WHITE PAPER

Creating Common Information Management Capabilities

To Address Both Privacy and Records Management

Abstract

Companies struggle with executing their records management programs, especially for electronic information. At the same time, new privacy and data protection requirements are adding additional compliance requirements. While seemingly different, both privacy and records management share many of the same information management requirements. Many companies are addressing their privacy and records management needs by developing a set of common information management of capabilities.

Sponsored by:

MICRO FOCUS®

contoural

READY. COMPLIANT. IN CONTROL.

Records Programs Challenged by Electronic Information

Records management execution is a source of frustration for many companies. They find it difficult to consistently apply retention, and especially deletion, to their documents and data as prescribed by their records policy and schedule. Instead, this information continues to accumulate, driving up risks and costs. Organizations often become keenly aware of this lack of compliance during eDiscovery or while trying to move to a new storage system. Moreover, records retention execution seemingly pits the legal and IT teams against employees and business units who often want to adopt a "save everything forever" approach.

The problem may not be your employees, but rather the information management capabiliteswithin your records program. Traditionally, records retention programs were designed for the retention and disposition of "official" paper records. Executing a records program came down to sorting the right paper into record storage boxes, and (sometimes) destroying those boxes once their retention period expired. Yet, as companies move into the digital age, their records management practices do not keep pace.

Defensible disposition of unneeded files and emails

As electronic information is more difficult to control than paper, the de facto strategy employed by many organizations was to essentially to never delete files, emails and other electronic information, letting it accumulate into large electronic piles throughout the enterprise. These companies believed that as they were meeting the minimum retention requirements spelled out by recordkeeping laws, they were hence technically compliant. This has resulted in companies having so much electronic information disorganized everywhere that their employees can't find relvant, valuable information that they need amongst the clutter. Records management practices for electronic information have essentially failed at many organizations. Even worse, this "save everything" strategy is quickly running afoul of newer privacy rules. Long term lack of success for managing electronic records have made many organizations reluctant to build out their electronic records capabilities.

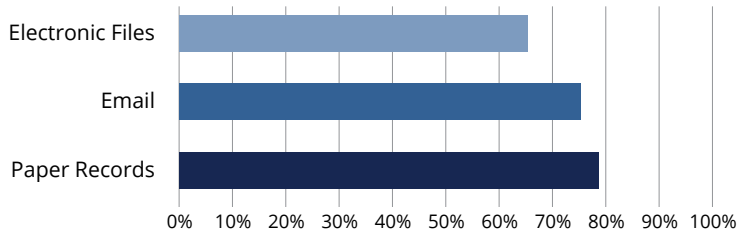


Figure 1. Average percentage of expired records and low-business-value information that can be deleted while maintaining compliance and retaining information still needed by the business.

Source: Contoural

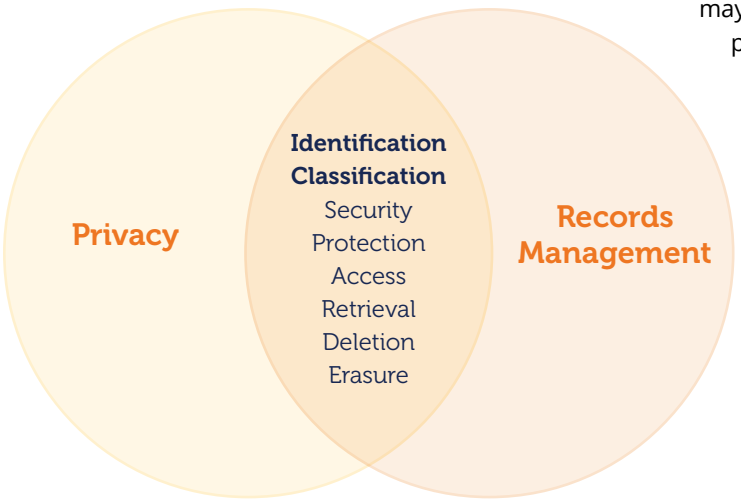
Global Privacy Rules Drive Additional Burden

Compliance and data risks are hitting companies from all sides. New and expanded privacy requirements penalize companies for overretention or improper protection of privacy information. The European Union was one of the first when it implemented its General Data Protection Regulations. Now California is the first of many U.S. States to implement strict privacy laws. Many others are following with their own legistlation, as literally, across the globe nearly all countries are implementing strict rules for management and safeguarding of personal information.

