Veritas Alta™ SaaS Protection Data Retention

Introduction

Compliance Challenges

Modern organizations face a complex challenge to achieve—and remain in—compliance, with several data retention regulations that govern the electronic data they maintain across a variety of storage platforms and mediums. These regulations apply to data assets stored on-premises, data stored in hybrid or public clouds, and data found in SaaS offerings such as Microsoft 365.

These regulations, such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the California Privacy Rights Act (CPRA), General Data Protection Regulation (GDPR), and the Fair Labor Standards Act (FLSA) may require organizations to retain data for a certain period, or may require organizations to delete the personal data of their users after a certain period. Not retaining data long enough and being found non-compliant, as well as keeping data for too long, represents significant risk. Organizations may be subject to multiple regulations at the same time. They need to establish data retention policies, and implement them properly to mitigate risk and ensure compliance.

Achieving compliance for SaaS data can be a unique challenge for organizations, since responsibilities in a SaaS ecosystem can be cloudy. SaaS offerings are provided as a service, and many of the responsibilities previously owned by the customer, such as providing hardware resources, installing, configuring, and updating the software elements, managing day-to-day health and operational readiness, and even providing a storage medium for data generated within or by the offering, are managed by the SaaS provider. With so many challenges moved off the shoulders of the customer and onto the SaaS provider, it may be erroneously presumed that critical services such as data protection and data retention are also provided by the SaaS provider.

Risks of Non-Compliance

The consequences of non-compliance are meaningful, regardless of where non-compliance is discovered. Organizations that are found to be non-compliant can be at risk of incurring hefty fines that can range from hundreds of thousands, to millions of dollars. In addition to financial penalties, organizations could potentially find their customer relationships and their brand damaged.

- British Information Commissioner (ICO) imposed a fine of €9 million on a U.S.-based artificial intelligence company in May 2022 for multiple violations, including the violation of storage limitation principle by not providing a data retention policy
- Italian Data Protection Authority imposed a fine of €200,000 on a major university in September 2021 for violations including not providing students with information regarding specific retention periods for personal data

GDPR

The GDPR security law is recognized by many as one of the toughest in the world. Regulatory fines related to GDPR compliance can be especially costly. In 2021, nearly €1.3 billion in fines were collected for GDPR violations. For the year 2023, more than €1.6 billion in fines have been collected as of May.

It is critical that all organizations ensure they are in compliance with all applicable laws and regulations regarding the security and retention of data.

Shared Responsibility

Understand Data Responsibility

Many organizations are surprised to learn that cloud service providers, such as Microsoft, have a shared responsibility model that places responsibility for several areas of data management squarely upon the shoulders of the client organization. Perhaps the most significant of these responsibilities is for the data itself, which remains the responsibility of the customer (client organization), regardless of where the data is hosted—be it in a SaaS, PaaS, IaaS, or on-premises infrastructure. This is illustrated by the image below from Microsoft:

