulatory requirements for retaining any given record.

Privacy and record retention rules often conflict. Figure 2 details, for example, California's record-retention requirements around employment information. Figure 3 lists the California Consumer Privacy Act requirement

for retaining personal information for no longer than is reasonably necessary. These examples are based on California law, but most privacy laws have similar requirements, resulting in similar potential conflicts with record-retention requirements.

Figure 2: An example of California's requirement for saving employment records.

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: The California Consumer Privacy Act requirements for retaining personal information seem to con with other California laws.

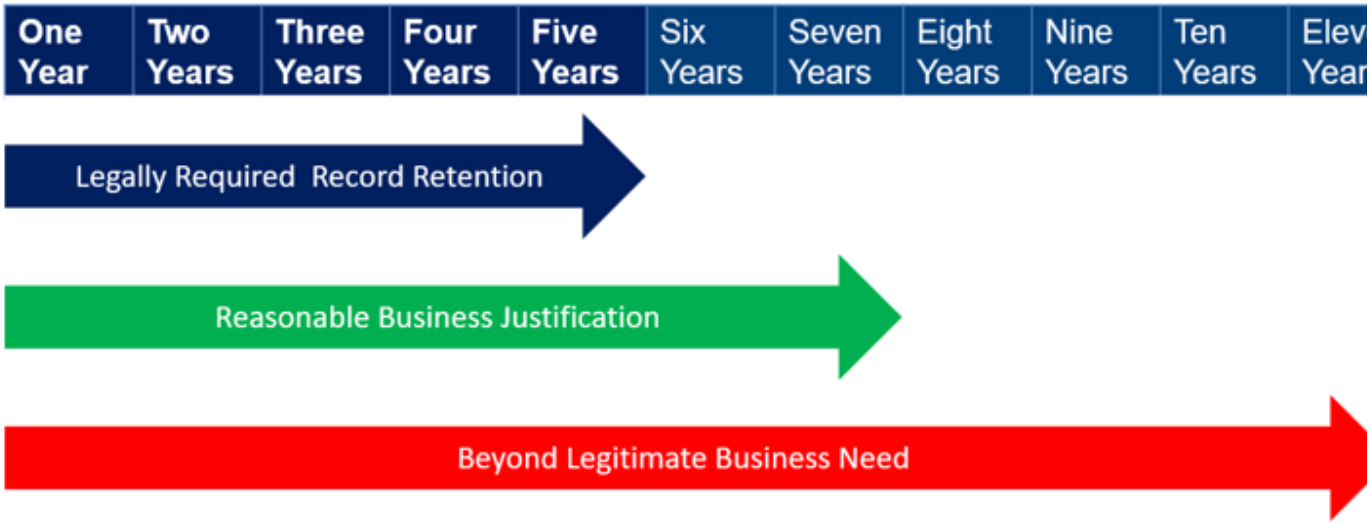
Citation	Records to be Kept	Retention/Limitation Period	Company Retention
Cal. Bus. and Comm. Code § 1798.100	Personal information, sensitive personal information	No longer than is reasonably necessary for [the] disclosed purpose	?????

Figure 4: Synchronization of data-retention and record-retention policies.

Data-retention and disposition policies and strategies must be synchronized with records-retention requirements (see Figure 4). How do organizations handle conflict? In general, legal and regulatory-based record-retention requirements trump personal information disposition requirements. These conflicts need to be identified. Conflicts existing in a separate data-retention policy and records-retention schedule can create noncompliance. 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 and 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. The name is not important. What matters is that data-retention policies are records-enabled, and records-retention schedules are privacy-enabled.

Retention justification process

Figure 5: Sample of applying business justification to determine personal information retention.



Can personal information be retained only as long as required by recordkeeping requirements? The European Union's General Data Protection Regulation and other privacy rules recognize that, in some cases, businesses have a legitimate business need to retain personal information (Figure 5). For example, auto manufacturers may need to retain personal information about their customers if they need to contact them for a recall. As recalls can occur literally decades after the initial purchase, in this case it is reasonable to argue that this personal information needs to be retained that long too.

Three factors that drive the retention of personal information:

Personal information must be retained at a minimum for legal and regulatory-driven record-retention periods. Legal and regulatory recordkeeping requirements override privacy deletion rules. In the example from the previous section, California requires that "any and all applications, personnel, membership, or employment referral records and files; personnel files of applicants or terminated employees" be retained for four years. All such records have a minimum four-year retention after the records/files are initially created/received or four years after the date the employment action was taken. Records-retention requirements serve as a "low water mark" retention period.

Companies may retain personal information for a longer period through business justification. There are many instances in which companies have a legitimate business need to retain personal information longer than legal and regulatory requirements. Personal information may be retained for these longer periods so long as there is a reasonable business justification. This justification should be documented in the data-retention policy (Figure 6).

Business justification must be reasonable. The ability to save personal information through a business justification process does not permit for very long times or indefinitely. The business justification must be reasonable. For example, many companies have significant stores of personal information saved in a data warehouse and other similar types of applications, some of which contain personal information that may be 10 or 20 years old. While this personal information may be useful for marketing purposes, it is difficult to see how this retention would be needed for business purposes supporting the sales to a customer.

Do data warehouses really count?