All of these privacy and data protection rules also give residents, consumers and other data subjects the right to know what of their personal information a company may be storing. Once a resident or consumer has requested to see their privacy information, companies and other covered organizations typically have between 30 to 45 days to respond to the request. Furthermore, most laws allow consumers to request that their personal information be deleted. Brazil's new LGPD data protection regulations even give residents the right to have any errors in their personal information rectified. There are steep penalities for non-compliance.

Poor records management and data retention practices are running headfirst into these new privacy rules.

Yet companies' de facto recordkeeping practices of keeping large amounts of electronic information will certainly be tested under these new requirements. Saving large stores of old files, emails and other electronic content which likely contains personal information is contrary to these regulator requirements. Having to search through these older stores across many systems and locations will only frustrate compliance with the subject access request practice. Poor records management and data retention practices are running head first into these new privacy rules.



Finally, the continous barrage of new global privacy requirements may tempt many organizations to only focus on meeting privacy requirements. These "siloed" programs tend to focus on the policy aspects of privacy, but often are weaker on program execution. As privacy requirements such as Europe's GDPR are being enforced, regulators are now focusing on ensuring that companies not only have the proper privacy policies, but that these companies arealso are enforcing them.

Privacy and Records Share Information Management Requirements

Instead of struggling with implementing privacy and records management separately, many companies are creating common information management capabilities that address both privacy and records management needs. By implementing common capabilities companies are finding they are more effective, efficient and compliant in each individual program.

This apparent conflict between the needs and practices of records management and privacy is false. Closer analysis reveals that both require a level of information management capabilities. Furthermore, while both come from different compliance regimes, many of the capabilities to successfully comply in these areas are the same. In other words, developing one common set of information management capabilities can enable companies to build both compliant and effective records management and privacy programs.

The content-focused nature of privacy and records management means that common information management capabilities can address many aspects of both sets of requirements.

Unlike information security, both privacy and records management are primarily concerned with content.

Unlike information security, both privacy and records management are primarily concerned with content. Information security ensures that systems and networks are secure, access is controlled, and the overall infrastructure is protected from threats. Privacy and records requirements are not focused on where or on what systems information lives, but rather personal information for privacy and record content for records management are identified, classified, and managed. The content-focused nature of privacy and records management means that common information management capabilities can address many aspects of both sets of requirements. Simply applying security controls to information will not meet privacy and records management requirements. Rather, organizations need to understand what content they have where, and govern this content effectively.

Privacy and records management common capabilities address four key areas:

Identification and Classification Both records management and privacy require documents and data to be identified and classified by its content. Under California's CCPA, for example, personal information is identified in whether the content can be reasonably associated with or linked to a consumer or household. Documents are classified as records based on their content.

Security and Protection Many of the newer privacy and data protection laws require an enhanced level of security to protect against breaches. Likewise, records management regulations require strict protection of records and other critical information. Note that files, emails and other types of unstructured and semi-structured data in the aggregate likely contain significant amounts of personal information as well as records. Storing these on fileshares and other loosely protected repositories is simply inviting risk.

Access and Retrieval Privacy requirements dictate that a data subject has the right to know what personal information a business has collected and with whom it has been shared. Many of these rules require businesses to show consumers their actual information. Records management also requires that specific records be identified and produced, either to a regulator or in court. Both require the ability to search through large stores of information and selectively produce documents and data based on their content.

Deletion and Erasure Nearly all of the new privacy and data protection regulations require personal information be deleted or "erased" when either the business purpose for which it has been collected has expired or is no longer needed, or if a consumer, resident or other type of data subject requests it to be deleted. There are several exemptions from erasure, including if the data still needs to be retained for recordkeeping purposes, or if it is under legal hold. Likewise, recordkeeping best practices call out for records that have met their expiration periods be deleted, except if they are under legal hold. Deletion or erasure needs to be suspended when these conditions are met and resumed when the original event has passed.

A single program capturing both personal information and records is easier than doing separate inventories for each.

Note that not all privacy requirements align with records management. There are various exceptions to how far back an individual can request their personal information, for example, while records management does not have those same exceptions for records maintained during the entire retention period. Nevertheless, the similarities in managing personal information for privacy and records for records management far outweigh their differences. Taking a step back, many companies are realizing that the similar needs of these programs require them to rethink how their approach.

