Microsoft

# Digital Sovereignty

## Balancing control, compliance, security, resilience and innovation

Legal/ Regulatory

Cybersecurity

Operational resilience

Technological innovation

# Table of contents





# Editorial


**MARK CHABAN**

Corporate Vice President,
Commercial Cloud Solutions,
Microsoft Europe, Middle East & Africa


Digital sovereignty has now become a strategic imperative for European companies. In the face of accelerating digital transformation, the multiplication of cyber-threats, and rapidly evolving regulations, it is essential for every organization to maintain control over its digital destiny.

However, digital sovereignty is not limited to a purely technological issue: it encompasses national dimensions (a country's ability to make its own decisions), economic dimensions (control over value chains), operational dimensions (control over resilience), legal dimensions (the regulatory framework governing data and services), and innovation dimensions (control over infrastructures and data). Its goal is to guarantee the autonomy of companies while enabling them to take advantage of the opportunities offered by the cloud and innovation.

Adopting a pragmatic approach to digital sovereignty means turning this challenge into a lever for growth, resilience, and differentiation in an increasingly competitive market. This white paper was designed to detail the issues related to digital sovereignty and to propose a risk-based analysis framework to support strategic decision-making at the executive committee level.

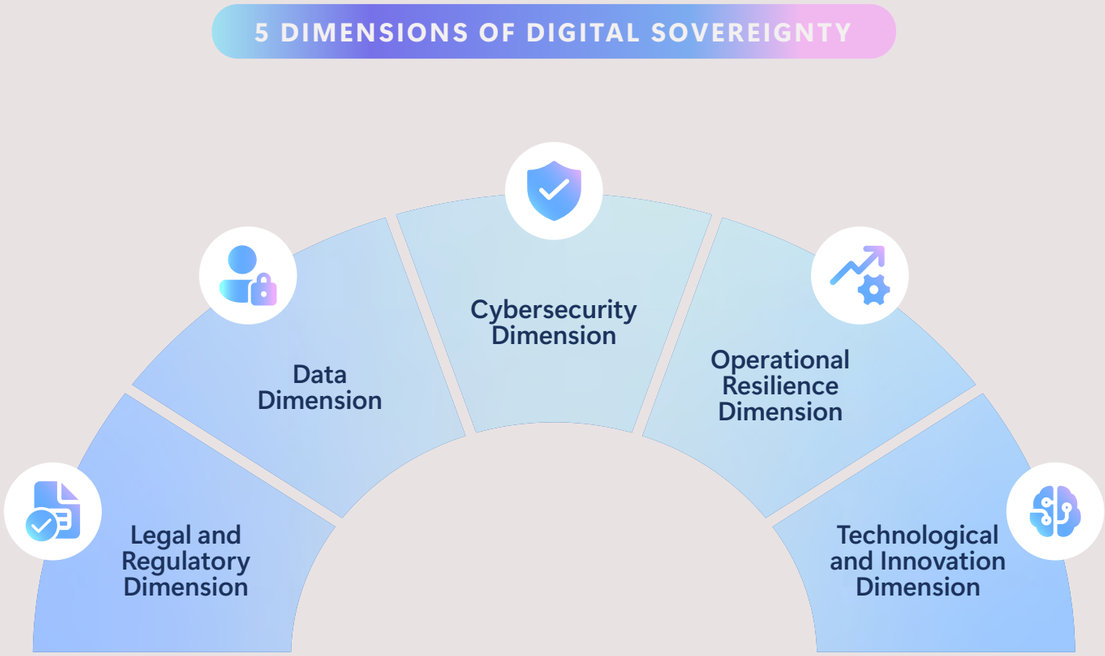
# 1 Digital Sovereignty in Europe: A Strategic Imperative for Businesses



## A Multifaceted Concept: Mastering One's Digital Destiny

**Digital sovereignty is defined as the capacity of a state or organization to operate within cyberspace in accordance with its own legal frameworks and strategic interests. In other words: "Who controls, stores, protects and determines how your data will be used?" Today, digital sovereignty stands at the center of European strategies, driven by the imperative to safeguard autonomy—of both values and data—in an increasingly interconnected world.**

