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.

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.