A LEONOVUS WHITE PAPER

GDPR compliant cloud storage: made possible

GDPR - The General Data Protection Regulation (EU) 2016/679, a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).

INTRODUCTION

GDPR came into effect in May 2018 and is now the gold standard for privacy regulations worldwide. Businesses collecting data from - or on - EU users (data subjects) are required to comply with rules that include:

- Creating processes with user data protection at its foundation;
- ensuring consumers' rights to be informed about the collection and use of their personal data;
- giving individuals the ability to access and to rectify, erase, port or restrict the processing of their personal data;
- notifying the proper authorities about personal data breaches within 72 hours of their occurrence.

A business (data controller) is required to know precisely what PII (Personally identifiable information) they have, where it's stored, how long it needs to be stored, and whether it has been breached. The regulation also covers data processors – like AWS, Google Cloud and Azure – for cloud storage compliance and several other aspects.

This paper will examine four areas of the GDPR that every organization with data in public cloud needs to address.

CONTENTS:

GDPR data governance and privacy will help your business

The European Commission states that "New rules should boost consumer confidence and in turn business." Furthermore, GDPR data governance and privacy regulations have inspired similar regulations in other markets. For instance, the California Consumer Privacy act goes live on Jan 1st, 2020 and it has considerable overlap with GDPR.

Privacy regulations require you to have well-defined and well-implemented data protection and data management strategies. GDPR – or similar upcoming regulations – are an opportunity for your business to project how much you value and how well you protect the privacy of your customers and employees.

> "Having the right mindset towards data protection helps to future proof a business. It will put it in the right place to keep up with legislation."
>
> Information Commissioner's office, UK

What does it take to comply with GDPR regulations?

Among other things, GDPR requires you to have a documented and verifiable implementation of:

- **Data governance** through audit-ready operations logs
- **Storage and retention** rules that are data-centric and region-restricted
- **Access control** to eliminate unauthorized or inadvertent loss, modification or movement of data
- **Response mechanism** to data subjects and manage their requests like exercising their "right to be forgotten"
- **Breach notification** mechanism to notify authorities and users

It's worth reiterating that these policies relate to a specific type of data – the PII of an individual. Therefore, all policies, procedures, and services need to be able to identify the PII, know its location and be able to manage this information as requested by a data subject. You also need to – by design and agreements – set-up IT resources including cloud storage to comply with GDPR regulations.

How Leonovus can help in this GDPR cloud compliance journey

IT organizations are striving to meet the "cloud-first" strategic imperative and regulations can be a barrier. If you are building a hybrid or multi-cloud storage ecosystem, you will need a strategy for GDPR compliant cloud storage.

GDPR mandates that you deliver "Data protection by design and by default," i.e., all your services should be sensitive to the type of data you are collecting from - or about - a data subject. Article 5, for instance, points to the wide-ranging principles of managing personal data.

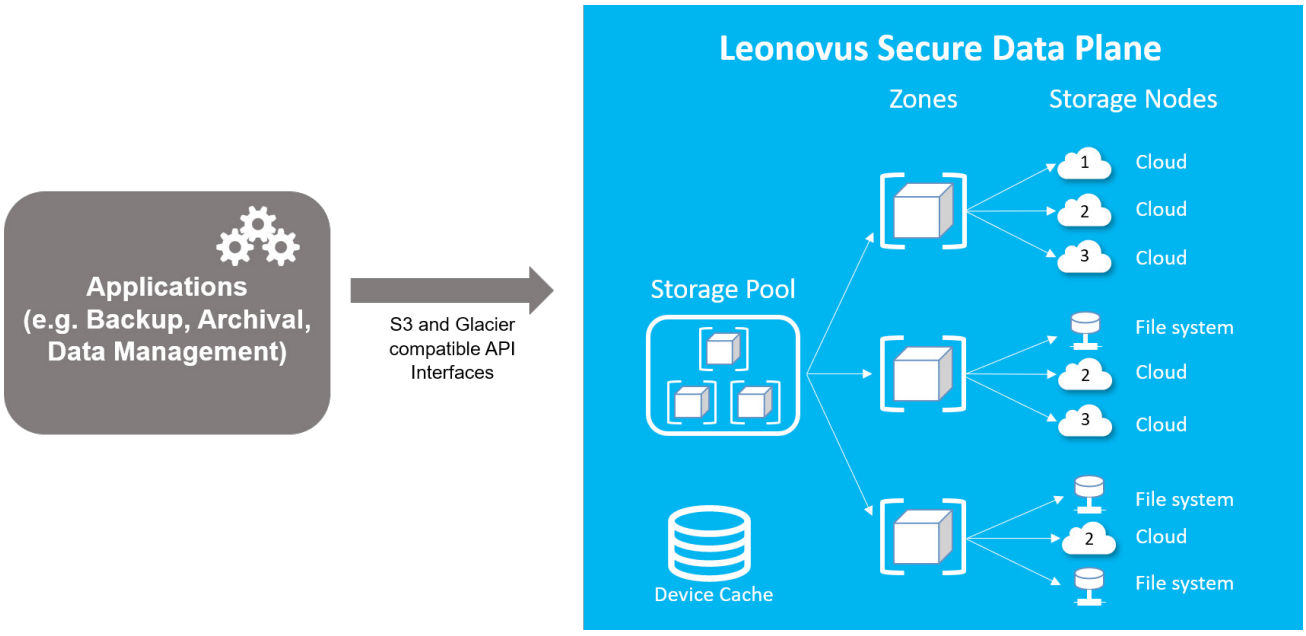
Leonovus' lets you consistently apply data-centric policy and greatly aids personal data management. You apply all policies through a single pane of glass - in hybrid and multi-cloud environments - and Leonovus is your unified storage target for all data sources. The resulting "last line of defense" can protect against malicious or unintended loss and movement of data.

