druva

White paper

How to protect your business from data compliance violations and costly fines

Implement a proactive data compliance monitoring approach

Q221-20178

The compliance landscape

As data continues to grow at a high-volume and is geographically dispersed across workloads and endpoints, your organization needs to increase data visibility and centralize control to ensure data compliance. The compliance landscape is driven by security and privacy concerns due to ever-changing compliance regulations (i.e., GDPR, HIPAA, CCPA, etc.). If your organization fails to adhere to these regulations, you can be subjected to long-term concrete ramifications — both reputational and financial.

According to CoreView, there has been approximately $429 million in GDPR fines to date[1] and in the past few years, there has been a 250 percent increase in data regulations. With these data regulation increases, "61 percent of a compliance officer's time is spent on other compliance tasks' such as management of regulatory implementation."[2] IT and compliance teams are witnessing higher levels of non-compliant data stored on user devices without any controls in place. Working with multiple teams, personnel, and systems for data collection has become a great challenge for most IT and compliance teams.

This paper outlines the challenges that IT and compliance teams face, including the need for proactive compliance monitoring, the risks and consequences associated with failed compliance regulations, and which solution can help defend against data compliance violations.

Most common compliance challenges

Unfortunately, your IT and compliance teams could have already experienced or are currently facing multiple compliance challenges. In order to overcome these challenges, compliance officers or managers typically hire third-party consultants, or leverage point solutions to manage data governance and compliance. However, there are also challenges and risks associated with this type of approach. To provide a brief overview, here are some key challenges organizations commonly face when it comes to data compliance and available solutions:

- New and multiplying regulatory and corporate data governance requirements
- Lack of resources to quickly respond to audits, resulting in additional costs
- Increasing fines and penalties for compliance violations
- Drastic impact on an organization's reputational capital
- Minimal central visibility into all data assets and geo-specific regulations
- Endpoint data risks and overspend ($1M-2M per year) associated with employee departures, which require regulatory audits and investigations
- Misconception that tools like Microsoft 365 can provide sufficient data protection and compliance capabilities

Common motivations for data compliance

Your organization might already have plans or is in the processing of implementing plans, to combat the security and compliance challenges listed in the previous section. Nonetheless, many organizations are also driven by other factors, aside from basic motivators like abiding by compliance rules and avoiding violation penalties and fees. Here are a few key data compliance motivations that are top-of-mind for organizations today.

- **Security —** Compliance is most often implemented and adhered to in the form of security controls. These security controls are spread across people, processes, and technology. Combining these three attributes in the form of security controls goes a long way to easing audit and compliance concerns. Audits and attestations that validate the existence of security capabilities help organizations portray a positive public image and give customers confidence that they are protected.

[1] Coreview,"Major GDPR Fine Tracker – An Ongoing, Always-Up-To-Date List of Enforcement Actions" 2020
[2] Thomson Reuters, 2020

- **Maintain brand reputation —** Brand reputation is the bedrock of customer trust and market share — precious commodities that can disappear in a nanosecond with a publicized security breach or negative compliance finding.
- **Avoid punitive or financial impacts —** When an organization is responsible for the security and confidentiality of private or sensitive data, loss of control of that information comes with its own consequences. Many compliance regulations today specify various financial, punitive, and even criminal sanctions in the event of a data breach. For example, an enterprise selling widgets online is a controller. The companies maintaining the website and shipping the product for that controller would be identified as processors. The enterprise/controller is the party responsible for GDPR compliance. However, if a shipper/processor fails to protect the customer's personal data, they may be subject to GDPR penalties as well.

Penalties for failed compliance regulation

The following table lists these negative impacts for security breaches under various compliance regulations:

The Health Insurance Portability and Accountability Act

- Healthcare organizations can face legal actions, including the suspension of business operations
- Financial and other fines can be imposed

The Payment Card Industry Data Security Standard

- Fines from card issuers and/or the government
- Claims and lawsuits against negligent organizations

The Sarbanes-Oxley Act of 2002

- Up to 20 years imprisonment for non-compliance
- Claims and lawsuits against negligent organizations

The California Consumer Privacy Act

- A civil penalty is $2,500 for each violation
- An intentional penalty is $7,500 for each violation[3]

While fines and prison terms are rather concrete consequences, in terms of being able to measure impact, there is also an intangible effect that comes with non-compliance in the form of a diminished reputation. Given that many regulations have mandatory reporting requirements to government agencies and media outlets in the event of breach or non-compliance, the following impacts can also take effect:

- Lack of consumer confidence
- Loss of sales and public perception
- Negative effect on stock price
- Negative media attention
- Future products and services called into question

Whatever the reasons for failing to meet regulatory and compliance requirements, the end result is the same when it comes to penalties and reputational impact.

