panzura

GDPR Compliance with Panzura CloudFS

Helping companies achieve their GDPR compliance with Panzura Freedom NAS, an enterprise hybrid cloud NAS

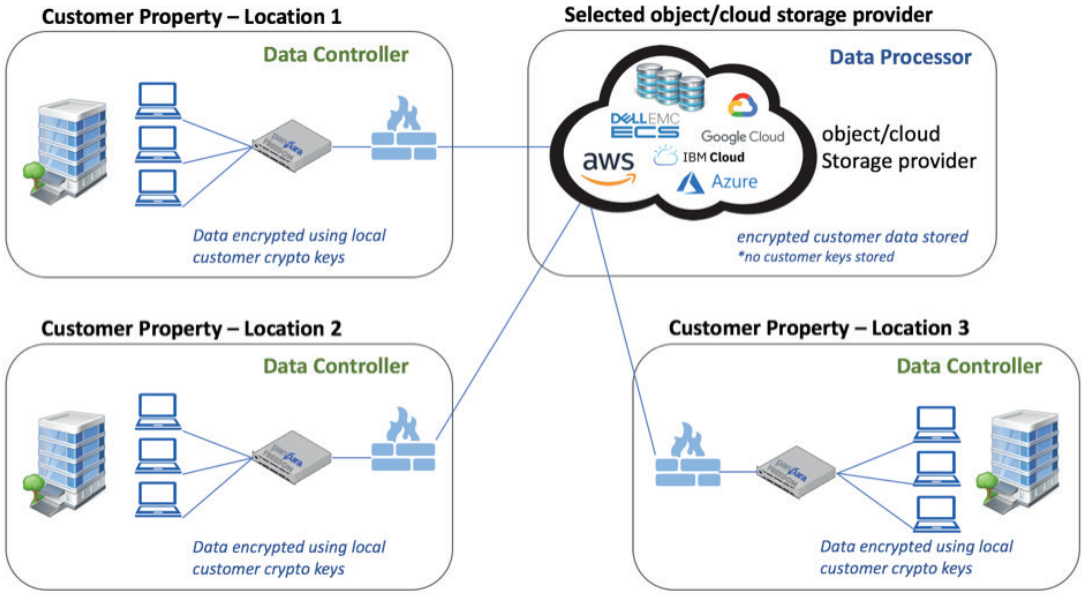
The General Data Protection Regulation (GDPR) is the new framework in the European Union ("EU") for data protection laws governing the protection of the personal and sensitive information of individual EU residents ("Personal Data"). The GDPR became effective on May 25, 2018. The GDPR applies to companies located in the EU, companies located outside of the EU which collect or process Personal Data for purposes, such as, offering goods and services or monitoring and tracking behavior of EU residents and companies within or outside of the EU which process and hold Personal Data.

The GDPR affords greater protection, accountability and visibility to individual EU residents as to the collection, use, disclosure, storage and destruction of their Personal Data and, subject to certain exceptions, grants such individuals the rights, such as the right of access to and to copy their Personal Data, the right to ask Personal Data be deleted, moved or corrected.

Panzura Freedom NAS™ is an intelligent hybrid cloud storage systems underpinned by Panzura CloudFS™, the first enterprise file system purpose built for the cloud. The enterprise class security features of CloudFS help companies meet their obligations to comply with GDPR in multiple ways.

REQUIREMENT	HOW PANZURA HELPS ACHIEVE COMPLIANCE
Personal right to be forgotten	Complying with the personal right to be forgotten or delete data in the cloud can be challenging. Panzura offers a Secure Delete feature that allows its customers to delete and wipe data from the edge all the way through to the cloud storage solution (public or private) by wiping not only metadata but data blocks stored encrypted in the cloud storage solution.
Data Encryption and Confidentiality	All data stored on the Panzura Freedom filer solution is fully protected with AES-256-bit encryption using customer supplied crypto keys which are never stored in the cloud/object storage. KMIP key management solutions are supported to seamlessly plug-in to existing customer environments. All data stored in the cloud is encrypted at rest. All communications are fully encrypted using TLS 1.2 SSL sessions both for managing the Panzura filer as well as any transport to and from the cloud. This ensures that the contracted cloud storage provider has no access to any of the data itself.
Data Privacy	Panzura does not resell, store or process any customer data itself. All data is under the control of the customer either directly or through its own contracted cloud/object storage provider. To further protect its customers, Panzura encrypts all data both in transit and at rest in that cloud/object storage using crypto keys provided and controlled by the customer. No crypto keys exist in the cloud to ensure that the cloud/object storage provider itself doesn't have access and cannot read or process that data.
Access & Authorization control	Panzura integrates with existing Microsoft Active Directory (AD) services to authenticate and authorize 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	Panzura takes advantage of the durability provided by object storage achieving up to 16 9s of durability with some providers. Multiple copies of your data is stored in the cloud (public or private) across multiple availability zones or even regions for redundancy. Panzura snapshot technology makes it possible to restore data to any point in time according to the established retention policy. Additionally, Panzura has implemented an immutable data architecture which provides for protection against ransomware or crypto-locker virus attacks further supplemented with ICAP support for inline virus scanning.
Record of Processing Activities	Panzura provides full file audit logging so that customers can track who created, accessed, modified or deleted what data when. File audit log information is maintained locally on the Panzura filers with options to integrate with 3rd party file audit policy solutions.
Data Availability	Panzura filers write all data to the cloud/object storage platform as soon as it is written locally making that data available to all configured filers in the configured CloudFS (cooperative mesh of filers in a global namespace). Data can be retrieved from any filer in the CloudFS in the case of a single or even multiple filer failure. Additionally Panzura offers both local standby filers that can take over services of a failed filer as well as global standby filers that can take over for remote filer failures if required. Any filer can be completely restored from the cloud in case of a disaster.
Data Integrity	All data written to the Panzura filer is validated with MD5 checksums both locally and to the cloud/object data storage platform. An MD5 checksum is calculated and then compared against an independent MD5 checksum calculated upon confirmation of any cloud write or read request.



Panzura, Inc. | 695 Campbell Technology Pkwy #225, Campbell, CA, USA | 855-PANZURA | www.panzura.com