SOLUTION BRIEF

Using Commvault Cloud to Assist in GDPR Compliance

The General Data Protection Regulation, or GDPR, is a set of rules effective in the European Union that grants individuals the right to control their personal information. The regulation applies to any organization that handles the data of EU citizens, regardless of where the organization is based. GDPR has become the standard for data privacy, and many countries and states in the U.S. have attempted to create legislation that mirrors it.

In addition to individuals' rights to control their data, the GDPR also emphasizes data security, privacy by design, and accountability for businesses handling EU citizen data. This requires information security and IT teams to understand the sensitive data they collect and store throughout their IT stack.

WHAT IS SENSITIVE DATA?

The GDPR covers information that can be used to identify a person, often called personal data or personally identifiable information (PII), including:

- Basic identification: Name, address, ID numbers
- Online identification: IP addresses, cookie IDs, location data from phone
- Biometric data: Fingerprints, facial recognition data
- Health data: Medical records, genetic information
- Personal characteristics, considered special categories of personal information (SPI): Race, ethnicity, political opinions, religious beliefs, sexual orientation

However, sensitive data can go far beyond what GDPR requires. Organizations' sensitive data may also include business-related information, such as financial data, confidential information, and internal-only documents pertaining to projects, human resources, or other proprietary information.

WHAT IS REQUIRED BY GDPR FOR PII AND SPI?

The GDPR helps organizations advance their security initiatives and improve their security posture by providing guidance on best handling and securing PII and SPI.

Like many regulations, the GDPR stops short of requiring specific actions but instead positions its recommendations to apply "appropriate technical and organizational measures" to protect data privacy.

Data security

At the core of data protection is securing the data itself. But before you apply protection mechanisms, it's crucial to understand what data you have. Data discovery and inventory is a key first step and includes scanning your entire data estate to understand the types of data you have (sensitive, confidential, or otherwise important). This process requires complete visibility into files and data. Data elements that are important to your organization should be maintained in a data inventory.

Once known, data security and protection mechanisms can be applied appropriately to your data. This includes ensuring that sensitive data is encrypted at rest and in transit so that unauthorized parties cannot see it.

Beyond encryption, appropriate access control is key to protecting data. Only people and applications with a need-to-know should be permitted to view, change, update, or delete sensitive data. This access control should be regularly evaluated, ensuring that overly permissive access is not granted beyond the appropriate amount of time required for that individual or application to do its job.

Data breach notification requirements

Acknowledging that data breaches do occur despite an organization's often best intentions, the GDPR requires the detection of breaches and the timely notification of any data subjects impacted by that breach. Data breaches must be disclosed by affected organizations to the EU Data Protection Authority (DPA) within 72 hours of the breach.

Privacy- and security-by-design principles

While many organizations include a privacy or security check in their system and product design, the GDPR codifies the requirements to include privacy during the initial architecture build-out and changes of systems and processes.

To help inform whether systems are affected by privacy issues, a privacy impact assessment, or PIA, is done. PIAs are required by the GDPR for projects with a high risk to individual privacy, including:

Implementing new data collection systems

Sharing user data with third parties

Processing sensitive personal data (racial origin, health data)

By conducting a PIA, organizations can demonstrate that they've carefully considered the privacy implications of their activities and taken steps to mitigate data security and privacy risks. This is essential for building trust with users and ensuring they are handling personal data responsibly.

Accountability and auditability

Knowing what data you have, who's responsible for it, and how it moves and changes throughout its lifecycle is important for data security and privacy. As humans and machines manipulate data, it can also be changed by malware, encrypted by ransomware, or exfiltrated as part of a data breach. Understanding those changes is key to ensuring that you're able to recover data to a point in time before changes or malicious activity like malware or ransomware.

COMMVAULT CLOUD FOR COMPLIANCE & DATA PROTECTION

Commvault is the gold standard in cyber resilience, leading the charge to protect the world against ransomware and other cyber threats by helping companies reduce risk, minimize downtime, and control costs. It's the only cyber resilience platform built for the hybrid world, offering the best data security for all workloads, anywhere, combined with rapid, enterprise-scale recovery.

Detect threats to your data and anomalies in your environment, earlier

Because Commvault Cloud already backs up your data, we can intelligently detect threats to that data. The Commvault Cloud platform can look for early warnings of suspicious activity using machine learning, analyzing event timelines, and establishing baseline behavior for each machine. By comparing file characteristic changes against established baselines, abnormal behaviors are identified and alerted to. This empowers administrators to take immediate action and mitigate risk.

In addition to looking at individual files for anomalies and changes, Commvault Cloud can help surface attackers by utilizing decoys. These decoys are designed to closely mimic appealing targets—like systems hosting sensitive data—for attackers who may be performing reconnaissance on your environment. They are invisible to legitimate users but incredibly appealing to an attacker.

Once an attacker engages with one of these traps, Commvault can immediately trigger high-fidelity alerts to security teams while preserving the threat actors' interactions for forensic investigation.

This early detection of threats may help minimize or prevent full-scale breaches.

Understand your data and reduce risks to privacy and security

With Commvault Cloud, organizations can effortlessly secure and defend sensitive data across their entire infrastructure. Complete visibility into the data present across your infrastructure is part of Commvault Cloud. As the platform scans and prepares data for backups, it also evaluates it, allowing you to identify and categorize sensitive data and understand risks easily.

Once understood, your security operations teams can implement appropriate security controls to mitigate potential data breaches and privacy issues, all while saving costs through smart, proactive data management strategies. Commvault Cloud Security IQ provides a view into your data protection and data security mechanisms, illustrating which security controls are in place and if any are failing. This allows teams to address security issues proactively before they become incidents.

In addition to looking for sensitive data, unstructured data can also be scanned with Commvault Cloud, which can also proactively identify and quarantine files affected by malware threats. This improves data security and also reduces infection of other data or reinfection of data environments during recovery. Commvault Cloud analyzes backup data to find encrypted or corrupted files so users can quickly recover trusted versions of their data.

Commvault Cloud has the ability to evaluate historical changes to data, as well, meaning that your teams have the auditability needed to understand what changed and when.

Test your plans

Commvault® Cloud Cleanroom™ Recovery provides an affordable, clean, secure, isolated recovery environment on demand for testing cyber recovery plans, conducting secure forensic analysis, and uninterrupted business continuity.

In the event of a data breach, security and IT teams need to make sure trusted data can be recovered and that it's done in a compliant, secure manner. Cyber recovery should include tools that help make sure security and privacy mechanisms remain in place, and that clean data is recovered successfully.

Unlike all other data security offerings with offerings limited to disaster recovery and constrained by a limited set of workloads and recovery options, and unlike traditional isolated recovery environments, which are too expensive to execute regularly and have become increasingly complex to manage for most organizations, only Commvault Cloud Cleanroom Recovery offers the ability to recover workloads from AWS, Azure, GCP, OCI, and on-prem environments, to a safe, on-demand cloud-isolated cleanroom. This comprehensive recovery platform lessens the complexity and cost of using disparate tools and delivers the strongest and most reliable cyber resilience and readiness.

Try Commvault Cloud Today

Commvault Cloud can help your organization achieve better resilience and help comply with several elements of GDPR around data security, privacy, and breaches. Commvault helps bolster your data governance and risk management by automating risk monitoring and providing real-time anomaly and threat detection. Incident management can be streamlined with cyber recovery planning. And now, you can use cleanroom technology to test and execute your data security, compliance, and resilience strategies in an efficient, proactive, and cost-effective way.

GET A LIVE DEMO OF COMMVAULT CLOUD TODAY.

Live demo →

To learn more, visit **commvault.com**