Let's look at four areas in GDPR that can use some help:

Data sovereignty

Relevant GDPR articles: Article 46

Leonovus enables your business to create a definite connection between data sources and storage destinations. Our model helps organize storage resources in a hierarchical structure through Zones and Pools. Zones are typically used as a logical grouping of public and private storage in a specific region. Pools, comparatively, are upstream and bring together multiple zones. Data placement and data movement obligations under GDPR Article 46(1) discourage moving data outside the EU. Location-restricted Zones and application-specific Pools will help you geo-fence your data and still benefit from Leonovus' unique ability to spread discrete data fragments across your storage nodes in the EU. Leonovus enables you to avoid investing in hardware/software for geo-fencing your data.



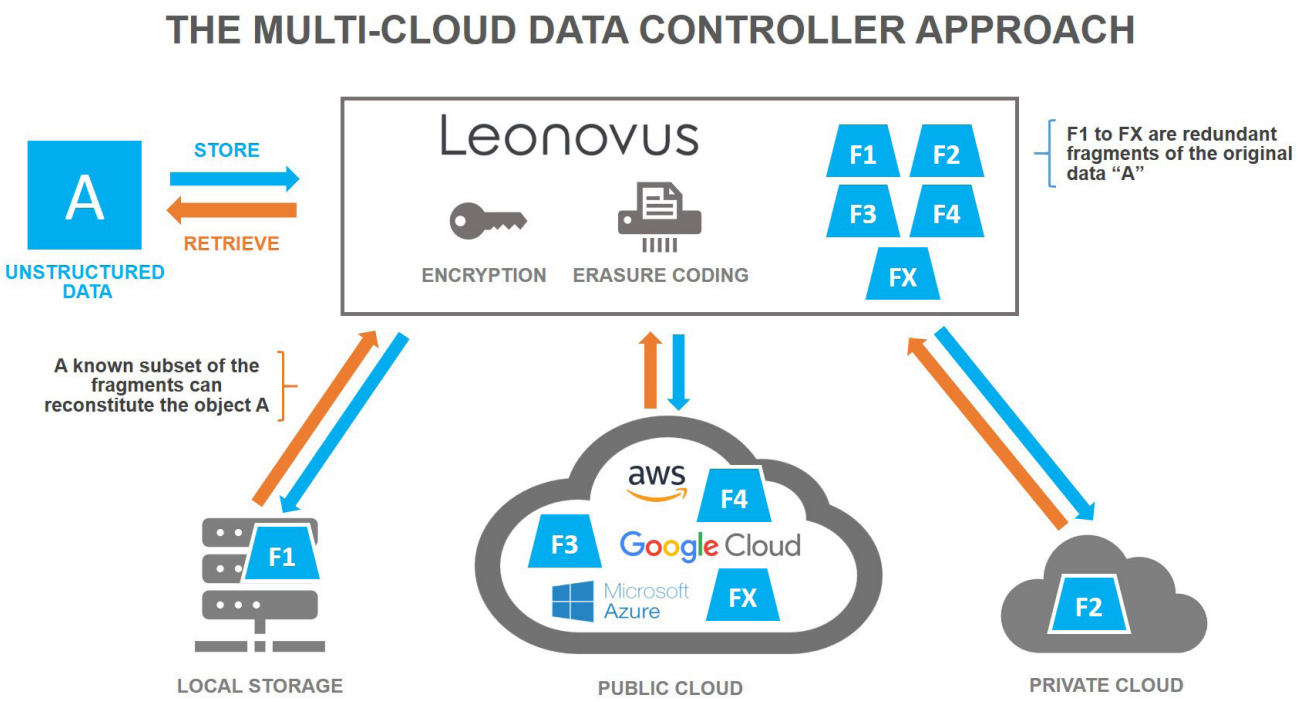
Data security and recoverability

Relevant GDPR articles: Article 5, Article 25, Article 32, Article 33

Leonovus employs AES-256 encryption for data-at-rest, TLS 1.2 for data-in-flight and SHA-256 for data integrity. In addition, by using erasure coding, Leonovus helps you meet the data security requirements of Art.5(1)(f) that states "personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."

Your IT architecture goals of "pseudonymization" and "data minimization" - under Art. 25(1) and Art. 32(1)(a,b,c), - will be aided by Leonovus' ability to encrypt, shred and spread data across multiple storage nodes. Our deployment of erasure coding not only provides RAID 5/6 equivalent data resilience but also optimizes the size and, consequently, minimizes the threat surface of your data.

Your security posture and data-resilience are now enhanced not only by encryption but also by storing data fragments across nodes of your choice. The combination of encryption and fragmentation render unusable any data lost to hackers or bad actors, and you can swiftly meet your "measures to mitigate" obligations under Art 33(3)(d).



Access control

Relevant GDPR articles: Article 25, Article 32

Regulating access to personal data is a crucial tenet of GDPR. With Leonovus, you get role-based access control (RBAC) that lets you decide which users and applications get access to specific Pools of data. RBAC helps meet the goals of Art. 25(2) and Art. 32(4) around authorized access.

Furthermore, to prevent "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed" as stated in Art. 32 (2), Leonovus can apply WORM locks on data buckets, keep detailed history on all data access and ensure the integrity of data for all data that transits through the software.

