● Whitepaper

Europe’s data at stake:

Six strategies to data sovereignty

eraneos

Contents

Executive summary

Data platforms have become the critical "crown jewels" of modern organizations, acting as the central brain and memory, powering operational and strategic decisions by storing, processing, and supplying vital data. Furthermore, increasingly its the engine that drives new innovative data driven processes and applications. Despite their importance, the overwhelming majority of these platforms are hosted on US cloud service providers (USCPSs), with an estimated 92% of EU data stored in US-controlled infrastructure. This alarming concentration introduces significant digital dependency and existential risks, including threats to availability, confidentiality, integrity, and privacy.

The risks are clear: when such a high percentage of data resides in a single market controlled externally, organizations effectively hand over their functioning, future, and survival to third parties. This raises a crucial question: Is this dependency appropriate?

To address these challenges, organizations must embark on the transition from digital dependency to digital sovereignty. This transformation is far from a simple IT initiative. It requires a strategic, integrated approach. Sovereign data platform strategies are pivotal in this journey. They enable organizations to mitigate existential risks while achieving higher levels of sovereignty readiness, striking a balance between control, cost, and complexity.

Key architectural enablers such as open standards and open-source software play a crucial role in these strategies. They help break free from vendor lock-in, improve system auditability against supply chain attacks, and allow organizations the freedom to inspect and adapt software as their needs evolve. Implementing these approaches requires careful planning and integration into a broader organizational framework spanning policy, people, and partnerships.

The journey toward digital sovereignty is best undertaken through a structured, phased approach:

1. **Conduct a data sovereignty inventory:** Assess current risks and dependencies.
2. **Define a data sovereignty roadmap:** Identify targeted strategies to minimize risks.
3. **Implement policies and technical systems:** Utilize coordinated efforts across teams.
4. **Establish continuous monitoring:** Safeguard against emerging risks and dependencies.

Eraneos is uniquely positioned to support organizations through this complex yet mission-critical transformation. With end-to-end services, combining deep industry expertise and technological excellence, we offer a pragmatic approach to navigating this challenge. In this whitepaper, we provide a strategic and technical guide to help organizations secure a sustainable, compliant, and sovereign trajectory, empowering them to turn complex data platform challenges into measurable strategic advantages.

The strategic imperative of digital sovereignty

Modern organizations are existentially dependent on information and communication technologies, including essential services like data storage and data processing, for their operational and strategic functioning.

Cloud data platforms are most often provided by foreign cloud service providers, with the majority of these being large US-based ones such as Amazon, Microsoft, and Google. Estimates suggest that as much as 92% of all EU data is now stored in the US, with only 4% stored in Europe.

The dependency challenge

When organizations utilize USCSPs, their services and critical data are only available with the consent and support of that CSP. All data is stored at an external party, in their data center, on their hardware, using their software, and administered by their people.

This dependency forces a critical set of trust questions regarding your most vital assets - your data platforms:

- **Availability:** Will they reliably continue service even in the face of political pressure or accidental outages?
- **Confidentiality:** Do they keep your data confidential even from foreign intelligence agencies?
- **Integrity:** Can your data be manipulated on their servers without your knowledge or ability to detect it?
- **Compliance & Privacy:** Is the privacy of your customers guaranteed, and can your organization comply with laws and regulations that govern your data (e.g. GDPR), given it is held in the US?

Recent geopolitical tensions between the EU and the US have fundamentally altered the trust equation, necessitating a critical reappraisal of the dependency relationship that organizations have with USCSPs.

Addressing the imperative

This whitepaper provides a framework for determining and selecting the level of sovereignty that is fitting for your organization, offering concrete next steps to mitigate any risks. Crucially, implementing digital sovereignty strategies for data platforms also creates opportunities for gaining more control, higher agility, better resilience, and potentially lower long-term costs.

Defining digital sovereignty

Digital sovereignty is fundamentally the ability of an organization to control and govern its own digital infrastructure, data, and technologies. When applied specifically to data platforms - the central repositories and processing engines for an organization's data, its most critical asset - it means ensuring that the systems that serve as the organization's "brain and memory" are fully aligned with the organization's broader interests, values, and jurisdictional requirements.