[3] California Consumer Privacy Act, 2020

Compliance frameworks and regulations

While there are many compliance frameworks and regulations depending on industry, vertical, and geography, the following are the most common that have an impact on the consumption of cloud services and the measurement of security within those services:

ISO/IEC 27001: 2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within the context of the organization. ISO 27001:2013 also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and intended to be applicable to all organizations, regardless of size or type.

Service Organization Control (SOC) is a set of accounting standards that measure the control of financial information for a service organization. SOCs are covered under both the SSAE 16 and the ISAE 3402 professional standards. While SOC 1 examines the financial reporting controls of an organization that provides services to end users, SOC 2 focuses on organizational controls based on Trust Service Principles (TSP). Those TSPs cover the areas of security, availability, processing integrity confidentiality, and/or privacy.

Within cloud service providers, SOC 2 is a common form of measurement to evaluate security controls. Within SOC 2, there are two different kinds of audits: Type 1 and Type 2. SOC 2 Type 1 measures organizational controls at a point in time, where Type 2 measures organizational controls for a period of time.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation from the European Union (EU) Parliament to strengthen and unify data protection for individuals within the EU). The GDPR also addresses exporting personal data outside the EU. The GDPR's main objectives are to give EU citizens control of their personal data, simplify the regulatory environment, and standardize international business practices. GDPR went into effect in 2018 and replaced the EU Data Protection Directive originally passed in 1995.

The California Consumer Privacy Act (CCPA) was enacted in 2018 and went into effect on January 1, 2020. This piece of legislation signals a new era for California consumer privacy rights. The CCPA grants California consumers the right to know what personal information is being collected, used, shared, or sold; the right to delete personal information held by businesses; the right to opt-out of the sale of personal information; and the right to non-discrimination in terms of price or service.

The CCPA applies to businesses that:

- Have gross annual revenues of more than $25 million
- Buy, sell, or receive information on the personal information of 50,000 or more consumers, households, or devices
- Derive 50% or more of annual revenues from selling consumers' personal information[4]

Passed in 1996, the **Health Insurance Portability and Accountability Act (HIPAA)**, is U.S.-specific legislation that provides data privacy and security provisions for safeguarding medical information. Of the original HIPAA legislation, Title II has the most impact on IT departments, as it directs the U.S. Department of Health and Human Services to establish national standards for processing electronic healthcare transactions. It also requires healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS.

HIPAA also went through additional updates in 2009 (HIPAA HITECH) and 2013 (HIPAA Omnibus Rule), which specified technology requirements as well as increased penalties for HIPAA compliance violations to a maximum of $1.5 million per incident and other criminal penalties.

[4] California Consumer Privacy Act, 2020

The Federal Risk and Authorization Management Program (FedRAMP) is an assessment and authorization process that U.S. federal agencies use to ensure security is in place when accessing cloud computing products and services. FedRAMP consists of a subset of NIST Special Publication 800-53 security controls which were specifically selected to provide protection in cloud environments. A subset has been defined for the FIPS 199 low categorization and the FIPS 199 moderate categorization. The FedRAMP program has also established a Joint Authorization Board (JAB) consisting of chief information officers from the Department of Defense (DoD), Department of Homeland Security (DHS), and the General Services Administration (GSA).

Before the introduction of FedRAMP, individual government agencies would use and manage their own assessment of cloud service providers using components of the Federal Information Security Management Act (FISMA) of 2002.

The critical need for data compliance monitoring

Data compliance monitoring is a risk-management approach to security and cyber threats that provides visibility into the attack surface of an organization. This monitoring capability is largely focused on point-in-time measures from a control perspective. Today's compliance officers and managers usually hire third-party consultants or use point solutions to manage data governance and compliance across the organization. But, why do you need data compliance monitoring?

Data compliance monitoring is essential for organizations to adhere to compliance regulations (i.e., GDPR, HIPAA, and CCPA). Organizations that fail to do so are subject to concrete fines and penalties in addition to other consequences. In order to adhere to these regulations, organizations need a solution to increase data visibility and central control to ensure data compliance across endpoints, workloads, and geographies.

Part of compliance monitoring is also responding to inquiries from government organizations (i.e. subpoenas). In order to do this, your organization must have solutions in place that simplify data collection and analysis no matter where it resides (i.e. eDiscovery). The ability to respond quickly to audit requests, whether ad hoc or planned, requires that your organization take a proactive approach to compliance monitoring.

Implementing a proactive compliance strategy

When your organization wants to protect its critical data, it is important to find a third-party partner that can ease compliance concerns on a global scale. Organizations cannot afford to be reactive and only take action when a violation is caught and high fines are given. With Druva, organizations remain in control of their data with proactive compliance monitoring, reduce data risks, and avoid fines related to data regulation. Here's how Druva can help your organization.