**Digital sovereignty extends beyond technology alone, involving multiple dimensions, each presenting distinct requirements.**



## LEGAL AND REGULATORY DIMENSION: COMPLIANCE AND JURISDICTION

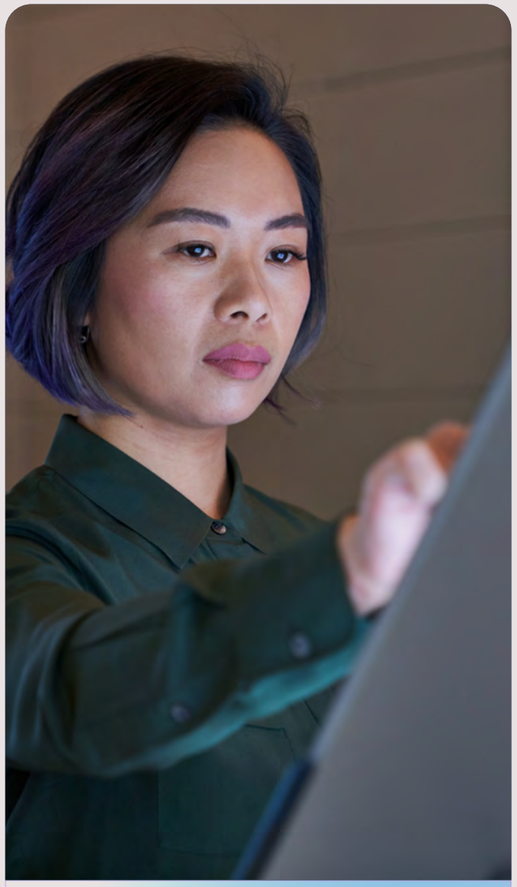
Adherence to the European legal framework is essential, particularly regarding personal data protection, network security, and both sectoral and national regulations. It is also imperative to ensure that critical data remains governed by European laws. The goal is to prevent any violations—which can result in penalties of over 4% of a company's worldwide revenue—and to protect against extraterritorial interference.

## DATA DIMENSION: MASTERY AND CONTROL OF INFORMATION

This involves maintaining control over strategic data, from its location to its usage. This requires a clear understanding of where sensitive data is stored and processed, identification of all individuals with access to it, and the ability to utilize it freely. A sovereign organization ensures that its critical data is hosted on trusted infrastructures, ideally within Europe, with mechanisms guaranteeing total confidentiality (strong encryption, locally managed keys, etc.). Digital sovereignty is about making sure organizations have control over where their data is stored, how it's used, and who manages it.

## CYBERSECURITY DIMENSION: SECURITY AND DIGITAL TRUST

This dimension focuses on providing strong protection for all information systems and data from cyber threats. This includes the ability to implement your own security requirements—such as data encryption, access controls, and incident response plans—to ensure that your cloud security is just as strong as what you'd use within your organization. Recent regulatory expectations from European authorities, such as the cybersecurity directive, require companies in critical sectors to provide strong guarantees—from multi-factor authentication and end-to-end encryption to crisis plans and regular audits—to strengthen resilience against attacks.



**A QUESTION TO CONSIDER:**

Are third-party data and services as secure as if we managed them ourselves, and can we verify and require this level of security?



## OPERATIONAL RESILIENCE DIMENSION: AUTONOMY AND BUSINESS CONTINUITY

Ensuring that the company remains operational during external shocks to its technologies is crucial. This means limiting situations of critical dependence on a single provider or on infrastructure beyond one's control. For example, it is necessary to anticipate the effects of a possible unavailability or degradation of a cloud service (major outage, sudden change in terms of use, geopolitical tension or embargo that could affect access to a given platform).

**A QUESTION TO CONSIDER:**

In the event of a major setback (severe cyberattack, contract termination, or political pressure on one of our foreign technology providers), are we able to continue our operations and protect our digital assets?

In other words: "Who do we accept to be dependent on, and for which links in our value chain?" This introspection is aligned with the idea of defining how far one can outsource without compromising the sovereignty of one's business activities.

