FAST LTA

COMEX

?!

Whitepaper

European Storage for Digital Sovereignty

“Without control over your data, there is no control over your intelligence.”

This statement touches the core of a growing awareness among IT leaders: digital sovereignty is no longer a luxury, but a necessity. Especially now that organizations are strategically focusing on artificial intelligence. In May 2025, Microsoft, at the request of the U.S. government, blocked the mailbox of the Chief Prosecutor of the International Criminal Court. An unprecedented move. An American tech company digitally paralyzing an international judicial institution on European soil—this is a new development. Trade journals and news websites were filled with it.

If access to email can already be used as a political pressure tool, how vulnerable is the rest of our IT infrastructure? What if access to your backup is restricted at the request of a foreign government? Or if American companies are no longer allowed to provide services to European organizations? This case sharply illustrates how quickly organizations can lose control when they are dependent on foreign cloud providers. Digital autonomy is accelerating from an abstract policy ideal to a concrete strategic priority. And with that, the demand for European storage is growing.

Since: July 2025

The Control Paradox: Convenience vs Grip

Every organization aims for maximum control over data, infrastructure, compliance, and continuity. Yet in practice, we see a paradox: by choosing outsourcing and cloud solutions that relieve internal management, organizations gradually lose the control they thought they were gaining. This control paradox is the feeling that everything is taken care of in the cloud, while in reality one has less and less in their own hands.

The massive adoption of „as-a-service“ models and a cloud-first strategy undeniably offer benefits: scalability, flexibility, and less pressure on internal teams. But convenience comes with a downside—loss of control. This manifests on three levels:

Legally, data stored in a foreign cloud often falls under a different jurisdiction. Overseas governments or regulators can demand access, even if the data is physically located in Europe. Extraterritorial laws such as the U.S. CLOUD Act allow foreign authorities to access European business data without the involvement of EU institutions. In extreme cases, access to data or applications can be completely blocked by order of a foreign power, as the ICC example demonstrates. This directly contradicts European regulations like the GDPR and places organizations in a legal conflict. For more information on the legal risks, refer to the whitepaper “A critical fact-check on data security: US Cloud Act, FISA, and the Data Privacy Framework” at https://www.comex.eu/en/knowledge-center/.

Operationally, relying entirely on external services such as backup, email, or recovery makes it harder to intervene at critical moments. An internet outage could mean an organization cannot access its cloud data. Consider the flood disaster in Germany’s Ahr Valley in 2021: a hospital in the disaster area lost access to all patient data for several days because the medical administration ran entirely in the cloud and internet access was down. Care came to a halt. No access means no control. Geopolitical developments can also disrupt operations: sanctions or sudden changes in service delivery can render externally managed applications unavailable to end users. When a provider unilaterally changes its SLA or licenses, the customer is backed into a corner. These operational risks often only become apparent when things go wrong.

Technically, cloud providers boast certifications and compliance with laws like NIS2 and DORA, but real control remains distant from the client. Organizations usually have little insight into how and where their data is stored, protected, and updated. They rely on promises from the provider. Crucial security measures—whether data is truly stored immutably, whether there is an offline backup (air gap), or when critical patches are applied—are rarely transparent or demonstrably under the client‘s control, even if all documentation is in order.

» So, the question becomes: *how do you know your cloud provider feels the same urgency during a security incident as you do? Do you want to rely on external service contracts and response times, or would you rather take matters into your own hands and restore operations instantly?*

This control paradox is the current reality. The more we lean on cloud and outsourcing models, the more urgent the downside becomes. An unintended side effect of modernization is that „what you don‘t see, can still hurt you“: visible benefits hide invisible vulnerabilities. How to stay ahead of this paradox? We’ll get back to that later.

Legal and Operational Risks for European Organizations

Loss of control does not come without consequences. For Dutch, Belgian, German and other European organizations, dependency on foreign cloud providers entails significant legal and operational risks.

To begin with, there is the risk of violating privacy legislation. The U.S. CLOUD Act and intelligence law FISA 702 grant U.S. authorities far-reaching powers to access data stored with American cloud providers—even if that data is physically located on European soil. This conflicts with the European GDPR: companies that entrust personal data to an American cloud risk that this data ends up in third-party hands outside the EU’s regulatory framework. In the worst case, this could be classified as a data breach or unlawful transfer, with fines up to 20 million euros or 4% of global annual revenue.

The recent Schrems II ruling has made it clear that „business as usual“ is no longer sufficient. Legal frameworks for transatlantic data exchange are shaky. The new EU-U.S. Data Privacy Framework (DPF) was intended to provide more certainty but largely depends on U.S. goodwill. After a change in the U.S. administration, the supervisory body of the DPF was practically paralyzed, and a future government could unilaterally revoke the agreements. In short: companies cannot rely on temporary political fixes to meet permanent privacy requirements.

