PANZURA

SOLUTION BRIEF

GDPR Compliance and Self-Reporting

How the CloudFS hybrid cloud file platform can assist organizations with GDPR compliance.

As the cumulative total amount of General Data Protection Regulation (GDPR) fines levied approaches €5 billion as of the end of 2024, it's clear that keeping data compliant with one of world's toughest data protection laws presents a significant challenge.

Panzura's unique approach to data management offers data privacy and security by design. Our hybrid cloud file services platform CloudFS and data intelligence layer Data Services allow organizations to keep data secure and protected, securely delete it when necessary, track data access and movement, and prove GDPR compliance when required.

This document should be read in conjunction with the technical whitepapers for both Panzura CloudFS and Data Services, for a full understanding of their capabilities. These can be downloaded from panzura.com/resources.

Data Consolidation and Location

Core to any organization's ability to manage and protect data is to know exactly where that data resides. For organizations operating localized data storage across multiple locations, simply finding all copies of relevant data is complex and time-consuming. Multiple similar — if not identical — copies of files sit in data silos across the organization. Exponentially more copies are made using traditional backup processes, plus offsite replication for redundancy.

This legacy approach to backup at each location makes yet another copy, which is retained per the organization's data retention policy. The result is multiple copies of individual files across the organization. This immeasurably complicates any requirement to identify, supply, prove compliance for or delete any piece of personal information.

Using the public or private cloud object storage of the organization's choice, CloudFS consolidates data into a single, authoritative data source that is de-duplicated, compressed and encrypted. Critically, this process simplifies data management, minimizes the storage footprint and ensures data integrity for the organization by removing redundant data.

CloudFS then allows secure, performant access to this authoritative data set to authorized users, from any location in an organization's network. CloudFS uniquely delivers real time global data consistency, ensuring that every authorized user sees the latest version of any file, without waiting for data to propagate between locations and without making copies.

Global organizations can restrict access to authorized users by geographic location by mapping specific drives within the global file system, and granting access as appropriate.

Data Access and Authentication

CloudFS integrates with Microsoft Active Directory services to allow only authorized data access for connected users for SMB. NFS exports based on host name(s), IP addresses, network, Netgroups and Kerberose integration are also supported for user authentication.

Data Protection

CloudFS guards against any data loss, damage or destruction by storing it in an immutable Write Once, Read Many (WORM) format and further protecting it with immutable snapshots. With CloudFS, once data is in the object store, it cannot be changed, overwritten, or damaged in any way. File changes are written as new data blocks, which have no effect on existing data. As new data is saved, CloudFS updates metadata file pointers to record which data blocks comprise a file at any given time.

Panzura's lightweight, immutable snapshots then provide a granular, point-in-time ability to recover any data, by restoring from the applicable snapshot. Individual files, folders, or even the entire file system can be restored in this way.

For early threat detection and defense, CloudFS integrates with Varonis as well as supported ICAP anti-virus and malware scanning providers. Additionally, Panzura Detect and Rescue further extends the protective capabilities of the platform by detecting ransomware attacks in near real time and interdicting them — stopping them in their tracks — at the user level.

Ransomware Protection

Because both the snapshots and the data itself are immutable, ransomware attacks do not damage files in CloudFS. Instead, attacks are shrugged off by quickly reverting back to previous data blocks, to make up uninfected files.

Data Availability

CloudFS is engineered for swift recovery in the event of any disaster, ensuring that data is available whenever it needs to be.

Firstly, data is protected through the high durability of the cloud. Public cloud storage providers typically offer durability of up to 16 9s, with geographic redundancy included in their service. CloudFS offers high availability with auto-failover, allowing for redundancy at all locations. Should an office location become unavailable, a CloudFS node can be deployed in any nearby cloud region, allowing performant access to authorized users from anywhere.

While cloud storage outages are infrequent, they are extremely disruptive. CloudFS uniquely allows organizations to mirror data across two object stores, reading from and writing to the primary store, while also writing to the secondary store in real time. In the event of an outage, CloudFS will failover to the secondary store, reading from and writing to it while the primary store is unavailable. This allows business operations to continue uninterrupted. Once the outage is resolved, CloudFS will sync new and changed data as operations switch back to the primary store.

Data Encryption and Privacy

The CloudFS solution is FIPS 140-3 certified. This international security standard covers cryptographic modules for the protection of data and certification is granted only after rigorous testing in conjunction with the National Institute of Standards and Technology (NIST). To guard against data breaches, military-grade AES-256-CBC encryption is used to encrypt data stored at the edge and in the cloud. Transport

layer security (TLS/SSL) encryption technology securely transmits data over the network between local nodes and the cloud.

Panzura CloudFS supports Key Management Interoperability Protocol (KMIP) servers for managing encryption certificates. This approach allows organizations to create encryption certificates that align with their specific security policies. Encryption keys are managed by the organization. These are never stored in the cloud, leaving cloud providers unable to read data in CloudFS.

Panzura further protects data using encryption technology to mask data stored in CloudFS, including directory names, file names, and file data. This obfuscation replaces randomly chosen characters with randomly chosen data — effectively making data unreadable in the event that it is intercepted.

In addition to encryption, Panzura chunks files, deduplicates them, and compresses the results before sending the data to the cloud. Collectively, these actions ensure that if someone unauthorized were able to access production data in the object store, they would only see incomprehensible strings of characters.

Right to be Forgotten and Secure Erase

CloudFS Secure Erase makes it possible to delete a file or folder from the global file system — from the edge, to the cloud store, to the snapshots that contain archive copies — so that the contents cannot be restored, even using the most advanced technology available. Secure Erase is the highest purge level that can be attained without physically destroying the disk drives.

Data Auditability and Record Keeping

CloudFS logs each and every action taken on every file within the platform. This comprehensive logging provides a complete view of user actions taken on within CloudFS. These logs can be used in conjunction with Panzura Data Services, as well as third-party data intelligence options such as Splunk to track and alert on unauthorized user access, or data movement between mapped drives.

Proving Compliance and Self-Reporting

Used in conjunction with Panzura Data Services, Splunk or another third-party data intelligence provider, organizations can monitor and track activities that run the risk of infringing upon GDPR rules, such as data spillage from one geographic region to another.

Proving early detection and demonstrating that spilled data has not been incorrectly accessed or used can help organizations to avoid the otherwise inevitable fines.