## TECHNOLOGICAL AND INNOVATION DIMENSION

Digital sovereignty also includes the ability to choose, master, and leverage strategic digital technologies, especially those shaping the future of the company: artificial intelligence (AI), automation, big data, collaborative platforms, etc. The challenge is twofold: not to depend exclusively on foreign technological solutions, and not to miss out on key innovations that enable competitiveness.

**A QUESTION TO CONSIDER:**

Are the solutions we use aligned with our sovereignty requirements (location, transparency, resilience, data control)?

Other aspects may also be considered, such as financial/tax sovereignty in relation to digital matters, or innovation sovereignty to maintain control over algorithms and patents, or to safeguard them through encryption of the execution environment. Digital sovereignty is transversal, covering technical (cloud choice, encryption, IT architecture, resilience zones), legal (contracts, compliance), and strategic (risk management, competitive differentiation through innovation, optimization of development and production costs, etc.) dimensions.

# **Approaching Sovereignty** as a Risk Analysis

**An effective way to address such a broad concept is to conduct a structured risk analysis. This approach makes it possible to contextualize digital sovereignty into concrete, measurable, and actionable issues.**

### ASSESS RISKS FOR EACH DIMENSION

This approach involves identifying the potential risks faced by the company for each of the dimensions. For example, regulatory risk refers to situations of non-compliance that may lead to financial penalties or blockages; data risks mean loss of control or leaks of sensitive data; cybersecurity risks involve the possibility of intrusion or sabotage via a provider; and resilience risks can mean a critical interruption of activity during an external failure, among others. Each risk is assessed based on its impact—whether operational, financial, or reputational—and its likelihood, to enable prioritization of the most critical risks.

### EVALUATING THE RISKS OF ACTION AND INACTION

Every strategic decision involves assessing both the risk of acting—such as adopting a technology not yet mastered in Europe, which may expose the organization to sovereignty risks—and the risk of not acting—such as refusing to migrate to the cloud, thereby risking a loss of competitiveness or security if internal systems are less effective. Each committee must therefore consider both aspects, weighing the cost of dependency against the cost of renunciation.

By approaching digital sovereignty through a risk-based lens, the organization defines its tolerances (what it accepts or not), its minimum requirements (technical or legal), and its action plan (mitigation measures, investments, internal policies) to reduce risks to an acceptable level. This approach transforms what can sometimes be an abstract concept into a clear roadmap for the organization.

## **Define Guiding Questions** for The Executive Committee

**At this stage, it is important for leaders to consider a series of key questions that help align the company's strategy with sovereignty challenges.**

### COMPLIANCE:

Do we meet European data and security requirements, and how do we demonstrate this?

### DATA LOCATION:

Do we know precisely where our strategic data is stored and processed and its jurisdiction? Are there contractual guarantees it remains in Europe?

### ACCESS CONTROL:

Which parties may access confidential information, including data stored with cloud service providers? Do we maintain control over encryption keys and access decisions?

### CYBER-RESILIENCE:

If a major cyberattack or critical cloud outage impacts a provider, do we have backup plans—such as recovery in another environment or isolated backups-to ensure continuity?

### TECHNOLOGICAL DEPENDENCY:

Does our digital activity heavily depend on a limited number of global providers? What is our alternative or multi-sourcing strategy to avoid vendors locked in?

### OPPORTUNITY AND INNOVATION:

Are there areas where our sovereignty concerns could cause us to miss out on key innovations-e.g., AI solutions not available in Europe? How do we balance the risk of "not doing" with the risks of "doing"?

These questions help structure reflection during strategic committees or risk reviews and clarify sovereignty requirements. For example, not having control over encryption keys may lead to requiring "zero knowledge" encryption from providers, and strong dependence on a single cloud may encourage adopting a multi-cloud architecture, combining sovereign and global clouds.

"Digital sovereignty is emerging as a strategic priority for European enterprises, ensuring autonomy while unlocking the value of cloud and innovation. When approached pragmatically, it becomes a powerful catalyst for growth, resilience, and competitive differentiation."