For a data platform to truly enable digital sovereignty, four core principles must be met:

- **Sovereignty of purpose:** The organization must be able to freely choose how and for what purpose to use the data platform without fear of coercion or interference from external parties (e.g. the cloud provider or its governing state). This ensures the system serves the organization's goals first.
- **Sovereignty of inspection (Trust and verify):** The organization must have the ability to understand, inspect, and audit the data platform. This is crucial for verifying that the platform is functioning correctly, that no adverse or hidden interests are being served, and that data integrity is maintained.
- **Sovereignty of adaptation (Agility):** The organization must be able to adapt the data platform to its evolving needs and unique context. Dependence on a closed, proprietary cloud data platform severely restricts this ability.
- **Sovereignty of provider (Freedom of choice):** An organization must be able to freely choose and switch between service providers, hosting, maintenance, and support partners, preventing dependence and lock-in to a single, powerful vendor.

Digital sovereignty requires more than just technology; it necessitates strategic choices in organizational policies, measures, procedures, partners, and people in addition to the underlying infrastructure, hardware, software, and technical expertise.

Ultimately, digital sovereignty is the opposite of digital dependency. The latter occurs when the data platform does not serve the interests of the organization but those of others - potentially misaligned or even malicious parties. It is characterized by an organization's inability to verify or audit the systems they depend on, adapt the platform to their needs, or switch providers. The reality is that the ubiquitous use of foreign cloud service providers places most organizations closer to digital dependency, introducing real and significant risks.

The risks of digital dependency

Cloud services, whether Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS), offer high flexibility and low maintenance. However, these benefits come with inherent trade-offs, including high costs, vendor lock-in, and significant dependence. For organizations hosting their critical data platforms in the cloud, particularly with USCSPs, there are four main sovereignty risks:

Service availability risk

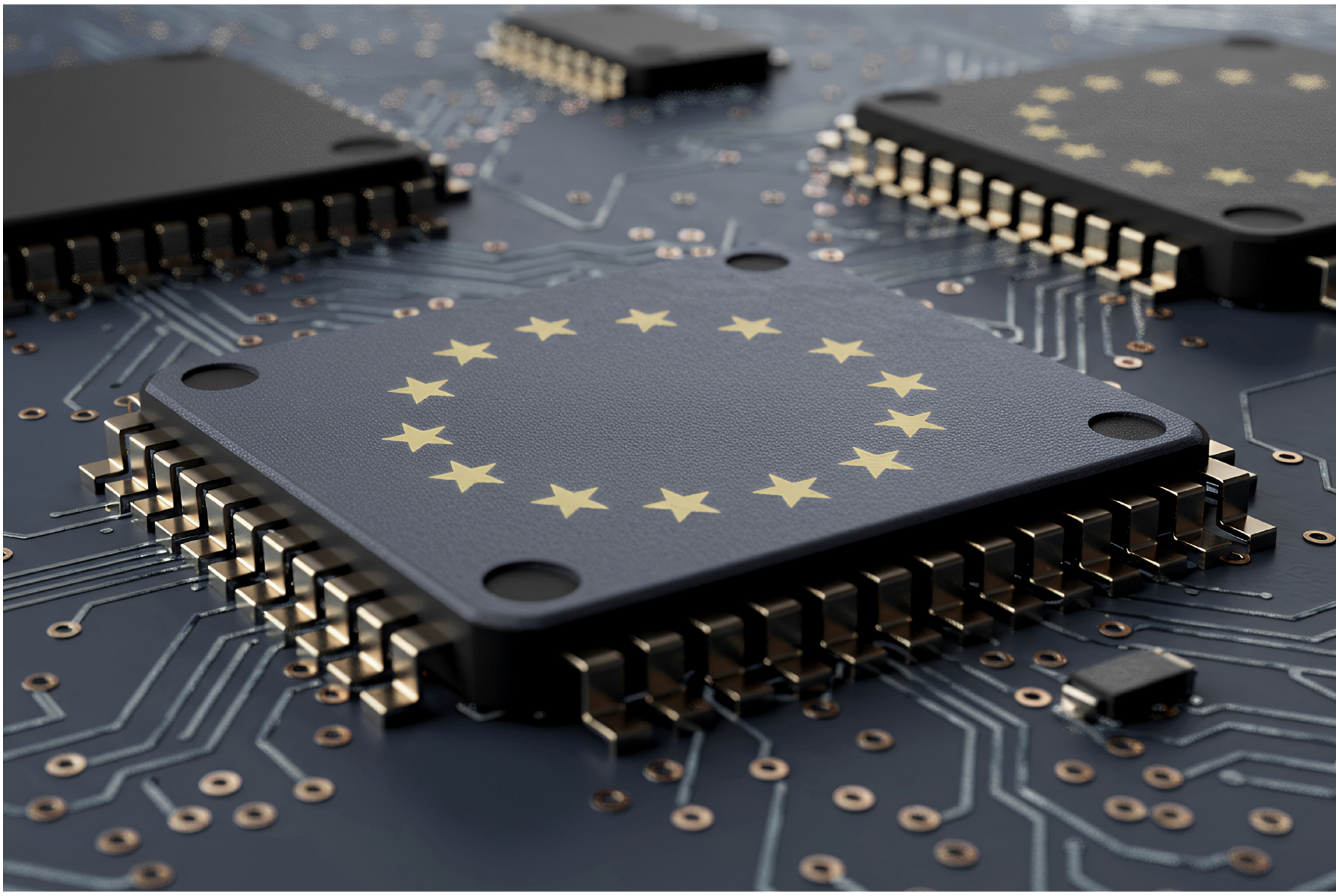
If the cloud service provider denies you their service, for whatever reason, can your organization still function, recover, and survive? This risk is not theoretical:

