MICRO FOCUS

3 Ways to Protect Private Data and Ease Compliance Concerns

Executive Summary

Laws mandating the protection of private data have been around for decades. But in recent years there has been a veritable explosion in both the number and jurisdictional reach of those laws. There are now more laws governing data privacy than ever before, with more of those laws applicable to a greater number of business organizations.

Even more data privacy laws are on the horizon.

As noted in a recent Forbes article, "2019 Data Privacy Wish List: Moving from Compliance to Concern," the task of maintaining compliance with these many laws has become increasingly difficult: "It's a messy landslide of different laws that can keep your legal and compliance teams running in circles."[1]

Stated simply, compliance with data privacy laws presents ever-increasing difficulties for companies that conduct business on a global scale. Any global enterprise is likely to be liable for maintaining compliance with many different data privacy laws originating from many different legislative bodies at all levels of government. Maintaining compliance has become so difficult and complex a task that it exceeds the capabilities of a single person, or even a single department. Compliance must now be considered an organization-wide effort, and an organization-wide priority.

This paper discusses some of the difficulties and complexities of compliance. It also explores how three information-management solution features can help to mitigate the risk of fines, sanctions and potentially negative legal ramifications by ensuring the proper management of information throughout its lifecycle.

The need to maintain compliance with governmental regulations mandating the protection and usage of private data isn't a new concept. Laws designed to protect personal data stretch back to 1973 when Sweden enacted The Data Act. Compliance with data protection laws certainly has not grown easier in the ensuing decades.

There's one clear indicator that many companies continue to struggle mightily with compliance: fines. Banks have been fined hundreds of billions of dollars in recent years for regulatory compliance failures.[2] Last year was a record-setting year for HIPAA compliance enforcement actions with more fines levied than in any previous year, exceeding the previous record-setting year (2016) by more than twenty percent.[3] And the recently-enacted General Data Protection

1 https://www.forbes.com/sites/forbestechcouncil/2019/01/15/2019-data-privacy-wish-list-moving-from-compliance-to-concern/#7d9cf5672493
2 https://www.marketwatch.com/story/banks-have-been-fined-a-staggering-243-billion-since-the-financial-crisis-2018-02-20
3 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2018enforcement/index.html

Regulation (GDPR) has resulted in more than 59,000 reported breaches and nearly a hundred compliance-failure fines levied in less than a year's time — including a massive €50 million fine levied against Google.[4]

The obvious takeaway? Compliance isn't easy.

Unfortunately, maintaining compliance is only going to increase in complexity and difficulty. The new GDPR regulations made compliance significantly more difficult and more important for many companies around the globe. That's a trend that will likely continue as more laws are enacted.

Consider, for example, the California Consumer Privacy Act (CCPA), set to become law in 2020. The CCPA will provide consumers with more control over their private information. The new law will also offer consumers a "private right of action" that is expected to unleash a veritable explosion of lawsuits against companies that fail to maintain compliance.[5]

Geography provides little protection for companies that might struggle to maintain compliance with laws such as the GDPR and CCPA. Companies that collect the personal data of citizens of governmental entities that have enacted these laws must comply, no matter the companies' geographic locations, and are liable to enforcement actions for compliance failures.

The Riskiest Compliance-Threatening Activities

Maintaining compliance with legal and regulatory mandates has become a perpetual headache for numerous companies. For many organizations around the world, in fact, the word "compliance" has become a virtual synonym for constant worry and ever-increasing risk.

Most of that worry and risk is generated through the following activities that, though necessary, generate considerable risk of compliance violations:

- **Archiving Compliance and Data Volumes.** Information archiving offers a wide range of benefits. Archiving can increase organization-wide operational efficiencies, boost employee productivity and lower storage costs. But information archiving can also challenge organizations' efforts to maintain compliance. Similarly, the massive volumes of data now available to most organizations can be used in many ways to boost profitability and enhance competitiveness. But managing that sheer volume of data poses compliance challenges.

- **Email Retention.** The retention of emails and other electronic communications is heavily regulated. Emails, particularly, can often contain sensitive or confidential information either in the body of the email or in attachments, magnifying compliance concerns.

4 https://www.helpnetsecurity.com/2019/02/07/gdpr-numbers-january-2019/

5 https://www.microfocus.com/en-us/assets/information-management-and-governance/best-practices-for-gdpr-and-ccpa-compliance

- **Social (and other new forms of) Media:** Social media has become an important tool both for internal communications and for maintaining and enhancing customer relationships. But the benefits of social media come at the cost of increased compliance complications. The multiple forms of data generated through social media exacerbate compliance difficulties, as does the sheer volume of data generated through social media activities.

While these activities generate much of the compliance risk faced by the typical organization, they also generate an impressive range of benefits that simply weren't available a few years ago. The answer to countering the compliance risks generated by these activities lies not in curtailing the activities. Instead, the answer is to implement a solution that will help mitigate the compliance liabilities generated by these activities.

Three Key Capabilities for a Compliance-Enhancing Solution

Any solution that can effectively enhance compliance will provide three very essential capabilities:

1. **The Consolidation of Data in a Central Repository:** In most organizations, archived data spans a wide array of disparate data types. In many organizations, that archived information eventually becomes segmented and siloed according to data type. But siloed archived information can lead to a host of problems.

   A solution that enables the storage of disparate data types within a central repository provides the flexibility that makes compliance easier, while also boosting the potential value that may be derived from the data. Storage within a central repository accommodates efforts to manage the information through a uniform policy in accordance with varying legal, regulatory and IT requirements.