**PHILIPPE LIMANTOUR**

Chief Technology & CyberSecurity Officer, Microsoft France

# **Finding a Balance** Between Sovereignty and Business Strategy

## COMBINING SOVEREIGNTY IMPERATIVES AND STRATEGIC OBJECTIVES.

One of the key messages for a leader is that digital sovereignty and business performance should not be opposed, but rather intelligently reconciled. An effective organization will know how to integrate its sovereignty requirements into its digital strategy without hindering its development. This means formulating a framework (policies, selection criteria) that guarantees critical aspects (compliance, data control, security) while allowing the company to innovate, transform, and remain competitive in its market. Digital sovereignty is neither a slogan nor a luxury, but a requirement for security, competitiveness, and compliance for the modern enterprise. When properly managed, it becomes a lever for trust and added value rather than a constraint.

## DO NOT SACRIFICE INNOVATION: AVOID TECHNOLOGICAL ISOLATION.

A pitfall would be to seek absolute sovereignty by isolating oneself from global solutions. Relying exclusively on domestic or internal providers for all digital services may result in a reduced access to technological advancements. Major cloud hyperscalers offer services of a richness and efficiency that are difficult to match. If these solutions are avoided entirely, there is a genuine risk of lagging in terms of innovation. This poses an industrial threat, as it opens the door to competitors advancing with artificial intelligence, big data, cybersecurity, or collaborative technologies. Achieving a suitable equilibrium is crucial. For instance, one approach could be to leverage external cloud while maintaining control over data through technical safeguards. This approach enables organizations to leverage the flexibility and innovative capabilities of cloud computing, while effectively neutralizing the risk of compromising data sovereignty.

## HYPERSCALE CLOUD AS PART OF THE SOLUTION.

Paradoxically, major international clouds—often seen as a threat to sovereignty—are also part of the answer, provided they are used in a controlled manner. Indeed, modern cloud services bring substantial benefits that address leaders' concerns:

• **Security and compliance:** Hyperscalers such as Microsoft invest massively in cybersecurity and comply with the strictest standards-ISO 27001 certifications, third-party audits, GDPR compliance. They provide advanced protection tools—including default encryption, AI-based intrusion detection, geo-redundant backups, and confidential computing—that would be expensive to develop in-house. Naturally, this does not exempt the company from requiring appropriate guarantees, such as a European storage location or contractual clauses prohibiting unauthorized disclosure. However, once these safeguards are established, a hypercloud delivers a robust and continuously evolving standard of security. This argument is crucial for reducing cyber risk, especially against industrialized attacks from nation states such as China, North Korea, Russia, or Iran.



• **Resilience and continuity:** Hypercloud datacenters are distributed worldwide, including across Europe, with redundancy and recovery capabilities in case of major incidents. Relying on a well-managed multi-regional cloud can therefore strengthen business continuity. Effective management is crucial in this context. Implementing a robust multi-cloud or hybrid architecture can address the challenge of the single point of failure. In summary, enhanced resilience is attainable through the strategic utilization of multiple cloud environments, including sovereign clouds, rather than relying solely on a single local infrastructure.

• **Innovation and agility:** Using public cloud gives access to a rich catalog of innovative services in terms of AI, cybersecurity, large-scale machine learning, analytics, IoT. These technologies accelerate R&D, product development, and optimize operations, ultimately creating a competitive advantage. Striking a balance does not mean rejecting global digital advances; instead, it involves making careful choices while maintaining necessary governance. For instance, you can use an AI cloud service and still keep input and output data encrypted or pseudonymized, protecting sensitive information from exposure.

• **Environmental and cost benefits:** The climate impact is a frequently overlooked factor when considering digital sovereignty. Major cloud providers operate hyper-optimized data centers, often powered by renewable energy and with much better energy efficiency than traditional private datacenters. Resource pooling in the cloud allows for very high server utilization rates, reducing energy waste, multiple clients sharing the same infrastructure instead of separate, underused infrastructures. Result: the carbon footprint per application decreases significantly.