- In 2022, the Amsterdam Trade Bank had to file for bankruptcy because Amazon denied its services due to US Sanctions.
- In 2024, UniSuper, an Australian USD 125 billion pension fund, had its Google cloud account accidentally deleted by Google.
- In 2025, the Microsoft email account of the Chief Prosecutor of the International Criminal Court was blocked following an executive order issued by the United States.

Data confidentiality risk

If the cloud service provider gives third parties access to your data without your consent, will this be in your interest, and would you even know? This is already the status quo:

- The US CLOUD Act allows US authorities access to data stored in the EU, even if held by EU subsidiaries of US companies.
- It is normal practice for US Intelligence agencies to buy EU data from US companies without consent or notification.
- Cloud providers acknowledge this risk; in 2025, Microsoft admitted it could not guarantee sovereignty for UK Police data hosted in its cloud.



Data integrity risk

Can the service provider protect your data platform from bad actors manipulating your data? Would you even be able to detect this?

- Data manipulation can result in hard-to-detect operational problems or failed strategic decision-making.
- If your data is surreptitiously altered on the cloud servers, it can be impossible to detect, and if detected, impossible to diagnose without active help from the cloud provider.
- Given that USCSPs operate outside your organization's jurisdiction, you have no recourse for integrity breaches.

Data privacy risk

Your organization handles sensitive personal information of employees, customers, and suppliers. If this data leaks or is improperly accessed, who will be held responsible?

- EU data privacy laws (GDPR/AVR/EU Data Act) protect citizens against privacy violations.
- The European Court of Justice (ECJ) ruled in the Schrems I & II cases that the US Foreign Surveillance Act violates the privacy rights of EU citizens.
- While the EU-US Data Privacy Framework (DPF) is cited as a solution, it explicitly allows US intelligence gathering on EU data. Furthermore, the reliance on oversight mechanisms, such as the Privacy and Civil Liberties Oversight Board (PCLOB), can be vulnerable, as demonstrated by the effective disabling of the PCLOB in February 2025 by the US administration.

Digital sovereignty readiness levels

To transition from passive digital dependency to active digital sovereignty, an organization must first map its current position on the dependency-sovereignty spectrum. This allows for the determination of targeted sovereignty ambitions and the effective implementation of mitigating strategies.

We define four Sovereignty Readiness Levels specific to the control and governance of an organization's crucial data platforms:

Level	Name	Description	Data platform implications
0	**Dependent**	The organization is strongly dependent on foreign service providers for its continued operation. Sovereignty risks are vaguely known but not analysed. No measures taken or procedures in place to mitigate sovereignty risks.	The core data platform, including sensitive data and processing logic, resides entirely on a foreign cloud platform with no disaster recovery procedures for a service denial event.
1	**Prepared**	The organization is dependent on foreign service providers for its digital technologies, data, and infrastructure. Sovereignty risks are identified and analysed. The organization can recover from a service and data availability disruption. Data confidentiality, integrity, and privacy risks are known but based on trust without verification.	Sovereign data backup or a fallback data platform is in place, ensuring data is not permanently lost. However, the main platform's operations and data remain vulnerable to the CSP’s control regarding confidentiality and integrity.
2	**Independent**	The organization is only partially dependent on foreign service providers. Sovereignty risks are known, analysed, and actively mitigated. The organization can ensure business continuity in the face of a service and data availability disruption. Critical and privacy-sensitive data is confidential by design. Data integrity is verifiable.	Strategies like end-to-end encrypted data platforms with self-managed keys or hosting on a sovereign cloud agnostic data platform are implemented. Storage or processing is decoupled from foreign control, making critical data confidential and verifiable by design.
3	**Sovereign**	The organization is almost independent of foreign service providers for its continuous operation. Sovereignty risks are continually monitored and actively managed throughout the organization. The organization has control over nearly all aspects of its digital infrastructure, including infrastructure, hardware, software, and expertise.	The organization utilizes sovereign data infrastructure (on-premises or fully controlled sovereign cloud). Control is maintained over the entire stack - hardware, software, data, and necessary expertise - for maximum resilience and control over availability, confidentiality, integrity, and privacy risks.

Sovereign Data Platform strategies

Data platforms are the central repository for all data an organization needs to function; both operationally and strategically. They gather data from inside and outside the organization, store it for future use, analyse it and then supply the relevant data products to systems and actors inside and outside the organization. Data platforms are the heartbeat, brain and memory of the modern organization.

Data platforms perform several high-level functions:

- **Data ingestion:** retrieving data from internal and external systems.
- **Data processing:** cleaning, combining and analysing data.
- **Data storage:** keeping data for historical analyses.
- **Data serving:** supplying data products to people and other systems.

Data platforms often store the ‘data crown jewels’ of an organization. A dependable and secure data platform is therefore of existential importance to modern organizations. This makes the data platform especially important to consider in the light of digital sovereignty.

Cloud data platforms like Databricks, Snowflake, Fabric and others are almost exclusively hosted on USCSPs, introducing the availability, confidentiality, integrity and privacy risks discussed previously. Could your organization continue to function when the central data platform is unavailable and its data unrecoverable?

In this section, we describe several strategies for mitigating the sovereignty risks that surround many modern data platforms. These sovereignty strategies serve as a starting point for thinking about increasing the sovereignty stance of your data platform.

01. Sovereign data backup

Sovereignty readiness level 1: prepared digital sovereignty

Implement an out-of-CSP backup encompassing all data, metadata, data ingestion logic, and data transformation logic associated with the data platform. This proactive measure fundamentally shifts the consequence of a sudden, potentially permanent service disruption from an existential crisis to a manageable disaster recovery crisis. Utilizing an open data format for the backup significantly enhances the organization’s choice of recovery destination.

This strategy provides a critical safeguard, preventing the total loss of all historical data and enabling a viable transition to a new data platform in the event of a forced exit. However, this approach entails a trade-off: significant downtime is probable, as a new data platform must be commissioned before the recovery process can commence. Furthermore, proprietary nature of the CSP data platform means that metadata, ingestion configuration, and transformation logic may be tightly coupled, potentially requiring complex reimplementation during recovery. Therefore, ensuring backup completeness, integrity, and usability necessitates ongoing effort in monitoring and routine recovery exercises.

Availability	★	Data is not lost permanently in case of service disruption.
	★	Recovery into a new data platform is possible.
	👎	Downtime while a new data platform is designed, built and commissioned.
Confidentiality	👎	All data is still vulnerable to confidentiality breaches by the CSP and intelligence services.
Integrity	★	The sovereign data backup could be used to detect surreptitious changes.
	👎	Data integrity breaches made before backups are not detectable.
Privacy	👎	Data is stored at a CSP and thus vulnerable to privacy breaches.

02. Fallback Data Platform

Sovereignty readiness level 1: prepared digital sovereignty

Organizations adopting this recovery approach employ a separate, sovereign data platform as a fallback that takes over in case of a service disruption or forced exit from a primary foreign-hosted platform. The fallback platform is strategically scoped to provide only critical data services. Non-critical services can be restored from a sovereign data backup during the eventual recovery phase.

This strategy delivers superior resilience by preventing both total data loss and downtime for critical services. However, this robust protection comes at the cost of significant duplicate effort: maintaining a separate data platform and ensuring it remains in sync with the main data platform requires ongoing resources. To validate operational integrity, recovery effectiveness must be regularly tested with comprehensive recovery drills.

