Why Companies Hate Data Compliance and How to Ease the Pain

No one wakes up in the morning thinking, "Wow, I just love regulatory compliance." Multiple governments and industries each impose separate, complex, and sometimes conflicting regulations. And these data compliance regulations continue to evolve. Consequently, keeping track of the changing landscape can feel like playing a high-stakes game of Whac-a-Mole.

Not playing the compliance game opens businesses up to a host of costly penalties, however, from fines to lawsuits and reputational damage. Consequently, businesses continue to invest in staff and equipment and pour time and resources into documentation, testing, and reporting. Meanwhile, data silos hinder efforts, and outdated technology struggles to keep pace.

With the right approach, data compliance does not have to cause so much angst. Automation and AI, for instance, improve speed and accuracy of many compliance tasks. Staff training helps to build an essential compliance culture. And proactively addressing data governance, cyber security, and other common compliance requirements helps to avoid costly issues.

Embrace Automation and Leverage Compliance Technology

Compliance technology has come a long way in recent years, particularly in the areas of analytics and automation. For example, AI-enhanced tools can analyze huge, diverse data sets that include privacy laws, industry regulations, and internal policies. These tools ease the process of identifying relevant regulations and mapping internal processes accordingly.

Secondly, intelligent compliance technologies automate important tasks such as data collection and classification, monitoring, and reporting. Humans alone cannot feasibly manage vast stores of data to achieve compliance, but automating these tasks can improve both speed and accuracy.

For instance, using both automated and manual classification, organizations can tag sensitive data such as personal health information (PHI) or financial data. They can then track that information wherever it travels. Customized alerts automatically notify compliance personnel of possible issues, and the technology can even automate certain remediation actions.

Invest in Training

While technology plays an essential role, compliance begins and ends with humans. Organizations must take the time to raise awareness and foster a culture of data compliance among their employees. Clear and consistent training will help employees understand relevant regulations and their role in compliance.

Compliance training should go hand in hand with security awareness training. For instance, employees need to understand how to safeguard sensitive information, including appropriate sharing and retention. They should also understand how to recognize and report potential cyber security threats such as phishing.

Shift Modes from Reactive to Proactive

To truly remove the pain from compliance efforts, organizations must move away from reactive mode and checkbox compliance. This will involve strengthening information governance and cyber security practices throughout the organization.

To begin with, conduct risk assessments and penetration testing to identify security vulnerabilities. Then adjust data security controls and policies accordingly. Additionally, conduct a data audit to determine what data the organization holds. Build a data map that identifies data location, owner, value, sensitivity, and retention needs.

With this information, organizations can begin to build effective data security and information governance frameworks. Strong information governance will address many compliance issues while also improving data value.

Prioritize Common Compliance Requirements

Facing a growing pile of compliance regulations can be overwhelming. But most regulations share several common elements. By building those common elements into information governance and security efforts, businesses stay ahead of the compliance game.

For instance, pay particular attention to sensitive data, as it requires special handling. Know where it lives, tag it, and monitor it. AI-enhanced compliance tools help by automating much of the data classification and monitoring.

Next, many regulations make businesses liable for how their vendors approach data privacy. Consequently, organizations should carefully and regularly review vendor contracts, looking for necessary language regarding data privacy and security. Carefully control vendor access and perform regular supply chain audits and monitoring.

Additionally, many regulations include provisions regarding privacy policies and the ability for consumers to exercise their rights. Make sure that privacy policies are clearly displayed on public-facing apps and websites. Include intuitive forms for consumers to specify their preferences regarding cookies, sharing of personal information, and targeted advertising.

Partner with Compliance Experts

To ease the process even more, many organizations choose to partner with compliance experts. Messaging Architects consultants deliver the tools and expertise to strengthen information governance and data security, automate many compliance tasks, and implement continuous compliance monitoring.