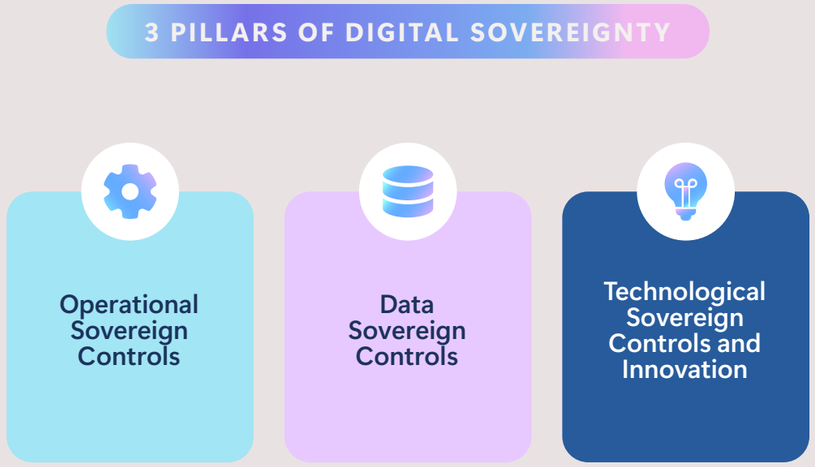
Blue Soft cut its infrastructure's carbon footprint by 55% after moving all servers to Microsoft Azure. This shift not only benefits the environment but also reduces long-term costs through lower energy use. Hyperclouds can help mitigate risks like energy obsolescence and regulatory non-compliance, supporting corporate sustainability goals.

# Microsoft Cloud in Europe: Sovereignty, Trust, and Resilience



In a context marked by rapidly evolving digital regulations, geopolitical uncertainties, and increasing sovereignty requirements, organizations—both public and private—must be able to rely on trustworthy technology partners. Microsoft offers a cloud platform tailored to meet the European leaders' expectations, balancing innovation with compliance, resilience, and operational control.

- Discover Microsoft's new digital commitments for Europe
- Learn how Microsoft cloud services protect your data and how to manage cloud data security and compliance for your organization




# A Strong and Lasting **European Presence**

Forty-two years ago, Microsoft released the very first version of Microsoft Word. It was a major milestone in the company's journey to enhance people's productivity through innovation. It also marked the young and growing company's first big step in Europe with the first Microsoft product localized in multiple European languages, starting with German and French.

Since then, our economic reliance on Europe has always run deep. We recognize that our business is critically dependent on sustaining the trust of customers, countries, and governments across Europe. We respect European values, comply with European laws, and actively defend Europe's cybersecurity. Our support for Europe has always been–and always will be–steadfast.

In a time of geopolitical volatility, we are committed to providing digital stability. Currently, the company is active in 16 European countries and operates in more than 70 cloud regions globally, with approximately 15 located in Europe. Microsoft intends to expand its cloud capacity in Europe by 40% by 2027.

Microsoft cloud services are provided through European legal entities, under local governance. A dedicated board of directors oversees cloud operations in Europe, ensuring alignment with the laws and expectations of EU member states.