Availability	★	Data is not lost permanently in case of service disruption.
	★	No downtime for critical data services.
	👎	Rebuild of non-critical data services necessary.
Confidentiality	👎	All data stored in the data platform is vulnerable to confidentiality breaches by the CSP and intelligence services.
Integrity	★	The fallback data platform could be used to detect and audit surreptitious historical data changes in the main data platform used for critical data flows.
Privacy	👎	All data is stored at a CSP and thus vulnerable to privacy breaches.

03. Sovereign domain/foreign domain

Sovereignty readiness level 1: prepared digital sovereignty

This strategy involves architecturally segmenting the data platform into two distinct components: a Sovereign Domain Data Platform and a Foreign Domain Data Platform. The core principle is to confine all sensitive data storage and processing to the Sovereign Domain, reserving the Foreign Domain for non-sovereignty critical workloads. Critically, the Sovereign Platform concurrently serves as the primary fallback platform and data backup.

Impact and trade-offs

This approach provides a robust mechanism to avoid critical service disruption and secure the organization's most sensitive data assets. However, it introduces inherent operational and architectural complexities:

Availability	★	No permanent data loss via core backup.
	★	Service disruption only impacts the foreign platform data flows.
	👎	Migration of non-core data services is necessary on forced exit.
Confidentiality	★	Data stored in the sovereign platform; not in the cloud.
	👎	Risk of data leakage from sovereign core to cloud platform.
Integrity	★	Data in the sovereign core is now outside of CSP.
	👎	Integrity violations in the cloud platform can leak into the sovereign core.
Privacy	★	Privacy-sensitive data can be stored in the sovereign core.
	👎	Privacy-sensitive data can only be processed in the sovereign domain.

04. End-to-end encrypted Data Platform

Sovereignty readiness level 2: independent

This strategy represents a foundational shift towards Sovereignty Readiness Level 2 (Independent), focusing on decoupling critical control elements from foreign CSPs. The architecture mandates the decoupling of storage, compute, and metadata storage, enabling encrypted data storage secured by self-managed keys. Under this model:

This approach delivers significant architectural flexibility: it enables the use of highly scalable storage on any CSP while simultaneously allowing the processing of non-sensitive data to be distributed across both sovereign and foreign compute providers.

Availability	★	No data loss in case of forced exit.
	★	Freedom of storage back-end enables fast recovery.
	👎	Switch to the sovereign data plane is necessary in the event of service denial.
Confidentiality	★	All data storage is encrypted with self-managed keys.
	★	All sensitive data processing is end-to-end encrypted.
Integrity	★	Data integrity violation prevented by encryption.
Privacy	★	All data on CSP is encrypted.

05. Sovereign cloud agnostic Data Platform

Sovereignty readiness level 3: sovereign

This strategic approach mandates the use of a sovereign data platform hosted on a sovereign CSP, architected around cloud-neutral data platforms. The implementation strongly favors solutions based on open standards and open-source software.

The core objective is to ensure that all data is stored and processed entirely within the jurisdiction of your choice, eliminating direct dependencies on US companies and their associated USCSPs. By adopting a cloud-neutral architecture, the organization gains the freedom to seamlessly choose and switch between different cloud service providers and support partners, effectively preventing vendor lock-in and its associated financial and operational risks.

While this strategy significantly reduces foreign dependencies and achieves a high level of data sovereignty, its execution requires substantial internal capability in the design and integration of open-source data platform components onto the sovereign cloud provider's infrastructure.

Availability	★	No dependency on USCSPs for the data platform.
	★	All data, ingestion, transformation and data products are sovereign.
	👎	Dependability of the data platform requires good design, implementation and maintenance.
Confidentiality	★	All data stored and processed on a sovereign cloud service provider.
Integrity	★	All data is now outside of USCSPs.
	👎	Integrity risk of the software supply chain still requires controls.
	👎	Hardware supply chain is out of scope.
Privacy	★	All privacy-sensitive data stored in a sovereign data platform.

6. Sovereign data infrastructure

Sovereignty readiness level 3: sovereign

This strategy represents the ultimate commitment to digital sovereignty by advocating for the deployment of a sovereign data platform on hardware and infrastructure fully owned and controlled by your organization (on-premises).

To implement this, organizations must proactively take expertise in-house to maintain and control the entire technology stack—the infrastructure, hardware, and software. This is achieved by either sourcing a vetted on-premises data platform solution or building one using open standards and open-source software, coupled with the use of carefully vetted hardware suppliers.