2. **Compliance Support Across Multiple Jurisdictions:** The geographic location of a business enterprise matters very little. Any organization must comply with the laws that are intended to protect the data of persons within any nation or state that the organization serves. A US-based organization, for example, must comply with GDPR mandates if the organization collects the data of individuals within the EU. Any organization that does business with California citizens, or handles the data of California citizens, will be required to comply with CCPA mandates. In the United States alone, at least 24 states have enacted their own data privacy laws.[6]

   Any enterprise that operates on a global scale is likely to require compliance support for, potentially, dozens of different locally-mandated data protection laws. A compliance solution must seamlessly support compliance with all applicable regulatory mandates.

6 http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

3. **Supports Multiple Content Formats:** Not long ago, databases could store and manipulate only a handful of different data types. That is no longer the case. Today, any organization might potentially manage thousands of disparate forms of content. Just a few examples include social media, websites, texts, images and voice files. A compliance solution must be capable of functioning at the high level of complexity required in supporting so many different types of content.

The Micro Focus Solution Support for Compliance

Micro Focus offers a range of solutions that work together in providing unequalled support in enabling regulatory compliance and mandates. The Micro Focus solutions focus upon three key business activities that must be conducted carefully to avoid compliance shortfalls: security, information archiving, and information lifecycle management.

Security Compliance. Security-related compliance failures may originate from both within and without an organization. The protection of sensitive data requires that internal users are monitored so that unauthorized actions are prevented. It's also necessary to constantly guard against external threats. An end-to-end, comprehensive approach is required to properly control data privacy, manage access authorizations and close audit gaps.

The Micro Focus security monitoring solution provides real-time alerts that inform of any occurrences of unauthorized access or unauthorized changes. It provides automated identification and alerting of unusual activity. These features enable organizations to quickly identify and respond to potential threats enterprise-wide, helping to ensure compliance with data protection regulations.

The Micro Focus security monitoring solution helps organizations:

- Detect and address policy violations that may generate IT compliance gaps
- Deliver an at-a-glance view that illustrates current IT compliance posture, and proves that sensitive data is consistently protected
- Ease compliance burdens through automation

Compliant Information Archiving. Modern information archiving requires the ability to store massive amounts of data consisting of multiple data types. Most compliance officers, though, must attempt the task of managing modern-day compliance with systems that require too many manual tasks, and that are infested with operational deficiencies. According to The Radicati Group's 2019 Market Quadrant — Information Archiving Report, obtaining help with compliance is now a key reason that organizations deploy information archiving solutions.[7]

7 https://www.microfocus.com/en-us/assets/information-management-and-governance/the-radicati-group-information-archiving-market-quadrant-2019?

The Micro Focus modular information archiving and risk management portfolio provides the help that so many organizations seek, helping to ease archiving burdens while mitigating the risk of compliance failures. Micro Focus solutions scale compliance and security in the world's largest private cloud, backed by world-class supervision and the ability to control multiple forms of structured and unstructured data — including email, mobile and social media records. End-users and administrators can quickly access, search and audit archived data to easily find the information needed while sustaining a high level of compliance.

All the above features and capabilities contributed to The Radicati Group's selection of Micro Focus to the Top Players quadrant in the information archiving market for 2019 — for the fifth year in a row.

Information Lifecycle Management. Information is any organization's most important asset. It must be carefully managed and protected. But information lifecycle management is a task that has grown increasingly difficult as the volume of information — and information types — has exploded in recent years. At the same time, the regulatory requirements mandating the storage, handling and usage of information have grown in both quantity and jurisdictional reach.

The Micro Focus Information Lifecycle Management solution addresses all the above concerns while simultaneously maximizing the opportunity inherent with the accumulation of massive amounts of data. The solution supports thousands of different types of content in a unified solution that simplifies and speeds compliance with public sector, jurisdictional and regulatory requirements.

In sum, this solution specifically helps with compliance by:

- Reducing the cost and complexity of securely managing structured and unstructured content through policy-based automation and integration with applications
- Lowering the risk of data security and privacy breaches
- Balancing the need for collaboration and content-sharing with security and privacy concerns
- Directly addressing the concerns of security and privacy by protecting content across the enterprise, and throughout the information lifecycle

A Comprehensive Suite of Compliance-Enhancing Solutions

Security, information archiving, and information lifecycle management are all integral to organizations' ongoing and ever-increasing need to comply with government regulations that mandate the protection of data.

Avoiding compliance failures requires a comprehensive approach that addresses the three critical areas of security, information archiving and information lifecycle management.

Micro Focus offers a comprehensive suite of solutions for managing IT risk and enhancing compliance with regulatory mandates.

As part of a complete policy lifecycle approach — from risk assessment through long-term data retention and archiving — the Micro Focus Security, Risk & Governance solutions help enterprises maintain data privacy, mitigate the impact of data and application breaches, and monitor threats to compliance audit visibility.

Together, Micro Focus solutions work to enable the most effective approach to protecting private data and easing compliance concerns.

Contact us today to learn more about how Micro Focus solutions enhance compliance across security, information archiving, and information lifecycle management — the three most common points-of-failure for organizations that struggle to achieve and maintain compliance.

Micro Focus offers decades of industry-leading information archiving experience, and currently manages the world's largest secure private cloud. Selected by Radicati as an archiving leader, Micro Focus offers information archiving services to both regulated and unregulated businesses.