# **Three Pillars** of Digital Sovereignty

### OPERATIONAL SOVEREIGN CONTROLS

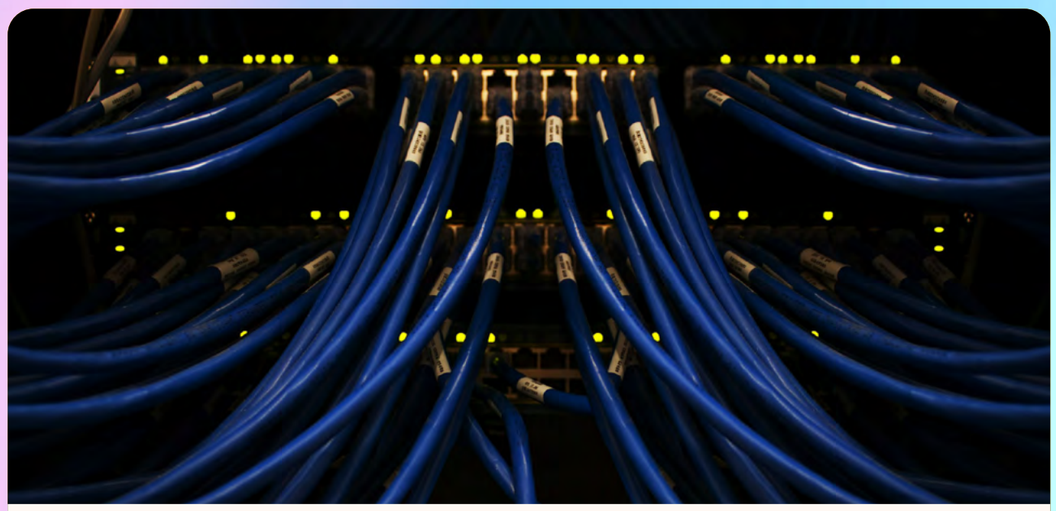
- Cloud operations are managed by staff based in the EU.
- The Data Guardian program ensures that only European employees can approve and supervise sensitive infrastructure access.
- Microsoft contractually commits to contest any injunction to suspend its services in Europe, including in cases of extraterritorial pressure.
- Continuity plans are in place with local partners, including secure source code transfer mechanisms.

### DATA SOVEREIGN CONTROLS

- At Microsoft, security is our top priority.
- All European customer data is stored and processed within the EU thanks to the EU Data Boundary initiative.
- Customers can manage their own encryption keys (Customer Key, External Key Management).
- Microsoft cannot access data without explicit authorization (Customer Lockbox and Data Guardian).
- The company is committed to legally defending data confidentiality against any request not compliant with European law.

### TECHNOLOGICAL SOVEREIGN CONTROLS AND INNOVATION

- Microsoft supports the European AI Act and adapts its services accordingly.
- Customer data is never used to train AI models without consent. AI tools remain accessible within a sovereign framework.
- Azure offers an open, interoperable ecosystem, integrating open-source models and European partners with confidential computing capabilities (e.g., Mistral AI).
- Governance, transparency, and filtering tools are integrated to ensure responsible and compliant AI.
- Azure and Microsoft 365 services are available with enhanced controls, without loss of functionality.
- Interoperability and portability: no exit fees, open-source support, compatibility with European standards.
- Sovereign Landing Zone blueprint enables secure, scalable workload deployment across Azure regions while ensuring regulatory alignment.



## Three Models of Sovereign Hosting

| Model | Platform | Usage |
|---|---|---|
| **Sovereign public cloud** | Microsoft (standard European public cloud with sovereign controls) | Sensitive data, GDPR compliance, no migration |
| **Sovereign private cloud** | Customer or local partner (Azure Local and M365 Local on private site) | Sensitive data, resilience, full autonomy, offline mode |
| **National partner cloud** | Local partner operator (e.g., Bleu in France, Delos in Germany) | National legal requirements, compliance with SecNumCloud v3.2 (France) |

These models are interoperable and based on a common platform (Azure, Microsoft 365), allowing clients to adapt their hosting strategy without technological disruption or high migration costs.

# **A strong and renewed commitment** to Europe's economic ecosystem

For more than 40 years, Microsoft has been contributing to the vitality of the European economy by supporting its digital transformation. Through a long-standing relationship within Europe, the company has consistently worked to foster innovation, develop skills, and address the major challenges facing our society.

- Training 6 million people across EMEA in AI-related skills in the next five years.
- Training 100,000 Europeans in cybersecurity through the European Cyber Skills Academy by the end of 2025.
- Major contributions to open source (2nd largest contributor to CNCF, founding member of Linux Foundation Europe).
- Targeting 100% renewable energy in European datacenters by 2025, with datacenters built from wood, low-carbon materials, equipment recycling, and transparency on environmental indicators.
- Providing consistent support to Ukraine in neutralizing cyberattacks, contributing to war crimes investigations, and providing financial support to humanitarian organizations.