While this approach yields the highest sovereignty level available for data platforms, this maximal control comes with the highest upfront and operational costs, requiring substantial investment in infrastructure, maintenance, and the development of deep internal technical expertise.

Availability	★ ★	All data, software, hardware, and infrastructure under own control/ High resilience because expertise is within the organization.
Confidentiality	★ 👎	Data only stored in own data center, on own hardware in own infrastructure. Closed-source firmware for hardware is a tail risk.
Integrity	★	All data is now within its own sovereign domain.
Privacy	★	All privacy-sensitive data stored on a sovereign platform.

These various data sovereignty strategies — ranging from basic sovereign backup to full sovereign infrastructure - represent a toolkit for addressing the most acute data platform sovereignty risks. However, selecting and executing the right strategy is only the first step. Organizations must recognize that technical architecture alone cannot deliver true digital sovereignty; it requires a systemic approach that aligns all facets of the business.

Positioning your Data Platform strategy within a broader sovereignty strategy

While selecting a sovereign data platform strategy is a necessary foundation, it is inherently insufficient on its own to comprehensively mitigate organizational sovereignty risks. The strategic choice for any data platform approach must therefore be embedded within a broader, overarching digital sovereignty strategy that addresses all critical vectors across the enterprise.

The sovereignty strategy for your organization includes:

1. **Policy:** the formal policy and procedures adopted by the organization.
2. **People:** the competence and capacity of people inside the organization.
3. **Software:** the strategic platforms and software systems used by the organization.
4. **Measures:** prepared actions taken by the organization to mitigate sovereignty risks.
5. **Partners:** external partners and agreements with them about data processing.
6. **Hardware:** the physical and virtual servers used by the organization.
7. **Data Management:** the management of data and processes across multiple systems and departments.

Data platforms, while occupying a central and critical place in the operational and strategic decision cycle of an organization, represent only one component within a larger, interconnected information and IT domain.

To effectively increase your digital sovereignty readiness level, it is crucial that the chosen data platform strategy is not isolated, but systematically matched and integrated with all other contributing factors of the organizational sovereignty strategy. These factors - including policy, people, partners, measures, software, hardware, and data management - must be holistically considered to ensure coherence and maximize risk mitigation across the enterprise.

Open standards and open source in digital sovereignty

Open standards and open-source software are not merely technical choices; they are powerful enablers that fundamentally improve an organization's digital sovereignty posture. By embracing openness, organizations transition from a position of blind trust to one of verifiable control.

With closed proprietary software, an organization is forced to trust the vendor implicitly regarding the software's functionality and security. Conversely, open source allows for full inspection and auditability. You can verify the code's behaviour, ensuring it aligns with expectations and does not serve hidden interests. While supply chain attacks are a reality for all software, the open nature of the code means external security researchers, auditors, and the public community can actively detect problems, backdoors, or suspicious behaviour, including potential surveillance features that may remain hidden in closed systems from foreign providers.

Open standards and open source dramatically enhance the principles of adaptation and provider choice:

- **Adaptation:** Your organization gains the freedom to inspect, change, and modify the software to its unique, evolving needs. You are no longer dependent on a single vendor's roadmap or permission to add features or fix critical problems. This freedom allows you to hire any competent developer or company to make changes, significantly increasing the speed and agility of your organization.
- **Provide choice:** By building systems on open standards (e.g., Apache Iceberg or Parquet formats), your data and systems become functionally independent of a single vendor. This allows for seamless migration between cloud providers or a pivot to on-premises infrastructure, effectively preventing vendor lock-in. Proprietary systems often employ closed formats and APIs specifically to create high switching costs and maintain a vendor's pricing power; using open standards directly diminishes this leverage.

Strategic trade-offs

It must be acknowledged that open source is not a silver bullet. While it solves the dependency problem, it introduces a requirement for technical expertise (either in-house or through specialized partners) and places the responsibility for maintenance on the organization. These are, however, solvable operational challenges - ones that grant control and verifiability in return for effort. The ultimate value of this trade-off depends entirely on the organization's strategic context and sovereignty ambition.