When most companies think of where their personal information is stored, they think of customer databases or other applications that hold customer information. However, one of the biggest stores of personal information are data warehouses used for business intelligence or analytics. These data warehouses contain copies of excerpts from the primary customer applications. In many cases, they contain years of client data and are used to make decisions, such as pricing, that are not directed at any specific individual. Some mistakenly think these data warehouses "don't count" and are not subject to privacy regulations. These data warehouses are very much subject to these laws and are increasingly a focus of regulators. This is a potential point of contention in an organization, as marketers and other stakeholders are loath to delete this useful personal information.

Documenting a reasonable business justification

Figure 6: An excerpt of a schedule entry listing type of personal information contained in the record and documenting the retention justification.

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 kee formal corporate information permanently. Laws in X and Y countries, where we have substantia operations, require that we keep forma corporate informati permanently. As a corporation, having a historical record c all decisions made the Board of Directo is important to our ongoing business.

Address Records Containing Personal Information >

Personal Information

- 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)

Identify Legitimate Business Need for the Retention Period >

Retention Justification

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 substanti operations, require that we keep formal corporate information permanently. As a corporation, havi a historical record of all decisions made by the Board of Directors is important to our ongoing business.

While record-retention requirements are clear, most privacy laws require a business justification for retaining personal information longer than this minimum. 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 needs. For nonprescriptive rules such as business justification, following a documented, good-faith process demonstrates compliance and provides defensibility.

Policy creation often gets stuck

Figure 7: Data-retention policy creation can stall.

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…

Creating a data retention and deletion policy at the outset appears to be a straightforward task. However, the effort often gets bogged down by endless inputs from and lack of consensus with multiple stakeholders (Figure 7). 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, nonprescriptive, watered-down, or ill-defined policies that may simply list hazy, imprecise retention rules. Avoid this, as it will do little to guide employees regarding what to save and not save.

There is sometimes a tendency by privacy, legal, or compliance teams to "go it alone" and create a data-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.

Attributes of an effective and compliant data-retention policy and schedule

When creating a data-retention policy, there is a temptation to simply create a list of legal requirements and call this the policy. Avoid this, as a poorly designed data-retention policy makes significantly more work. Time invested in creating a compliant and effective policy not only drives better compliance but also saves energy and effort in program execution.

Attributes of an effective data retention policy include:

Address information across all media. A data-retention policy and schedule should reflect a media-agnostic approach that does not focus exclusively on application information stored in databases but addresses all media, including files, emails, and paper documents. Furthermore, the policy and schedule should not, for example, classify email as a record type but rather recognizes email as a medium that contains both records and nonrecords.

Compliant with legal and regulatory record retention requirements. The policy and schedule should reflect federal, state, industry-specific, country-specific, and international record-retention mandates. The schedule should include minimum retention periods, retention trigger events, and descriptions of the records (paper/physical and electronic) that the organization maintains in the regular course of business.

Global policy with local exceptions as necessary. Despite the wide array of privacy and recordkeeping requirements across countries and individual states, it is better to have a single, global schedule with local exceptions where necessary than having multiple geography-specific schedules. It is exceedingly difficult to implement numerous policies, especially as companies often have the same content management system for multiple countries. Note that there are some outliers. For example, China requires retention of some accounting records for 15 years, which substantially exceeds the typical seven-year retention in the United States and the eight-year retention required in several European countries. It may make sense to set the global policy for eight years with a specific local exception for China.

Reflects business value of information. Some information has value to the business. This can include intellectual property, business processes, operational information, etc. Retention should be based on business value. In other words, a company can declare to save information for some time because it has business value even if there is no underlying regulatory requirement.

Identify personal information and retention justification. Data-retention policies should detail which records contain personal information and include a business-retention justification for retaining this personal information.

Focus on "big bucket" categories. In the last decade, many organizations have shifted to a strategy where records are grouped together, with fewer overall retention periods. A simplified system based on broad retention categories—sometimes called "big buckets"—and a limited number of retention periods (such as one year, five years, seven years, 10 years, permanent, etc.) make it easier for employees to comprehend, as well as making disposition easier to automate.

Clear and useable. A data-retention schedule must be easy to understand. The schedule must be identified and organized to make it easy for any given employee to find records in a familiar language. It is helpful to provide specific definitions of record and nonrecord, as well as examples that employees actually use. To improve the results, do not burden employees with descriptions of record types they are not likely to encounter. The traditional approach is to organize the schedule from the perspective of the records manager. Keep it simple and straightforward.

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 privacy or records expiration or disposition. Policies should acknowledge this responsibility.

Socialize and 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.

Final thoughts

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. It may be more work initially, but well-crafted policies make execution much easier and reduce downstream conflicts. It is worth the effort to do it right.

Takeaways

- Most privacy laws require that personal information be kept only "as long as necessary" to fulfill the

purpose for which the information was collected.

- Retention and disposition requirements for personal information have not generally been meaningfully enforced, but that is quickly changing. The "wait-and-see" approach is coming to an end.
- Data-retention and disposition policies and strategies must be synchronized with records-retention requirements. For most organizations, the data-retention policy will enhance their records retention schedule.
- Getting consensus and collaboration from the stakeholders is key to success.
- Time invested in creating a compliant and effective policy not only drives better compliance but also saves energy and effort in program execution.