# Digital Sovereignty: Risk Analysis and Microsoft Guarantees

A risk-based approach helps turn the idea of digital sovereignty into specific, practical concerns. For each area, it involves pinpointing threats, then evaluating their potential impact and setting up measures to reduce these risks along with minimum standards.

The aim is to achieve a practical balance between maintaining control and fostering innovation, so that organizations can safeguard their digital futures while still taking advantage of new cloud technologies.

In this perspective, Microsoft acts as a trusted partner in Europe: its cloud platform integrates sovereignty guarantees that allow clients to retain control (jurisdiction, data, security, resilience) while accelerating their digital transformation. The table below summarizes, for each of the five dimensions of digital sovereignty, the main risks identified, and the responses or solutions provided by Microsoft to address them.

| Main Risks | Microsoft Guarantees and Solutions |
|---|---|
| **Legal and Regulatory – Compliance and Jurisdiction (Legal framework, legal sovereignty)** | |
| **Non-compliance with European laws and regulations** (GDPR, sectoral directives), exposing the company to severe penalties or **extraterritorial injunctions** (e.g., the U.S. Cloud Act) that could force the disclosure of data outside Europe, threatening confidentiality and legal sovereignty. | Microsoft is **contractually committed to complying with all regulations** applicable to its activities, including the GDPR and the AI Act. We offer a **contractual defense commitment contesting** any access or suspension request not compliant with European law. |
| **"Data" – Mastery and Control of Information (Location, access, and data governance)** | |
| **Loss of control over strategic data:** unknown or non-EU location, indirect access by third parties, risk of leakage or unauthorized use of sensitive data.<br><br>**Lack of control over encryption:** if the cloud provider manages the keys alone, the company has no technical veto over access to its data (risk of unwanted access or breach of confidentiality). | With the ***EU Data Boundary*** initiative, **customer data is stored and processed within the EU** (local datacenters). Through **Customer Lockbox** and the **Data Guardian** program Microsoft **cannot access customer data without explicit authorization**.<br><br>***Customer Key*** and ***External Key Management*** allow organizations to provide and manage their own encryption keys. The provider cannot access clear text data, ensuring **end-to-end encryption** controlled by the client. |

| Main Risks | Microsoft Guarantees and Solutions |
|---|---|
| **Cybersecurity – Security and Digital Trust (Protection of systems and data against threats)** | |
| **Intrusion or sabotage via the cloud:** risk that a vulnerability at the provider compromises the company's systems or data (e.g., attacks on shared infrastructures, hijacked cloud accounts).<br><br>**Insufficient or unverifiable security level:** concern that external services may not be protected as strictly as internal ones (encryption, access controls, incident response).<br><br>**Doubt about the ability to audit and demand this level of security from a cloud provider.** | Microsoft applies **security standards at the highest industry level** (e.g., ISO 27001 certifications, external audits), and strictly **complies with European regulations** (GDPR, NIS2 directive, etc.).<br><br>Several billions yearly investments in cybersecurity to offer **advanced protection and proactive monitoring**, e.g. data encryption per default, multi-factor authentication, AI-driven intrusion detection, behavioral threat analysis, geo-redundant backups, confidential computing, etc.<br><br>Microsoft systems are continuously updated against new threats, reducing **residual cyber risk** for the client. |