How to choose a Data Platform sovereignty strategy

Throughout this whitepaper, we have illustrated a suite of sovereignty strategies for data platforms, analysing their specific trade-offs and direct impact on mitigating core sovereignty risks (availability, confidentiality, integrity, and privacy). It is crucial to recognize that these examples represent only point samples within a large, complex solution space for digital sovereignty.

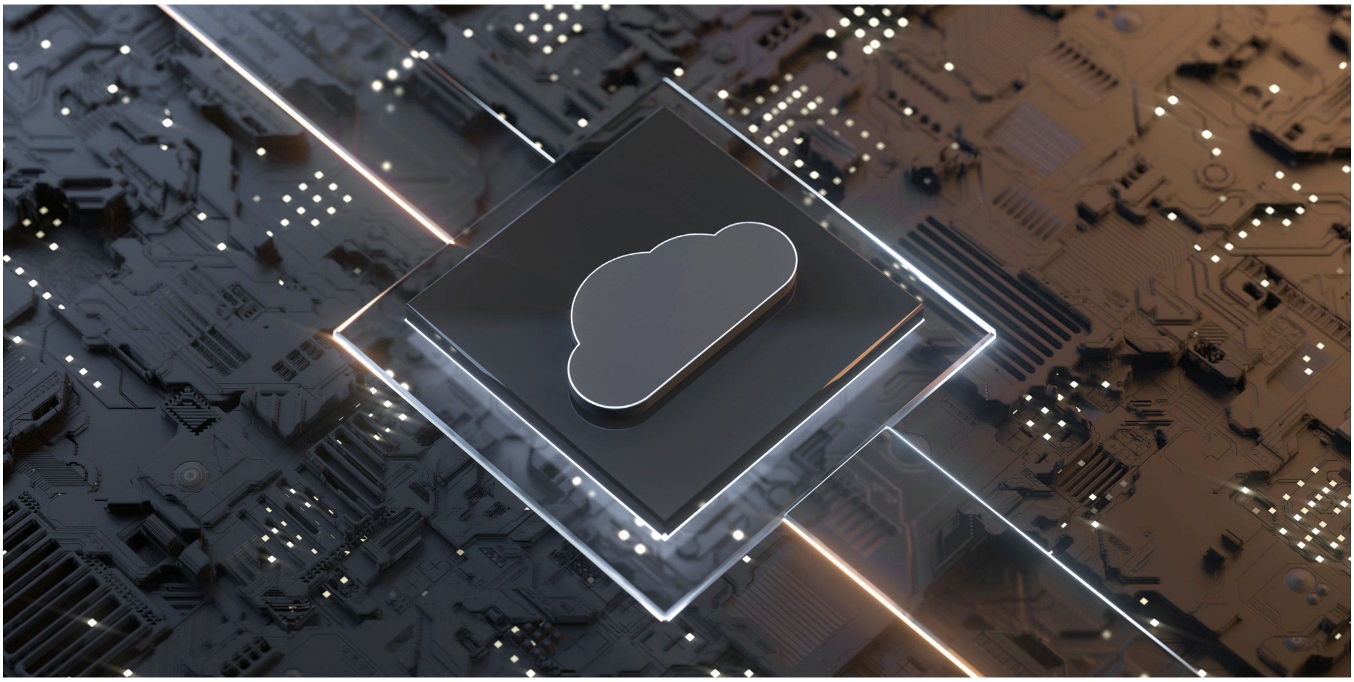
Determining the fitting sovereignty trajectory is inherently context-dependent and must be rigorously tailored to the unique risk profile and strategic ambitions of each organization. Increasing your digital sovereignty is not a singular action but a sustained effort across multiple, interconnected dimensions.

To effectively increase your sovereignty readiness level we propose a 4-phase approach:

Phase 1: Data sovereignty inventory

Increasing the data sovereignty of your organization while maximizing benefits and reducing impact starts with understanding the organization's goals, sovereignty ambitions, and current data landscape.

- **Data landscape map:** This identifies what data is stored, where it is stored, how it is processed, and where. This map is crucial for identifying where **your "data crown jewels" reside and where dependencies exist.**
- **Data sovereignty risk assessment:** Perform a risk assessment based on the inventory to identify the specific Availability, Confidentiality, Integrity, and Privacy risks, their severity, and potential mitigations for each platform or data set.



Phase 2: Data sovereignty roadmap

Once the risks and their potential mitigations are identified, a strategic plan is necessary.