For more information on this topic, refer to the whitepaper “EU Data in the Hands of the U.S.: An Analysis of the Status of Transatlantic Data Protection Efforts” at www.comex.eu/en/knowledge-center/.

There is also the risk of **extraterritorial interference**. Foreign laws can directly affect European organizations. For instance, FISA 702 allows U.S. intelligence services to access data of non-Americans outside the U.S. without a court order. European citizens and companies do not enjoy the same protections under the U.S. Constitution as Americans. This means confidential business information, intellectual property, or customer data could end up in foreign hands without the organization’s knowledge or the ability to object. Edward Snowden’s revelations in 2013—also known as the PRISM scandal—already revealed the vast scope of such surveillance. For European companies in sensitive sectors, this forms a continuous compliance dilemma: fulfilling business cloud requirements without violating national and EU laws or the expectations of citizens.

FAST LTA

?!

Feitencheck

EU data in de handen van de VS

Een analyse van de status van trans-Atlantische inspanningen op het gebied van gegevensbescherming

Stand: april 2025

Continuity and dependency on foreign parties also form a real risk. The ICC incident is not isolated. It raises the question of how robust the continuity of Dutch organizations really is if they are fundamentally dependent on non-EU suppliers. What if, tomorrow, a major U.S. supplier—under pressure from its government—must restrict support services or access for your organization? This no longer seems far-fetched. Commercial decisions can also cause damage: consider a cloud provider that suddenly doubles its prices or discontinues a service. Organizations may face downtime or high migration costs. This so-called “Total Cost of Trust”—the sum of hidden risks and costs due to blind trust in foreign IT—is often higher than expected. Think of legal exposure, vulnerability to sanctions, delivery issues, and loss of control over critical data. A cost that only becomes clear once it’s too late.

Finally, **supervision and regulation** bring obligations. Recently introduced European directives such as NIS2 (for network and information security) and DORA (for digital operational resilience in the financial sector) raise the bar for governance and risk management. Organizations must demonstrably know where their data resides, who has access to it, and how quickly systems can be restored after incidents. If critical processes are outsourced, it becomes harder to prove compliance with these standards. As an organization, you remain responsible—even if the execution lies with a supplier. Digital sovereignty—being able to control your own data and systems—is thus not only a security issue, but also a compliance obligation.

European On-Premises Storage: Foundation for Hybrid Control

Fortunately, this new reality does not mean that the cloud must be completely abandoned. On the contrary, it’s about balance: regain control by bringing critical data and systems back under your own management, without giving up the advantages of the cloud. More and more organizations are opting for a hybrid infrastructure—a combination of cloud and local on-premises solutions—to retain flexibility while strengthening control.

European on-premises storage can serve as a solid foundation for such a hybrid strategy. By storing data on storage platforms that are produced and managed within Europe, organizations gain several advantages. Take for example the **European Storage from FAST LTA:**

Sovereign Off-cloud AI Application

Silent AI

Ransomwareproof Backup and Recovery with Air Gap

Silent Bricks

Compliant Long-term Archiving without Data Loss

Silent Cubes

1 First, there is **legal certainty**. Data stored on a European on-prem solution falls entirely under EU law. This prevents direct exposure to the CLOUD Act or FISA 702, as there is no American entity that can be forced to grant access. Moreover, local management makes it easier to comply with GDPR requirements and national regulations, as data residency and sovereignty are guaranteed. Auditors and regulators are more confident when it's demonstrable that sensitive data does not fall under foreign jurisdiction.

2 Second, it provides **operational autonomy**. A European on-prem storage solution gives organizations control during incidents. Air-gapped backups and archives located on-site remain accessible, even when internet connectivity fails or a cloud provider experiences an outage. A ransomware attack on a hospital in Düsseldorf in 2020 demonstrated how life-saving this can be. Patient records stored on hardware-based WORM storage could not be made inaccessible by hackers and remained available. A reassuring thought for any continuity manager. Additionally, having your own solution means independence from vendor decisions: you set update schedules, recovery procedures, and service agreements yourself.

3 Third, it offers technical **control and resilience**. With on-prem storage, you have full insight and authority over how data is stored and protected. Technologies such as immutability (unalterable storage), hardware-based WORM (Write Once Read Many), and air-gapped media (physically separated backups) can be implemented in-house, ensuring that backups cannot be tampered with and ransomware has no chance. In the Düsseldorf hospital case, local European-made WORM storage proved crucial: 400 terabytes of patient data remained safe and available despite a devastating cyberattack. Such measures are hard to enforce in a pure cloud environment—but on-prem, you control the last line of defense. This increases the Zero Loss objective: no data loss and no loss of control.

