COHESITY

Ensuring GDPR Compliance with Cohesity

GDPR and Data Storage

The EU General Data Protection Regulation (GDPR) is a regulation designed to strengthen data protection for residents of the EU. GDPR will become effective on May 25th, 2018, and applies to any company controlling or processing personal data of EU residents, regardless of the location of the company.

GDPR imposes a broad set of legal, governance and technical requirements on companies processing personal data. A subset of these requirements – those related to data protection and data management – are particularly relevant for storage platforms used to store personal data. They include:

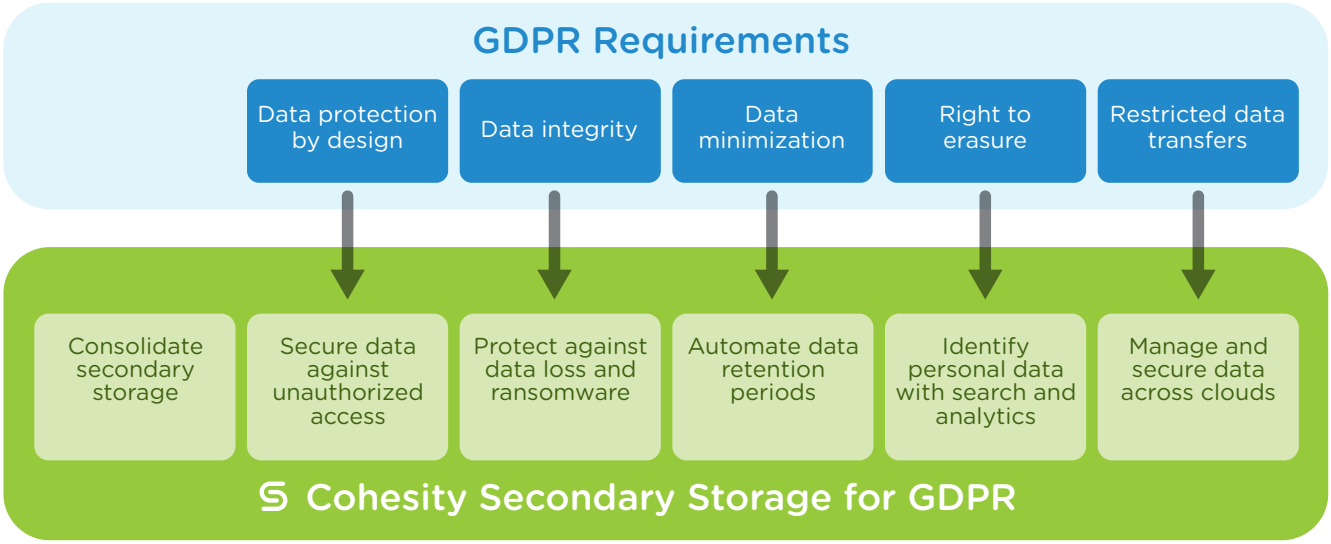
- **Data protection by design:** Personal data must be secured against unauthorized or unlawful access. Companies should encrypt the data and restrict access to the entities processing the data.
- **Data integrity:** Personal data must be protected against accidental loss, destruction or damage, including ransomware.
- **Data minimization:** Companies should minimize the personal data they store, and only keep the minimum set of data required for processing purposes. Data should be deleted once the use case for processing concludes.
- **Right to erasure / right to be forgotten:** Data subjects have the right to request the erasure of their personal data from the company's systems.
- **Restricted data transfers:** Transfers of personal data to "third countries" must be restricted to countries and organizations that offer an adequate level of protection. Data transferred to other countries or locations – such as a public cloud – must continue to meet GDPR requirements for data protection.

Cohesity Simplifies GDPR Compliance

Legacy secondary storage consists of a patchwork of point appliances that make GDPR compliance difficult to achieve. Data is copied across silos (for backups, archive, test/dev, and analytics) and must be protected and managed multiple times across silos using a variety of point solutions. If any single one of these silos is non-compliant, the whole organization could be liable for significant penalties.

Cohesity provides a better storage platform for achieving GDPR compliance. Cohesity is a web-scale platform designed to consolidate all secondary data. Cohesity consolidates data protection, files, objects, test/dev, analytics, and cloud gateway in one unified solution. And Cohesity provides simple data protection, encryption, data retention, search, analytics, and many other capabilities to facilitate GDPR compliance. With Cohesity – there's just one secondary storage platform to keep compliant, and compliance is easier to achieve.

COHESITY



Cohesity simplifies GDPR compliance with the following capabilities:

- **Consolidate secondary storage:** Cohesity consolidates target storage, backup software, files, objects, test/dev copies, and analytics data on one web-scale platform. By consolidating secondary storage, companies don't copy data multiple times across point appliances. Cohesity minimizes data copies, reduces attack footprint, and centralizes data management on one platform – thereby simplifying GDPR compliance. Data governance, security, search and analytics become a lot simpler when done on a single platform.