Creating Capabilities That Address Both Privacy and Records

Realizing these similarities between privacy and records management needs, many companies are building core information management capabilities, that address the overlapping needs of privacy and records management. This typically includes the following steps:

Conducting enterprise-wide, combined personal information and information types inventories

Information inventories need to be created both for personal information as well as records across the document and data landscape. This includes a review of sensitive information and records across email, files, databases, and other electronic media as well as paper stores. A single program capturing both personal information and records is easier than doing separate inventories for each.

Developing, updating and harmonizing privacy, data protection and records management policies

Organizations needs to develop both privacy policies that define what and how they will manage personal information as well as records policies and schedules that determine how long information will be maintained. Syncing these two policies minimizes conflicts.

Implementing and configuring information management technologies

Once policies are in place, organizations need to develop the technical capabilities of implementing these policies. This includes identification, classification, securing, managing, searching, producing and disposing of personal information and records. The same technology and process can be leveraged to address both needs.

Some companies are finding it easier, less expensive and more compliant to simply combine their privacy and records programs.

Creating these core capabilities that address both privacy and records provides tangible benefits. First, conflicts between privacy and records, especially in day-to-day practices, are avoided. Second, managing similar capabilities and processes under a single program helps create an economy of scale. This also lowers costs, as fewer resources can be deployed more efficiently. Finally, organizations that have combined programs have increased compliance for both privacy and records management. In summary, companies are finding it easier, less expensive and more compliant to simply combine their privacy and records programs.

Final Word – The Hidden Win

Many organizations start out combining their programs to drive better compliance, reduce costs and reduce risks. Somewhere along their journey they find that their main program drivers change. These compliance and cost issues are still important, but they find the biggest benefit is increased employee productivity and collaboration. Creating better information management capabilities for privacy and records management drives better management of all information. Employees spend less time searching through redundant, obsolete and trivial information, and instead can find relevant, higher value information more easily. And they spend less time re-creating information that has already been created. They find better information management increases collaboration both within and across different teams. In short, what started as a project to simply drive better compliance, now is viewed as an employee productivity initiative that helps the business meet their goals and reduce risk.

About Micro Focus

Micro Focus delivers file analysis and data lifecycle solutions to help reduce the total cost of regulatory compliance, optimize data, reduce the risks associated with managing sensitive information, decrease the threat of fines, sanctions and penalties for non-compliance while delivering insight, security and governance across business-critical lead applications and repositories.

- **Governance and Compliance:** Deep data discovery, audit trails, data workflow, data classification, and analysis across unstructured and structured information to evaluate, detect and govern sensitive/ high-value information and optimization associated IT systems and infrastructure.
- **Risk mitigation:** Develop custom policies and controls to monitor, remediate and proactively manage identities and data access across critical data repositories to reduce the impact of insider or external data threats and data loss/ IP loss which reduces the threat of fines, sanctions and reputational damage.
- **Time to value and analytics:** subscription pricing and rapid deployment model enables organizations to start tackling in addition to analysis that present data in a way that provides insight, identifies anomalies, and in-depth analytics to drive business decisions
- **Efficiency and optimization:** Data lifecycle management capabilities ensure data efficiency and optimization that reduces storage footprint and/or improves storage efficiency and drives the data lifecycle.

Micro Focus is a global software company with 40 years of experience in delivering and supporting enterprise software solutions that help customers innovate faster with lower risk. Micro Focus is uniquely positioned to help customers maximize existing software Investments and embrace innovation in a world of Hybrid IT - from mainframe to mobile to cloud. www.microfocus.com/scm.

About Contoural

Contoural is the largest independent provider of strategic Information Governance consulting services. We work with more than 30 percent of the Fortune 500 and numerous mid-sized and small companies and provide services across the globe. We are subject matter experts in Information Governance, including traditional records and information management, litigation preparedness/regulatory inquiry, information privacy and the control of sensitive information, combining the understanding of business, legal and compliance objectives, along with operational and infrastructure thresholds, to develop and execute programs that are appropriately sized, practical and "real-world."

As an independent services provider, Contoural sells no products, takes no referral fees from product vendors, nor provides any "reactive" eDiscovery, document review or document storage/warehousing services. This independence allows us to give our clients unbiased and impartial advice while serving as a trusted advisor.

contoural

READY. COMPLIANT. IN CONTROL.

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

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