Audit reporting

Relevant GDPR articles: Article 24, Article 30, Article 17

The data controller, i.e., the business that holds personal data is responsible under Art. 24(1) to demonstrate compliance. Your compliance with Art. 24(1) relies – in part - on your ability to record and report all events related to personal data of data subjects.
Leonovus' aids your compliance needs by keeping a detailed history of all access to data. For example, it can capture your compliant action on a data subject's request under Art. 17(1),17(2) (right to be forgotten)

Also, Leonovus Object Explorer allows you to view the exact disposition of not only complete files stored by it but also all resulting fragments. This information helps you meet a variety of reporting obligations under GDPR.

Finally, Leonovus solves the problem of extending audit-related information securely under Art. 30(4) by keeping a detailed audit log for all access to data. This log can be made available to authorities as necessary.

"However fast regulation moves, technology moves faster. Especially as far as data is concerned."

Information Commissioner's office, UK

CONCLUSION

With 99 clauses in the regulation, no one vendor, or platform can be a silver bullet for GDPR compliance. GDPR is multi-faceted and requires you to build processes, designate key personnel, and deploy all means and technologies necessary to protect citizen data.

As you strive to meet – or prepare for – the "cloud-first" strategic imperative, you will need a strategy for GDPR compliant cloud storage. Leonovus helps address four key areas for GDPR compliance for cloud storage:

- **Data sovereignty** – Geo-fence data through Zones and Pools
- **Data security and recoverability** – Enterprise-managed keys, encryption, and erasure coding
- **Access control** – Leverage RBAC, WORM locks and detailed history of data access
- **Audit reporting** – Maintain detailed audit logs on all data access across your distributed storage architecture

Leonovus will help you create a sustainable and non-disruptive solution for your GDPR requirements. With a lowered barrier to enter or operate in the EU and EEA region, you can better focus on delivering value to your users, employees, and customers.

Additional resources:

Whitepaper: Solving the enterprise data storage problem

Whitepaper: Secure Multi-Cloud Storage for Highly Regulated Industries

Video: How Leonovus Works

Follow us on: LinkedIn | Twitter | Facebook
LinkedIn: linkedin.com/company/leonovus-inc./
Twitter: @leonovusInc