- **Secure data against unauthorized access:** Cohesity provides software-based encryption of data at-rest and in-flight. Under GDPR rules, encrypting data and storing the keys in a separate location is considered equivalent to pseudonymization of personal data. Cohesity provides full support for pseudonymization using encryption keys. In addition, fine-grained Role-Based Access Control (RBAC) ensures that only authorized users have access to the data.

- **Protect against data loss and ransomware:** Cohesity provides erasure coding and replication to ensure data resiliency within a cluster. Data is protected in immutable, automated snapshots to protect against data loss and ransomware. Data can also be replicated and archived to tape or cloud to provide off-site data protection.

- **Automate data retention periods:** To comply with data minimization requirements, Cohesity enables backup administrators to specify data retention periods with automated policies. Data can be automatically retained and deleted or expired based on these policies.

- **Identify personal data with search and analytics:** Under GDPR, individuals have the right to request the erasure of their personal data from the company's systems. In these situations, companies first have to identify all instances of that personal data across secondary storage. Cohesity indexes all file and VM metadata upon ingestion in the system, enabling global Google-like search to quickly identify individual files. Cohesity also enables in-place custom analytics to quickly identify sensitive and Personally Identifiable Data across an entire cluster. Cohesity also allows for integration with 3rd party analytics, compliance and eDiscovery products. Finally, customers can use Cohesity to replace tape with public cloud or any NFS and S3 compatible storage, making archives much more searchable and manageable.

- **Manage and secure data across multicloud environments:** Many customers are using or plan to use the public cloud for data storage. Yet GDPR restricts the list of locations and providers to which personal data may be sent. Cohesity enables users to replicate data across clusters and to the cloud, and archive data to the cloud or any NFS and S3 compatible storage. Cohesity provides simple control of data location across multicloud environments. And the data in the cloud can be encrypted, indexed and analyzed to enable GDPR compliance regardless of location.

COHESITY

Cohesity Technical Features That Support GDPR

How Cohesity Simplifies GDPR Compliance	Cohesity Technical Features and Capabilities
Consolidate secondary storage	• Web-scale platform with unlimited scalability • Consolidate all secondary storage on one platform o Data protection for Virtual Machines, physical servers, Microsoft SQL Server, Oracle databases, NAS devices, and Pure Storage o Storage for database dumps and copies o Storage for 3rd party backup products o Files (NFS and SMB) o Objects (S3 compatible) o Test/dev copies • Replace tape with cloud or any NFS / S3 compatible storage to increase manageability o Index and search archive data o Recover individual files from archive o Selectively delete archive data
Secure data against unauthorized access	• Encryption o Data at-rest and in-flight (cloud, replication) o Software-based, AES 256 o FIPS-compliant o Encryption keys managed by Cohesity cluster or external KMS • Role-Based Access Control o Permissions by type of user o Permissions by data source o AD integration • Data isolation o Physical isolation between partitions o Logical isolation between View Boxes
Protect against data loss and ransomware	• Data resiliency within cluster o Erasure coding o Replication • Data protection within cluster o Automated, immutable snapshots of backup jobs and Cohesity volumes o Instant restore to any prior snapshot • Off-site data protection o Cloud archival and replication o Cross-cluster replication • Write-Once Read-Many (WORM) volumes for sensitive data
Automate data retention periods	• Data retention policies to minimize personal data storage o Define policies with data retention and deletion periods o Assign policies to specific types of data o Automate data deletion based on policies

COHESITY

How Cohesity Simplifies GDPR Compliance	Cohesity Technical Features and Capabilities
Identify personal data with search and analytics	• Global search o Index all VM and file data on the system o Enable global, Google-like search across an entire cluster • Custom analytics to identify Personally Identifiable Information o Run custom analytics jobs using Analytics WorkBench (AWB) o Inject custom code or use predefined analytics jobs o Quickly locate personal data • Integrate with 3rd party analytics, compliance and eDiscovery products o Provide access to Cohesity volumes and buckets o Enable in-place analytics via Analytics WorkBench
Manage and secure data across multicloud environments	• Send data to any location o Replicate to the cloud or to another Cohesity cluster o Archive to the cloud or to any NFS / S3 compatible storage o Control data location for any backup job or volume • Secure data across locations o Encrypt data in-flight for replication and archival o Encrypt data at-rest in replication and archival targets • Manage data across locations o Index, search and analyze data regardless of location o Enable simple access, deletion and transfer of personal data across locations

Cohesity, Inc.
Address 451 El Camino Real, Santa Clara, CA 95050
Email contact@cohesity.com www.cohesity.com
@cohesity