The Strategic Necessity of Sovereign Object Storage

Value Creation for MSPs and Their Customers in Europe



Table of Contents

1. Introduction: The Rise of Sovereign Cloud Solutions in Europe
2. What is Sovereign Object Storage?
3. Key Drivers for Sovereign Object Storage in Europe
    - Geopolitical Tensions and Dependence on Hyperscalers
    - Regulations and Compliance (GDPR, CLOUD Act)
    - Enhanced Security and Data Control
4. Pain points for MSPs and their customers in today's cloud landscape
    - Costs and Vendor Lock-in
    - Ransomware and Data Loss
    - Compliance with More Complex Regulations
    - Lack of Control and Transparency
    - Gaps in the European Cloud Market
5. The added value of Sovereign Object Storage for MSPs and solutions for their customers
    - Compliance as a Service
    - Cost Efficiency and Transparency
    - Enhanced Security and Cyber Resilience
    - Strategic Independence and Customer Trust
    - Seamless Integration and Scalability
    - Opportunity for differentiation in the market
6. Conclusion

1. Introduction: The Rise of Sovereign Cloud Solutions in Europe

In today's digital age, data is the lifeblood of businesses. From customer information to sensitive financial data, the data that companies process on a daily basis must be protected and managed with the utmost care. This need for strict data protection has led to the concept of the Sovereign Cloud, a solution that has received considerable attention, particularly in the context of European and national legislation. Europe is making a strong move towards implementing sovereign cloud solutions, driven by concerns about data sovereignty, privacy, and geopolitical tensions.

2. What is Sovereign Object Storage?

Sovereign object storage refers to a cloud computing environment where data is stored, managed, and processed within the borders of a specific country or region, in accordance with local legal and regulatory frameworks. In the Belgian context, for example, this means that all data is stored and managed on Belgian soil and in Belgian data centers. This concept is essential for organizations that process confidential data, as cloud computing, often based in the US or China, can subject valuable data to less protective and more intrusive laws.

Object storage is a data storage architecture in which data is stored and managed as independent units called objects. Each object contains a key, the data itself, and optional metadata. This API-friendly and highly scalable form of storage is the preferred format for public cloud storage services such as Amazon S3. Objects function as modular units, complete with metadata that describes details such as permissions, privacy, and security. The main advantages are virtually unlimited scalability, on-demand payment for storage capacity, metadata-driven data analysis, API support, and improved data integrity through erasure coding.

3. Key Drivers for Sovereign Object Storage in Europe

The demand for sovereign object storage in Europe is driven by several fundamental factors:

- Geopolitical Tensions and Dependence on Hyperscalers The dominance of American tech giants such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, which control more than 60% of the global cloud market, has led to significant concerns among European policymakers and businesses. The changing geopolitical landscape, including international tensions, reinforces the need for an independent European cloud infrastructure that supports data sovereignty. For example, the Dutch parliament voted overwhelmingly to reduce dependence on US technology companies, creating opportunities for local businesses and strengthening data sovereignty. Europe still lags far behind in the global cloud market, with a collective market share of less than 10% for EU Cloud Service Providers (CSPs) and more than 90% of shared data outside EU jurisdiction.

- Regulations and Compliance (GDPR, CLOUD Act) The General Data Protection Regulation (GDPR) is one of the strictest data protection laws in the world, requiring a high degree of care and transparency in the processing of personal data. Data stored within Belgium (and by extension Europe) is protected by Belgian law and the GDPR. Failure to comply with local data protection laws can result in legal fines and loss of customer trust. There is also growing concern that the US CLOUD Act could be abused. If data is stored in Belgian data centers, foreign governments cannot access it under their own legal systems, such as the CLOUD Act or Patriot Act. European cloud providers report that customers cite the CLOUD Act as a major reason for switching from US companies.
- Improved Security and Data Control Digital sovereignty is about maintaining control over data and digital infrastructures within one's own country and organization. This is crucial for organizations that process confidential data. Sovereign cloud solutions implement cloud infrastructure that meets specific geographic and legal requirements to ensure data residency and compliance with local regulations. European data centers, such as DC Antwerp, comply with strict security standards and certifications such as ISO 27001:2022, and DC Antwerp is even the first and only one in Belgium with a Tier IV certification from the Uptime Institute, which guarantees the highest level of security. This provides an extra layer of protection for data and gives companies complete control over how their data is managed and who has access to it.

