WHITE PAPER

Beyond Policy

Five Key Information Management Capabilities for Complying with Global Privacy Requirements

Abstract

Companies face a new global wave of disparate privacy and data protection laws. Complying with this patchwork of requirements requires enabling five basic personal information management capabilities. These capabilities can be enabled through implementing smart technology strategies. Compliance with these new requirements not only mitigates risk, but also can protect and enhance an organization's reputation.

Sponsored by:

MICRO FOCUS®

contoural

READY. COMPLIANT. IN CONTROL.

The Challenge of New and Emerging Global Privacy Requirements

Across the world companies and other organizations face a wave of new and proposed privacy laws and data protection regulation. Once limited to European residents, these requirements now span the globe from Asia to South and North America and even Africa. Additional privacy rules are also emerging within countries at the provincial and state level. Even more new laws are on the way as countries have either proposed or are about to implement their own rules. Soon nearly every country and provinces and states within those countries could have their own privacy rules. Traditional archiving approaches fall short of meeting these new requirements, and this is driving many companies to re-examine how they manage information.

Figure 1. New and emerging global privacy rules

Unlike other types of compliance regimes introduced in the past 20 years, these privacy laws are different. They are not being instigated by the regulators themselves, but rather by residents, consumers and employees who see misuse of their personal information as a violation of their rights. Thus this newer legislation has enjoyed tremendous popular support. As such we can expect ongoing and vigorous enforcement, and even additional expansion of these rules. They are not going away. Failure to protect personal information is not only likely to invite regulatory scrutiny and fines, it's likely to invite the ire of consumers and customers.

Unfortunately, these laws are far from uniform. Some of the new privacy laws are similar to Europe's General Data Protection Regulation (GDPR). Other proposed laws are closer to California's Consumer Privacy Act (CCPA). Still there are a large number of variations across all of these laws. These include definitions of personal information, consumer opt-in vs opt-out requirements and most important, enforcement mechanisms. The result is that companies that either have customers or have operations across more than one state or country are likely to face a patchwork of requirements. Today there are no global privacy or data protection standards, and nor are any anticipated to emerge in the near future.

Finally, as with any new wave of legislation, the greatest challenge is simply understanding these laws. Many of the new laws are vague and non-prescriptive. In some cases, laws have come into effect without regulatory guidance on how to actually implement them (see call out box). Understanding what constitutes personal information, how it is to be managed, and what are the rights of residents and other data subjects in many cases is poorly defined and subject to interpretation. It may take years for more substantial guidance from regulators on how to comply with these new rules, yet companies are expected to comply today.

Data Protection vs. Privacy—What's the Difference?

Data protection is about securing data from unauthorized access. Privacy is about who has authorized access and how long it can be retained. Many of the new and emerging regulations address a combination of data protection and privacy requirements, so often these terms are used interchangeably.

A Case Study in Non-Prescription

California Consumer Privacy Act Goes into Effect Without Final Regulations

The California Consumer Privacy Act went into effect on January 1, 2020. Companies are expected to comply with the law's requirements for managing the personal information of California residents. Nevertheless, while the law went into effect in January, the California State Attorney General is not expected to issue final regulations on the law until the Spring of 2020, many months after the law went into effect. These regulations include final determinations on the definition of personal information, management of third parties as well as a number of other critical implementation requirements. Enforcement commences on July 1, 2020 and will be retroactive to the management of personal information back to January 1, 2020. In other words, companies are expected today to fully comply with a law that has not been fully defined.

Why Just a Privacy Policy is Not Enough

Faced with this patchwork of new and emerging privacy laws coupled with a lack of prescriptive guidance on how to implement these rules, many organizations may be tempted simply to create a privacy policy but defer implementing it until there is additional regulatory clarity. This would be a mistake.

First, simply creating a privacy policy without actually implementing it is riskier than having no policy at all. In creating a policy, companies are making a commitment on how they will handle personal information. Failure to implement a policy or follow data protection guidelines once adapted will be viewed by courts, regulators and other stakeholders as at best bad faith to their commitment, or at worst as a deliberate effort to subvert the new requirements.

Second, nearly all of the existing and emerging privacy and data protection regulations have significant consequences for violations. Failure to ensure and demonstrate compliance can lead to significant fines or other regulatory action.

Many believe California's privacy legislation will spawn a new legal industry litigating under the law's private right of action. According to the California Chamber of Commerce "[CCPA's] unchecked liability will lead to a barrage of shakedown lawsuits, as companies facing such substantial liability will be leveraged into immediate settlement, regardless of the strength of their legal defense."

Non-compliance with Europe's GDPR can lead to fines as much as 5% of a company's annual turnover (revenue). A company's uncertainty on how to implement a non-prescriptive regulation does not excuse it from implementing it.

