rubrik

Accelerate GDPR Compliance with Rubrik

NEW DATA PRIVACY REGULATION WITH A GLOBAL IMPACT

On May 25, 2018, any company that processes data around EU citizens, regardless of the company's location, will be impacted by the General Data Protection Regulation (GDPR). The wide-reaching regulation aims to standardize data privacy laws across Europe, protect EU citizen data privacy, and reshape how companies approach data privacy. Non-compliance can lead to steep penalties of up to €20 million or 4% of global annual turnover (revenue) from the preceding financial year (whichever is greater).

UTILIZING MODERN DATA MANAGEMENT SOLUTIONS TO EASE INTO GDPR COMPLIANCE

To ease the path of GDPR compliance, companies should invest in data management solutions that are equipped to:

- Span modern enterprise IT environments from data center to cloud while ensuring end-to-end data security (data encryption);
- Handle surge in digital data growth such that data can still be managed in a single system;
- Automate data protection policies and expiration to reflect business SLAs and appropriate retention periods;
- Provide visibility and reporting on retention, compliance, and system, user and log events; and
- Define and exercise granular control of user access to data.

Rubrik delivers this in a single platform, collapsing a complex landscape of point solutions that are cobbled together to deliver data protection. Companies use one interface to easily manage the data lifecycle from creation to expiration. Legacy data protection solutions tend to fragment the data landscape due to architectural complexity and inability to scale, increasing the difficulties for enterprises to meet GDPR compliance.

GDPR IMPACT ON DATA MANAGEMENT AND HOW RUBRIK HELPS

Below is a summary of key GDPR changes that impact data management and how Rubrik can help enterprises meet GDPR compliance.

Key GDPR Changes	How Rubrik Helps
Companies need to be accountable for how they comply with data privacy and protection via technical and organizational measures (Article 5). Using a solution with strong reporting capabilities enables companies to demonstrate compliance.	• Companies can use Rubrik Envision to deliver custom visual reporting on retention, compliance, and capacity. • Custom reports can be configured with a few clicks to span the entire Rubrik environment, on-prem to cloud. System, user, and log events are also readily accessible.
Right to be Forgotten (Article 17) requires companies to delete personal data when a data subject requests erasure of personal data.	• Rubrik can expedite data discovery for expiration through its global predictive search technology. Rubrik indexes all data managed within the system, with metadata maintained for all data managed on-premises or in the cloud. • Users conduct Google-like searches – type in the query, and Rubrik instantly returns predictive search results across the entire system. • Possible deletion of data is dependent on the source, including its impact on related data and other applicable regulations.

Defining use cases and managing consent (Article 6) requires companies to define a clear use case for gathering data and obtain consent from EU citizens. Data should be deleted once the use case concludes. To comply, companies need to ensure the right data retention and deletion policies from data collection to storage.	• With Rubrik, companies can simplify the process by which they apply and ensure data retention and deletion. Users define 1) retention policies that map to business SLAs or the data use case and 2) what data sets should receive this policy. • Rubrik automates the execution of these policies, and reporting (Envision) discloses whether compliance was met.
Data Protection by Design and Default (Article 25) requires that data protection is designed into the development of business processes for products and services from the very beginning vs. tacking on data protection at a later point. Article 23 mandates that companies should hold and process only the data absolutely necessary for the completion of the use case (data minimization), as well as limiting the access to personal data to those needing to act out the processing. Privacy settings must be set at a high level by default.	• By using Rubrik, companies can leverage end-to-end encryption to enforce data security and privacy. Users can choose from hardware- or software-based encryption to encrypt data-at-rest. • For hardware-based encryption, Rubrik offers the r528, a FIPS 140-2 Level 2 certified solution. For software-based encryption, Rubrik offers the r300s Series, which utilizes AES-256 encryption. Any data sent to the public or private cloud (object storage, NFS) is encrypted in-flight and at-rest to maintain privacy regardless of the location of the data. • Companies can also define and exercise granular control of user data via role-based access control (specific roles mapped to specific data objects). This limits access to user data to only those who should be processing the data.
State of the Art (SOTA, Articles 25 and 32) encourages companies to implement IT solutions and processes that always protect personal data in the best possible way. Investing in market-leading data protection and security solutions with a track record of rapid innovation makes it easier to comply.	• By investing in Rubrik, companies are investing in a modern data management solution that aims to simplify data management for enterprises as they operate services on-premises or in the cloud. • Rubrik has established a track record of rapid innovation by delivering nine product releases in the span of three years, supporting the key operating environments used by enterprises worldwide.
Companies must assess the risk of processing and accessing personal data and implement measures that ensure an appropriate level of security (Article 32). This includes the ability to promptly restore the availability and access to personal data. The effectiveness of such security measures should be regularly tested and evaluated.	• Rubrik expedites the recovery of data breaches, including Ransomware. Data is stored on Rubrik in an immutable format such that a company can quickly recover without data loss, no downtime, and without paying a ransom. • Customers leverage Rubrik's Instant Recovery (Live Mount) and API-first platform to automate file and application recovery. Customers can also use the Live Mount feature to test their DR plan without impacting production workloads and to prevent creation of a separate copy for Dev/Test or DR.
Companies using cloud services should understand what data is stored in the cloud, where it resides, and how compliance is being met. Data transfers to countries outside the EU should be either to countries with similar standards in data privacy protection (Articles 45) or under an agreement that ensures compliance with the GDPR through the usage of model contract clauses for transfer of personal data to third countries (Articles 46, 47).	• Rubrik is designed for the cloud era – if companies utilize cloud services, Rubrik Envision can deliver custom reporting to help users understand what data is stored in the cloud, where it resides, and whether compliance is being met.