- **Determine the appropriate strategy:** Select and formulate the fitting data platform sovereignty strategy based on the data sovereignty risk assessment and the data landscape map from Phase 1.
- **Roadmap design:** A data sovereignty roadmap can be designed that identifies the impact and weighs the trade-offs between implementation effort and risk reduction of various sovereignty strategies (e.g., comparing an end-to-end encrypted data platform vs. sovereign data backup).
- **Alignment:** This plan aligns both the technical and the organizational steps required to mitigate the data sovereignty risks. The roadmap serves as the crucial guide for all subsequent implementation efforts.

Phase 3: Data sovereignty implementation

This phase involves the simultaneous, coordinated execution of the roadmap.

- **Data platform development:** Migrating or implementing a data platform is a large venture that requires continuous development to match your internal data needs.
- **Coordination:** Implementing the data sovereignty roadmap requires the simultaneous coordination of policies, measures, people, and technical systems.

Phase 4: Data sovereignty monitoring

Digital sovereignty, much like cybersecurity, is not a one-time fix but an ongoing operational function.

- **Continuous oversight:** Data sovereignty requires a monitoring approach to prevent new sovereignty risks from being introduced, ensuring continuous adherence to the new policies and maintaining the desired sovereignty readiness level.

Charting your Data Platform's path to digital sovereignty

The journey from digital dependency to digital sovereignty is not a binary choice but a strategic path that each organization must navigate based on its unique risk profile, operational requirements, and resources. For the data platform, the geopolitical landscape has fundamentally altered the trust equation between European organizations and USCSPs, transforming platform decisions from purely technical considerations into a strategic imperative with existential implications.

The cost of inaction is rising. Recent events - from service denials driven by political sanctions to the dismantling of privacy oversight mechanisms (such as the PCLOB, which oversees US intelligence access to data) - demonstrate that sovereignty risks are not theoretical but immediate and material. Organizations that fail to assess and mitigate these risks face potential business continuity crises, severe regulatory non-compliance (e.g. GDPR), and the subsequent loss of competitive advantage.

There is no universal solution. A financial institution handling sensitive transaction data requires different sovereignty measures than a manufacturing company analyzing production metrics. The strategies outlined in this whitepaper - from sovereign data backups and end-to-end encrypted data platforms to fully independent data infrastructure - represent a toolkit from which organizations must select based on their specific sovereignty readiness ambitions and constraints.

Open standards and open source provide critical leverage. While achieving full sovereignty often requires significant investment, architectural choices around open standards (like Apache Iceberg or Parquet) and open-source software can dramatically reduce vendor lock-in, drastically improve the ability to audit system integrity, and preserve future optionality - even when immediate full sovereignty is not feasible.

Start with assessment, proceed incrementally. Organizations need not - and often should not - attempt a wholesale transformation overnight. Begin with a comprehensive data sovereignty inventory to understand current dependencies and risks (where data is stored and processed). Design a pragmatic roadmap that prioritizes high-impact, lower-complexity interventions first. Build organizational capability and expertise progressively while maintaining operational continuity.

The path to digital sovereignty requires vision, commitment, and sustained effort across technical, organizational, and policy dimensions. But the alternative - continued uncritical dependence on foreign infrastructure for your organization's most critical data assets - is becoming increasingly untenable. The question is no longer whether to pursue digital sovereignty, but how quickly and effectively your organization can chart its course toward it.

End-to-end services that deliver impact

Navigating the strategic, architectural, and compliance complexities of data sovereignty requires expert guidance. Eraneos offers end-to-end services that deliver measurable business impact, combining deep industry expertise with technological excellence in data platforms and governance. Our pragmatic approach ensures sustainable adoption over experimental implementation. We specialize in building secure, scalable data foundations with full sovereignty and compliance in mind.

Partner with Eraneos to transform your data sovereignty into a competitive advantage.

Author:

Mathijs de Meijer
Senior Consultant – Data & AI
Eraneos

mathijs.de.meijer@eraneos.com

Get in touch

Claudia Schulze
Partner – Data & AI
Germany
claudia.schulze@eraneos.com

Dave Kiwi
Practice Lead – Data & AI
Netherlands
dave.kiwi@eraneos.com

Katharina Fulterer
Partner – Data & AI
Switzerland
katharina.fulterer@eraneos.com

Antonio Rodriguez
Senior Manager – Data & AI
Spain
antonio.rodriguez@eraneos.com

eraneos.com