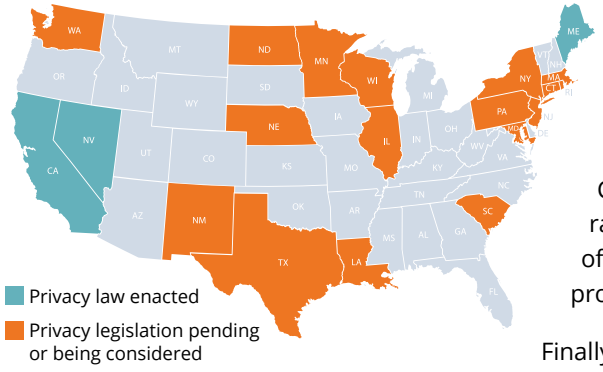

Figure 2. Many states in the U.S. have proposed new privacy legislation based either on Europe's GDPR or California's CCPA.

Even if not facing non-compliance actions by a regulator, companies under CCPA and other new regulations face litigation by third parties. These laws grant a private right of action for breaches, or for some of the proposed legislation, simply non-compliance. A private right of action allows private parties to bring lawsuits on behalf of others. Companies could face significant litigation – not from regulators – but rather from emboldened class action litigators representing thousands of consumers or residents. Simply defending against these claims may prove to be extremely expensive.

Finally, it may be many years before there is any standardization or normalization of these privacy requirements either across states or across countries. "Waiting for what we need to really do" may be a long wait indeed. Waiting for a level of clarity which is not likely to arrive soon simply defers implementation that needs to occur quickly and puts companies farther behind.

Global Privacy Laws: All Share Five Key Requirements

Fortunately, the challenge of implementing a privacy program or data protection guidelines today while facing uncertain and unclear requirements can be addressed. While this collection of global and local privacy laws and data protection requirements have a number of differences, nearly all share five key requirements for managing personal information. If organizations can implement basic capabilities that meet these five requirements, they will be able to meet most or in some cases all, of the existing privacy rules. Furthermore, meeting these five key requirements today will allow companies to launch a general privacy program that is likely to survive an onslaught of new requirements – without the need to significantly redesign their programs as new laws emerge. Put another way, instead of implementing compliance for privacy and data protection laws on a piece-meal basis, organizations are encouraged to develop five basic capabilities first. Then the additional variations of any given privacy law can be addressed, typically with limited effort.

Five Key Privacy Information Management Capabilities

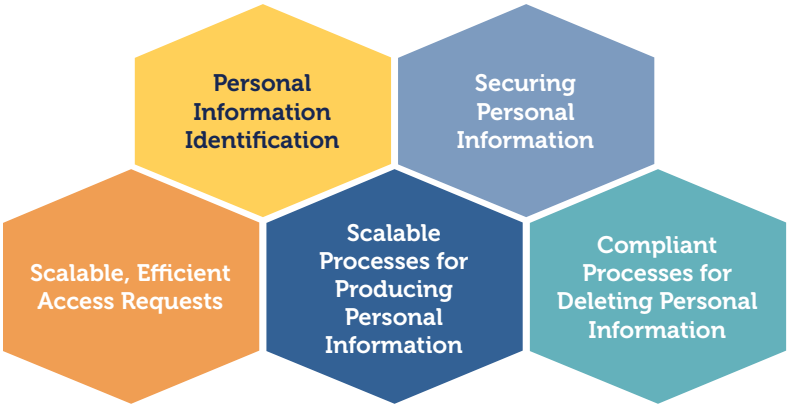

Figure 3. Key privacy information management capabilities.

While privacy laws and data protection regulations across different countries and various states have different specific requirements, nearly all call for some basic capabilities for identifying, securing, managing and selectively deleting personal information. These can be divided into five key information management capabilities:

Personal Information Management Capability 1: Identify What Personal Information You Have Where and With Whom it Has Been Shared

All privacy regulations fundamentally require organizations to identify what personal information is created, received and shared with others. This includes tracking the workflow of personal information through and across various applications, as well as determining where personal information is stored. Many of these regulations also require organizations to track and report with whom privacy information is shared. Creating and keeping up to date an accurate personal information inventory is essential. Note that most companies are using a broader definition of personal information, such as California's CCPA, of what constitutes privacy information. This also protects them in the event the current regulations that define personal information narrowly in the future increase the scope of their definition.

Special attention in personal information inventorying process needs to be paid to structured data contained in databases. Organizations need to identify all of the structured data repositories that contain personal information, including any older, legacy databases that may not longer be active. Likewise, organizations need to examine that data flows between structured systems, both within the company as well as outside to third parties.