4 Finally, there's the advantage of a **short supply chain and local support**. European storage solutions also bring practical benefits. Products designed and built within Europe typically have shorter delivery times and fewer availability risks. Additionally, support is often more direct and faster through local partners. There's no dependency on support teams across the globe or components stuck in customs. This enhances business continuity and predictability. Crucially, it eliminates dependence on a single cloud provider (vendor lock-in), because data is locally available in a standardized format and can easily be copied to other environments if needed.

It's important to note that all of this does not stem from distrust, but from realism. By building a European foundation under your IT, you create a secure safety net within an otherwise flexible, modern infrastructure. Cloud where it fits, in-house control where it matters. Only then will your organization

Specialist in Secondary Storage

At Comex, we have been the specialist in secondary storage for more than 30 years. We provide reliable solutions for backup, archiving and AI infrastructure, with full control over your data as foundation for digital sovereignty. Our focus and approach?

- **Zero Loss Storage**: No data loss, maximum control and fully compliant.
- **Digital Sovereignty**: Your data remains within European
- jurisdiction, protected from foreign laws such as the U.S. CLOUD Act.
- **Hybrid Solutions**: Combination of local and cloud storage for optimal flexibility and security.
- **Long-term Support**: Up to 10 years of service and support for our solutions.

10 YEARS

MINIMUM LIFESPAN

SERVICE AGREEMENT

INVESTMENT PROTECTION

ALL INCLUSIVE SERVICE

Recommendations: Steps Toward Digital Sovereignty

You don’t acquire digital sovereignty overnight. It requires deliberate choices and concrete steps. Organizations that want to gain more control over their data would do well to proceed systematically.

1

Mapping Data Flows and Risks

Step one is mapping data flows and risks. Perform a systematic inventory of all data streams to foreign, particularly U.S.-based, cloud and SaaS services. Analyze which data and processes are sensitive or business-critical. This forms the basis for identifying where the greatest sovereignty risks lie.

2

Revieuw your Cloud Strategie and Repatriate Sensitive Data

Next, it’s important to review your cloud strategy and repatriate sensitive data to your own infrastructure where necessary. Consider relocating highly sensitive or business-critical data to on-premises solutions, especially where legal or continuity risks are high. Data that cannot be kept in-house should ideally be encrypted end-to-end with self-managed keys. This way, you maintain control even when data is in the cloud. Always take GDPR requirements into account when choosing cloud locations and providers.

3

Embrace a Hybrid Infrastructure

It also makes sense to embrace a hybrid infrastructure. Seek a healthy balance between cloud and your own local environment. Combine the best of both worlds by leveraging the flexibility and scalability of the cloud where possible, while implementing local storage and backups for critical data. This creates redundancy and avoids a single point of failure. After all, cloud is a means, not a goal in itself.

4

Implement Immutability and Air Gap

Another crucial step is to implement immutability and air-gapped backups. Ensure there is always a copy of your data that cannot be attacked or deleted in the event of an incident. Unalterable storage—such as WORM or immutability—in combination with physically separated backups (air gap) protects against ransomware, human error, and even malicious insiders. Regularly test whether these backups are truly accessible and intact. They form your last line of defense.

5

Transparency and Demonstrable Compliance

Additionally, transparency and demonstrable compliance are essential. Know at all times where your data is and who has access to it. Document this chain so you can show auditors and regulators how data is stored and protected. Transparency in data storage and access is not only technically desirable but also necessary under regulations like NIS2 and DORA. You must be able to demonstrate that you are in control, regardless of whether you use cloud services.

6

Choose European Technologies and Partners

Finally, it is wise to consciously choose European technology and partners. Where possible, use solutions developed and hosted in Europe. This avoids dependence on foreign laws and so-called black-box technologies. You also benefit from shorter lines in support and delivery. European storage solutions and IT infrastructure offer an extra guarantee that your data does not unintentionally become part of a geopolitical tug-of-war. More and more organizations in public and regulated sectors are consciously choosing homegrown IT.

Digital sovereignty requires vision and action. Control is not a luxury—it's a necessity. More organizations are realizing that data sovereignty is not achieved through a good contract or a checkbox in the SLA, but rather requires structural control over the entire information chain. The way you store, protect, and restore data says everything about your organization's resilience. In a time when geopolitics, cyber threats, and strict legislation converge, regaining control is not merely an IT project—it is a strategic investment in your organization's future. Take back control today so you can keep innovating with confidence tomorrow.

FAST LTA

FAST LTA
Rüdesheimer Str. 11
80686 München
info@fast-lta.de
www.fast-lta.de

Design,
Entwicklung
und Support
in **Deutschland**