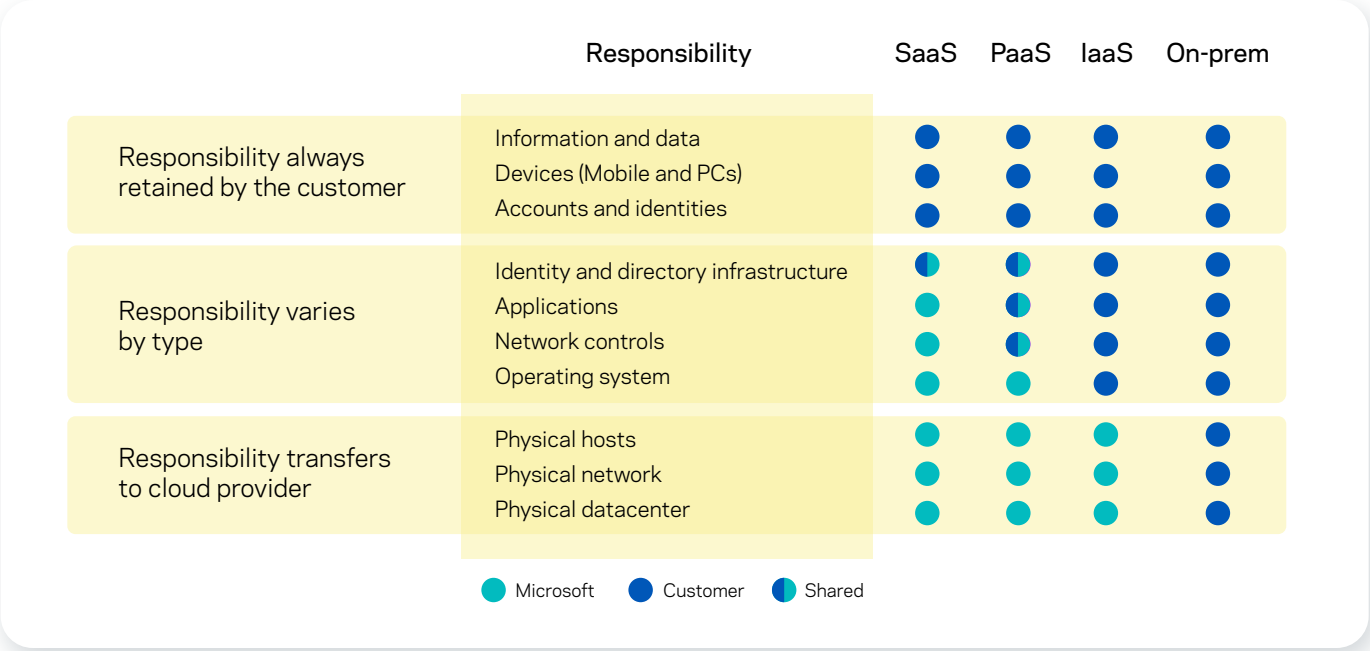

Figure 1: Microsoft's division of responsibility

Compliance is Up to You

If SaaS applications and data are not properly managed from a data retention and regulatory point of view, it is the organization that will be found liable and responsible for the resulting fines, not the SaaS provider. Each organization with investments in SaaS offerings must take steps to implement policies and procedures to ensure they are in compliance.

Achieve Data Retention and Compliance for SaaS Data

Reduce Risk, Eliminate Uncertainty, and Take Control of SaaS Data

Modern businesses can protect and secure their cloud-based, business-critical SaaS data against loss and retain their data in compliance with industry regulations with the help of Veritas Alta SaaS Protection along with other data retention best practices. Veritas Alta SaaS Protection is a powerful data management and protection solution that delivers a managed, cost-effective, automated backup as a service (BaaS) for the leading SaaS business applications—through a single, intuitive interface.

These unparalleled data protection and retention capabilities include:

- **Policy-Based Management:** Designed for performance and scale. Powerful data identification and tagging by a variety of attributes inform the creation of automated policies to govern how long data is retained within the Veritas Alta SaaS Protection ecosystem. Additional retention features control data collection, preservation, processing, review, and analysis.

- **Immutable Storage:** Backups are stored on immutable storage, that is, storage that does not allow alteration of the data and does not allow anyone—even administrators—to delete any of the data before the expiration of its set retention period.
- **Data Retention:** Administrators can create custom retention policies for their data that provide the flexibility to set different retention periods for different types of data. This capability effectively provides automated compliance with data retention regulations.
- **Data Location Controls:** Organizations operating internationally may come across data sovereignty regulations that require any data related to business conducted in a specific country or with customers residing in a specific country to be stored within the borders of that country. Veritas Alta SaaS Protection allows customers to set data location controls to determine where to store different backup data, providing automated compliance with data sovereignty regulations.
- **Federated Search:** Veritas Alta SaaS Protection indexes all backup data it ingests and can perform full-text indexing of its content, allowing for blazingly-fast results when searching the backup data. Veritas Alta SaaS Protection is supported by highly-configurable search filters for the inclusion and/or exclusion of data based on any combination of criteria you care to define.
- **Exporting Data:** Veritas Alta SaaS Protection makes it easy to export copies of data as needed, so you can easily fulfill your duties in the context of data retention regulations.

Learn More

For more information about getting started with Veritas Alta SaaS Protection, visit the Veritas Alta SaaS Protection website, or contact Veritas Sales.

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1966 08/23