4. Pain points for MSPs and their customers in today's cloud landscape

Despite the advantages of cloud storage, MSPs and their customers face various challenges, especially when they depend on non-European hyperscalers:

- Costs and vendor lock-in Traditional hyperscalers often charge hidden costs, such as egress fees (costs for retrieving data) and API requests. These costs can be crippling and sometimes feel like ransom. This makes it difficult to test backups and restore data without unexpected expenses. Customers are confronted with complex pricing models and vendor lock-in, which hinders flexibility.
- Ransomware and data loss Ransomware attacks are a constant and growing threat. Backups are often a favorite target of cybercriminals, as encrypting both primary systems and backups increases the pressure to pay ransom. Without a robust defense and recovery strategy, companies can be minutes away from total business shutdown. Accidental data deletion is also a risk.
- Compliance with more complex regulations Navigating the complexity of international data laws and regulations, particularly when data crosses borders, is a significant challenge. Companies struggle to comply with local laws and avoid the legal complexities and risks associated with transferring data to countries outside the EU with less stringent laws.
- Lack of control and transparency Customers are concerned about where their personal information is stored and managed. Dependence on foreign cloud providers can lead to a feeling of loss of control over sensitive data and digital infrastructures, particularly due to the threat of foreign legislation such as the CLOUD Act.
- Gaps in the European cloud market Despite significant investments in the Digital Decade Program, Europe is lagging far behind. There is a critical gap in the European cloud market, leaving companies without a comprehensive, sovereign, and competitive solution.

Individual European Cloud Service Providers (CSPs) often struggle with insufficient scale and limited service portfolios, while European initiatives focus primarily on enforcing compliance but fail to deliver concrete commercial offerings.

5. The added value of Sovereign Object Storage for MSPs and solutions for their customers

Sovereign object storage offers MSPs a unique opportunity to address these pain points and provide added value to their customers:

- Compliance as a Service MSPs can reassure their customers that their data is stored and managed in accordance with Belgian and EU regulations, in particular the GDPR. European cloud providers such as Impossible Cloud's infrastructure is rooted in European data centers and ensures compliance with regulations such as GDPR, ISO 27001, PCI DSS, and SOC 2. By partnering with certified data centers, such as DC Antwerp (ISO 27001:2022, Tier IV certified), MSPs can offer "compliance-as-a-service" that eliminates legal complexity and risk.
- Cost efficiency and transparency Sovereign cloud solutions often offer a transparent pricing model with no hidden costs such as egress fees or API requests. This enables MSPs to offer their customers significant cost savings, sometimes up to 80% on cloud storage costs. This predictable and fair pricing model increases profitability for MSPs and offers customers greater budget certainty, which also encourages backup testing.
- Enhanced security and cyber resilience European cloud solutions implement rigorous security protocols, including encryption of data in transit and at rest, strict authentication controls (IAM, MFA, SSO), and multi-level encryption. A crucial aspect is immutable storage (Object Lock), which protects data from ransomware and accidental deletion. Immutable storage creates a "logical air gap" through encryption and hashing, making data unchangeable, even for system administrators, for a set retention period. This means that in the event of a ransomware attack, companies can recover data quickly and affordably without having to pay a ransom.
- Strategic independence and customer trust By offering European sovereign solutions, MSPs contribute to the EU's strategic goal of achieving digital sovereignty and strengthen the infrastructure of European technological innovation. This enables companies to maintain control over their data and protect themselves from foreign interference. MSPs can reassure customers that their data is stored and managed locally, under the protection of local laws, which is essential for building trust in today's data-driven world.
- Seamless integration and scalability Many sovereign object storage solutions are S3 API-compatible. This compatibility with industry standards (such as AWS S3) facilitates effortless integration with existing systems and leading data backup solutions, such as Veeam. This enables MSPs to expand their service portfolios without extensive reconfiguration and to easily grow with their customers' needs.
- Opportunity for differentiation in the market In a market largely dominated by American hyperscalers, offering a truly European, compliant, and secure solution gives MSPs a significant competitive advantage. MSPs can position themselves as strategic partners who not only deliver technical solutions but also meet their customers' growing demands for digital sovereignty and data protection.

6. Conclusion

The European drive for sovereign object storage solutions is undeniable and is driven by a complex mix of geopolitical considerations, strict regulations, and the inherent need for data control and security. For MSPs, this shift represents not only a response to growing market demand, but also a strategic opportunity to enrich their service offerings.

By partnering with European cloud providers that offer transparent pricing models, advanced security features such as immutable storage, and compliance with the strictest EU regulations, MSPs can help their customers regain control of their digital assets. This not only leads to improved cyber resilience and cost efficiency, but also strengthens customer confidence and contributes to the broader goal of digital sovereignty for Europe. It is time for MSPs to embrace this strategic shift and consolidate their role as key players in building a resilient and independent European digital infrastructure.

More information ?

Cubixion.com

info@cubixion.com

Sign up for your free trial account!