| Main Risks | Microsoft Guarantees and Solutions |
|---|---|
| **Operational Resilience – Autonomy and Business Continuity (Dependencies, continuity in crisis)** | |
| **Critical dependence on a single provider – vendor lock-in:** risk of business disruption in the event of a serious failure by the provider (major outage, cyberattack, bankruptcy) or an external event blocking access to the service (geopolitical embargo, contract termination). Key question: "Can we continue our digital operations in the event of a major setback affecting our cloud provider?"<br><br>**Service interruption and loss of control:** if the infrastructure is beyond direct control, there is a risk of prolonged unavailability or service degradation without a backup plan (e.g., a cloud datacenter outage without sufficient redundancy).<br><br>**Technological lock-in:** difficulty migrating elsewhere or reverting, if no alternative solution is planned (prohibitive exit costs and delays, non-portable proprietary formats). | Microsoft cloud architecture is based on more than 70 datacenter regions worldwide, with a strong presence in Europe. Critical data and services can be **replicated redundantly across several European regions**. In case of disaster at one site, the load can switch to another region (*failover*), ensuring **uninterrupted business continuity**. This design **eliminates the single point of failure** and improves resilience compared to any isolated datacenter.<br><br>To avoid lock-in, Microsoft enables **data portability, no exit fees** and **compatibility with open standards**. Clients retain the freedom to migrate to another environment or adopt a **hybrid multicloud strategy**.<br><br>Microsoft offers **private sovereign cloud technology solutions** enabling customers to run cloud services on self-controlled/owned hardware. We have engaged in **local sovereign cloud partnerships** to address extreme scenarios. For example, in France, or Germany, agreements with local operators offer a **locally controlled cloud infrastructure** able to take over for clients with increased sovereignty requirements. Secure mechanisms for transferring code and data to these partners are in place, that, if needed, the company can **operate autonomously on a backup infrastructure**. |

| Main Risks | Microsoft Guarantees and Solutions |
|---|---|
| **Technological and Innovation (Technological choices, new capabilities, competitiveness)** | |
| **Dependence on non-sovereign technologies:** excessive reliance on foreign technological solutions, which can lead to a loss of strategic control (for example, if changes or terms of use are unilaterally imposed from abroad).<br><br>**Lag in innovation:** conversely, fearing the use of global cloud services out of a desire for absolute sovereignty can deprive the company of key innovations (AI, big data, latest-generation collaborative tools, etc.) and harm its competitiveness.<br><br>**The challenge is not to sacrifice innovation while maintaining control** (finding the right balance between technological self-sufficiency and blind adoption). | The Azure platform is designed to be **interoperable and open**. It natively supports many open-source tools and standards (containers, Linux, PostgreSQL, etc.) and even integrates advanced European technologies, e.g. **French open-source AI models** like *Mistral AI* can be deployed on Azure, also with confidential computing protecting algorithms.<br><br>Microsoft is one of the leading contributors to open source, strengthening **ecosystem trust** and avoiding proprietary lock-in.<br><br>Microsoft's cloud services provide **full access to cloud innovation** with **enhanced controls**. The **three hosting models** provide access to a wide range of **innovative services** in public cloud, private cloud and national sovereign environments.<br><br>Microsoft removes barriers to entry or exit, ensuring that adopting new technologies is **without risk of irreversible dependency**. |



**By applying a risk-based approach to digital sovereignty, organizations can establish a well-defined set of requirements—including data localization, managed encryption, compliance, and the ability to reverse decisions. This enables them to take advantage of both approaches: opting for local sovereign solutions when needed, while choosing global options where they offer significant benefits like scalability or advanced features.**

**With these guarantees, Microsoft acts as a strategic partner for European companies, providing a cloud that is secure, compliant, and sovereign, while maintaining innovation and competitiveness.**



# Conclusion

Digital sovereignty is not synonymous with autarky: it's a winning strategy that combines rigor and openness. By setting a clear framework—European data hosted locally, end-to-end encryption, strict access controls, transparency, and cloud service reversibility—companies can harness the best of both worlds: the security and compliance of trusted local clouds, combined with the innovation power and scalability of global solutions.

This positioning turns digital sovereignty into a true competitive advantage. Organizations that make this choice reduce their risks, strengthen trust with partners and customers, while preserving their ability to innovate and differentiate.

In an international context where each country imposes its own requirements, compliance becomes a major strategic challenge. This legal and operational risk calls for a structured response. Leveraging a hyperscaler then becomes a control mechanism: by facilitating local compliance in each jurisdiction, it enables companies to secure operations, reduce costs linked to regulatory fragmentation, and focus resources on innovation and performance.

By placing digital sovereignty at the heart of their strategy, European companies tackle cybersecurity challenges while opening new horizons. It's this subtle balance between control and openness that will allow them to fully harness digital opportunities, remaining sovereign over their choices and their future.