Data Compliance Best Practices for 2023 Safeguard Critical Data Assets

With four more states enacting new data privacy laws in 2023, organizations must pay special attention to compliance. An increasing volume of data, combined with a hybrid workforce and sophisticated cyber threats, makes compliance challenging. But companies that use data compliance best practices reduce risk and enhance their competitive position.

Compliance involves addressing both cyber security and data privacy. Data retention and destruction policies also play a key role. Consequently, compliance best practices involve improving data visibility through information governance and monitoring. They also include updating data policies and security practices and addressing the human component.

Use AI to Strengthen Information Governance

Because achieving compliance requires that organizations know what data they have, where it lives and who has access to it, information governance plays an important part. For instance, several privacy regulations include the "right to be forgotten." This means that a company must be able to find and delete an individual's personal data upon request.

Additionally, rules such as HIPAA and PCI DSS mandate the careful control of sensitive data such as protected health information (PHI) and financial data. These regulations require that organizations locate and tag all sensitive data wherever it lives or travels. With vast amounts of data on multiple platforms, finding and tagging that data represents a monumental task.

Fortunately, AI and machine learning can help. The average company manages hundreds of terabytes of data, with new data created every minute. Humans cannot feasibly find and classify all sensitive data manually. However, using pattern matching and machine learning, automated AI tools can find and classify sensitive data quickly and accurately.

Gain Visibility Through Compliance Monitoring

To identify compliance gaps, organizations should conduct regular compliance and security audits. In addition, continuous compliance monitoring allows data administrators to proactively address any potential compliance issues. Here again, automation plays a critical role.

Much of a company's most sensitive information hides in unstructured data such as emails, PDF files and instant messages. This data can prove difficult to manage. But automated tools, powered by AI, monitor both structured and unstructured data for compliance violations.

These monitoring systems deliver automated alerts to appropriate personnel while taking precautionary action. For example, if a user attempts to improperly share PHI, the system will block the action and alert compliance officers. In addition to keeping sensitive data safe, monitoring allows the organization to demonstrate compliance in the event of an audit.

Regularly Review Data Policies

Data policies play an essential role in compliance. For instance, policies mandate who can access data and how long data should be retained. They also govern how users can share data and with whom. And they may cover certain security actions, such as the encryption of sensitive data.

An effective electronic communications policy includes not just the written policy, but also the technology to enforce that policy. For example, tools such as Microsoft 365 allow organizations to automatically prohibit sharing or destruction of sensitive data. Data policies require regular review and updates as the regulatory landscape changes and as the company adopts new tools.

Implement Essential Cyber Security Practices

Because compliance requires keeping data safe and secure from unauthorized access, data compliance best practices necessarily include security measures. At a minimum, organizations should use firewalls, keep software up to date, change default passwords and implement both multi-factor authentication and encryption.

In addition, security teams should regularly review access rights and permissions. Apply the principle of least privilege to ensure that users have the minimum amount of access they need. And make sure to remove user accounts and access when no longer needed. Tools such as Microsoft Entra help to automate access and identity management.

Provide Compliance and Security Awareness Training

Regardless of the technology involved, no compliance or security effort will prove successful if it ignores the human component. Take time to engage employees at all levels through regular privacy and security awareness training. Complement the training with phishing simulations and internal events such as privacy awareness month.

Compliance Technology Powers Data Compliance Best Practices

With a rapidly evolving regulatory environment, compliance experts suggest taking a big picture approach to achieving compliance. That is, look for privacy solutions that apply to most privacy laws, rather than applying different rules to different locations in compliance with individual states.

Technology will prove essential to a successful compliance strategy. For instance, intelligent compliance solutions from eGovernance provide insight into all indexed data through a single portal. Automatic reports alert auditors whenever an issue arises, allowing for immediate remediation. Proactive intervention saves time and money while delivering peace of mind.