Proactive data compliance monitoring and testing

Druva enables your organization to proactively and automatically monitor data compliance across all your workloads — and receive and respond to violation alerts — all from a single dashboard. For instance, you'll get continuous, 100% automated compliance scanning alerts to violations across data sources like endpoints, emails, Microsoft 365, OneDrive and Google Drive. You'll also receive global search for sensitive files.

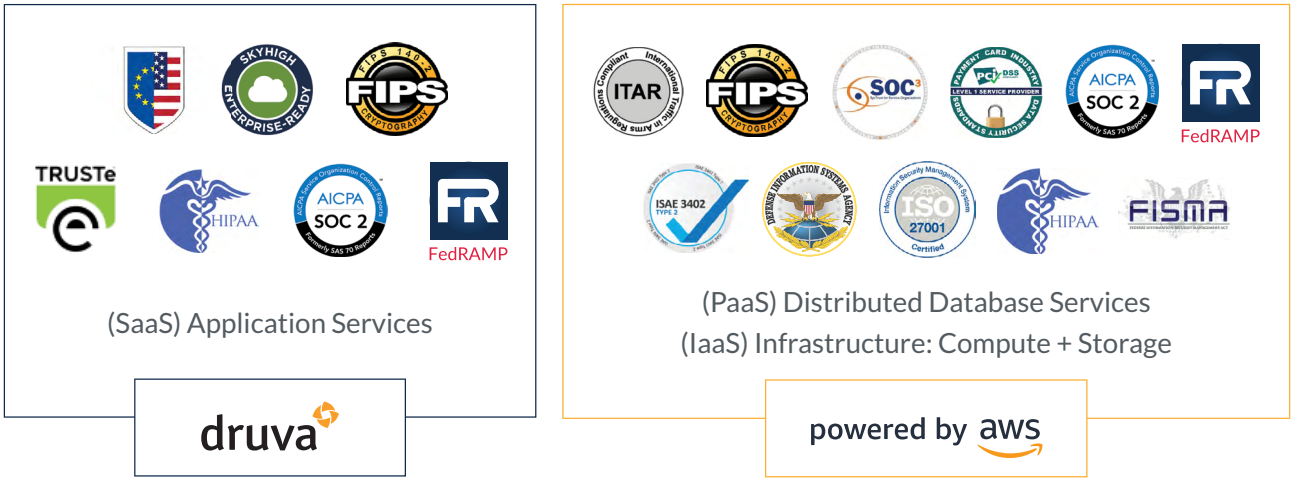
With Druva, compliance is also delivered, at speed:

- Defensible deletion of non-compliant data
- 'Right to be forgotten' and 'right to access'
- Limit distribution of sensitive files

Security and compliance frameworks

While many SaaS vendors simply rely on the certifications that the CSPs provide for the infrastructure as their security model, Druva has gone above and beyond, achieving compliance and attestations for its cloud service. Druva is certified or can claim compliance with the following certifications and frameworks:

- SOC 2 type II audited
- HIPAA compliance
- FIPS 140-2 compliant
- FedRAMP moderate ATO



Pre-built, customizable templates and rules

Druva's pre-built, customizable templates and rules allow you to monitor for potential violations of key global regulations like GDPR, HIPAA, CCPA. Empower your organization with the flexibility to customize out-of-the-box templates and rules, or build your own, to support regulatory or internal governance requirements.

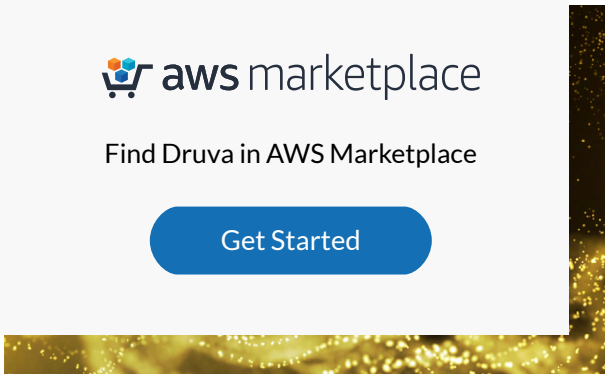
Reduce business risk and quickly respond to violations

With Druva, you can proactively and automatically monitor data regulation compliance, across workloads, and get alerts, within 24 hours of a violation. You'll also be able to promptly address violations, from a single compliance dashboard, by defensibly deleting sensitive data in backup or in source, or both.

Conclusion

As your organization's business-critical data volume increases and is dispersed geographically amongst endpoints and workloads, you'll need a centralized, modern, and proactive compliance monitoring solution that helps your organization reduce risks and avoid fines related to data regulations. Start evaluating your current data compliance monitoring strategy and consider a more modern and effective approach. A third-party cloud data protection leader, like Druva, provides unique solution features such as policy and rules automation — giving you the compliance monitoring tools you need to easily keep account of key regulations, report violations, and implement defensible deletion.

Defend against data compliance violations with proactive compliance monitoring druva.com/solutions/proactive-compliance/



druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.