UNSTRUCTURED DATA	SEMI-STRUCTURED DATA	ON-SITE PHYSICAL	OFF-SITE PHYSICAL	OTHER PLACES
Databases Database Extracts Desktops File Shares BYOD Enterprise Content Management Office 365/ SharePoint	Email Archive Email Server Email PST Files	On-Site Paper Backup Tapes	Off-Site Paper Backup Tapes Third Parties	BYOD Personal Cloud Storage Apps

Figure 4. Personal information can live not only in databases, but across a variety of repositories or other storage areas.

Personal Information Management Capability 2: Secure All Personal Information Across the Enterprise

Once personal information is identified it must be secured against potential breach or inadvertent disclosure. While breach notification requirements have been around for many years, many of these newer laws such as GDPR put strict new requirements on keeping information secure, as well as timely disclosure in the event information is breached. The greatest risk of a breach incident is typically not the large centralized databases containing customer information, but rather personal information on the fringes: extracts from databases on file shares, laptops with files containing customer lists, etc. Many breaches occur from locations that were not believed to hold personal information. Everything – both large and small repositories – needs to be protected. It is likely that a thorough personal information inventory will uncover unprotected personal information. All of this newly-identified personal information needs to be secured.

Many breaches occur from locations that were not believed to hold personal information. Everything—both large and small repositories—needs to be protected.

Personal Information Management Capability 3: Create a Scalable and Efficient Process for Meeting Subject Access Requests

Nearly all the new and emerging privacy laws have some type of subject access request requirements, in which residents or consumers can find out what of their personal information a company possesses, and who else it has been shared with. While the timelines for responding to access requests varies across countries, they typically must be responded to within 30 to 45 days. Furthermore, the response must address personal information across all locations, not just the larger customer service applications. For any organization that receives more than a handful of these requests per week, it needs to be efficient with scalable processes for conducting these searches.

Security vs. Data Privacy: While information security is a critical component of data privacy, they are different. Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure. It focuses on the IT infrastructure. Privacy is ensuring that personal information content within the IT infrastructure is protected and governed. Good information security capabilities do not guarantee privacy requirements are being met.

Personal Information Management Capability 4: Design Scalable Process for Producing Personal Information

In addition to identifying what types of personal information about consumers or residents a company retains, many of these laws give these data subjects the right to ask companies to produce copies of their actual personal information. These production requests must have the capability to collect and produce from a variety of sources, and then consolidate this personal information into a single package to serve the request.

Personal Information Management Capability 5: Compliant Process for Deleting Personal Information

Finally, consumers and other data subjects have the right to have their personal information deleted, or in some cases de-identified. To be compliant, deletion or erasure should not occur against records that are being maintained per compliance regulations or data under legal hold. Finally, the deletion as well as any encryption or de-identification processes need to be careful that they do not inadvertently lose referential integrity with a database system, such that the deleted data removes pointers between data elements.

There may be specific, additional requirements for any given privacy regime. Europe's GDPR, for example, requires the identification of "special categories" of privacy data. As new privacy rules emerge, there are likely to be more special cases to manage this information. Nevertheless, implementing these key capabilities first will allow companies to address any additional variations as exceptions. The core privacy capabilities will remain the same.

Smarter Strategy is Leveraging Technology to Meet Key Capabilities

Many organizations may be tempted to implement manual processes to meet emerging privacy rules. Complying through manual processes is a fool's errand. Privacy rules require identification, classification and securing of personal information in fairly dynamic environments. Data moves and migrates both through and within an enterprise. While manual processes might be able to capture a one time "snapshot" of this personal information, this quickly becomes outdated. Companies need systematic and preferably automated processes for tracking, managing and securing all of their personal information, and continue that tracking for the life of the data.

Furthermore, companies greatly underestimate the amount and breadth of personal information across the enterprise and missing or misclassifying personal information presents a significant risk. Personal information inventories have shown that companies often have two to three times more personal information than they initially believed. Tracking, managing and securing this ever-changing pool of personal information without tools and technology is nearly impossible. Any strategy for complying with privacy needs to incorporate the right technology.

The other significant challenge company's face is scaling their operational capabilities to meet the likely increase in subject access requests. As the breadth and scope of privacy laws increase, the population of those who can make subject access requests also increases. Managing anything but a handful of these requests to be comprehensive and timely through manual processes is not likely to scale. Instead, companies need to build efficient, centralized processes for searching, producing and deleting personal information from these access requests. This will only be manageable through the deployment of effective technology.

Final Thoughts: Better Information Management for Personal Information Brings Business Benefits

While some companies may begrudge their new privacy responsibilities, complying with these new rules is not optional. There is, however, a silver lining to this dark cloud of privacy requirements. Customers and individuals share their personal information trusting that companies and organizations will be effective custodians of this information. Companies that cannot properly protect personal information will lose the trust of their clients. On the other hand, those that can demonstrate that they can protect personal information will not only avoid risk, but earn more trust for their customers. Privacy capabilities implemented today will allow companies to run a better overall business tomorrow.

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