Get Prepared for GDPR Compliance

Checklist

On May 25, 2018, the General Data Protection Regulation (GDPR) goes into effect, applying to all companies processing and holding personal data of EU residents, regardless of the company's location. Companies that fail to comply face potential fines of up to €20 million or 4 percent of annual global turnover.

GDPR is a multifaceted set of regulations, and no single platform will ensure compliance. But as you evaluate data management solutions, consider these key steps to accelerate the process towards compliance:

Determine how GDPR compliance impacts your organization and its business goals, budget, and resources.

Many companies manage data that is fragmented across different locations on-premises and in the cloud. Selecting a single solution to manage data across all your environments is cost effecient, simplifies data protection, and diminishes learning curves.

Identify sources of personal data and where they are stored.

Also define the use cases for gathering your data and when this data should be deleted. These steps help determine compliant retention and deletion policies. Set automation policies for data storage, retention, archival, and access.

Assess the risk of your current processes and systems.

Evaluate how a solution complies with changes such as customer consent, data portability, access rights, and data erasure. GDPR requires companies to implement measures that ensure an appropriate level of security, including quick data recovery. A platform that delivers near-zero RTO and immutable snapshots can help comply with these criteria.

Test and evaluate your security measures.

Regularly testing your disaster recovery plan helps ensure that you are delivering the appropriate level of recoverability. However, disaster recovery or test/dev workloads should not impact your production workloads.

Manage your data across all locations, whether on-premises or in the cloud.

Simplify this process with a single solution that can manage virtual and physical workloads across your entire infrastructure. GDPR requires that companies understand where data stored in the cloud is located and how compliance is

being met. Select a solution that provides customizable reporting and insight into what data is stored in the cloud and where it resides. Use an API-first architecture to further automate workflows with third-party tools.

Secure your data against breaches and losses.

GDPR requires that data protection is designed and developed into products from the beginning. A strong solution delivers end-to-end data encryption, and data sent to the cloud is encrypted both in-transit and at-rest. It also enables quick recovery from a disaster without any data loss.

Protect against employee-caused security breaches.

GDPR also covers security breaches caused by employees. Leverage Role-Based Access Control (RBAC) to limit data access to only those who need it.

Monitor and report your data compliance.

Deliver proactive monitoring that promptly notifies you of any failures. Set a process for notifying authorities of breaches and responding to individual requests on deleting or editing personal data.