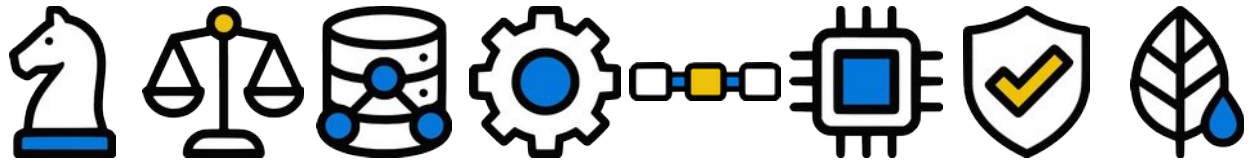
Microsoft Cloud Services Sovereignty Assessment Under the EU Cloud Sovereignty Framework



Technical analysis based on EC Cloud Sovereignty Framework v1.2.1 (October 2025)

Preface

Context and Methodology

BeLibre (belibre.be) is committed to supporting Belgian local governments and entrepreneurs in making informed decisions about digital sovereignty and cloud infrastructure choices. As part of this mission, we have repeatedly reached out to Microsoft representatives to understand how their cloud solutions perform under the European Commission's Cloud Sovereignty Framework.

Despite multiple requests across various forums and direct communications, Microsoft has not provided any form of assessment of their offerings against the EU Cloud Sovereignty Framework criteria. This absence of official guidance from Microsoft necessitated that we conduct our own independent analysis.

Note that while this research focuses on Microsoft, this is merely because it is currently the largest partner in Belgium public infrastructure by large. But **these structural ceilings are not unique to Microsoft and apply similarly to any US-jurisdictioned provider** (AWS, Google Cloud, etc.)

This assessment is published as a living document, subject to peer review and correction

Nature of This Document

This analysis is **not an authoritative or certified document**. It represents a **best-effort assessment** based on:

- Publicly available Microsoft documentation
- European Commission Cloud Sovereignty Framework v1.2.1 (October 2025)
- Public statements by Microsoft representatives (including testimony before the French Senate, July 2025)
- Independent technical research and analysis
- Industry reports and sovereign cloud taxonomies

We acknowledge that this assessment may contain gaps or interpretations that could be clarified with direct input from Microsoft. We remain open to corrections, additional information, or official SEAL assessments from Microsoft that would improve the accuracy of this analysis.

Invitation to Critical Evaluation

The EU Cloud Sovereignty Framework is designed to be **applied by organizations to their specific contexts and requirements**. We strongly encourage:

- **Belgian local governments and public institutions** to conduct their own SEAL assessments based on their unique workload classifications, risk tolerance, and regulatory requirements
- **Belgian entrepreneurs and businesses** to evaluate their cloud needs using this framework as a tool for informed decision-making
- **Technology providers** (including Microsoft) to publish their own SEAL assessments to provide transparency for their customers
- **Independent security researchers** to verify or challenge our findings

Sovereignty is not a one-size-fits-all concept. Different data classifications, organizational mandates, and operational contexts will yield different conclusions about appropriate cloud solutions. This document provides one analytical perspective to inform that broader conversation among Belgian decision-makers.

We believe transparency and open analysis serve the public interest. Digital sovereignty decisions affect local governance, citizen privacy, business competitiveness, and strategic autonomy for decades to come. These choices deserve rigorous, evidence-based evaluation.

Jurgen Gaeremyn
BeLibre
February 2026

For inquiries, corrections, or additional information: jurgen@belibre.be

Table of Contents

Framework Overview

The European Commission's Cloud Sovereignty Framework defines eight Sovereignty Objectives (SOV-1 through SOV-8) and five Sovereignty Effectiveness Assurance Levels (SEAL-0 through SEAL-4).

While these weights are a good starting point for a general reference, it’s obvious that these are merely indicative and may differ given the situation of your company, organization or government.

Furthermore, while environmental sustainability is an important goal, it’s difficult to frame this inside a cloud sovereignty context. Environmental sustainability should certainly merit its own place when assessing different solutions for your organization – and shouldn’t be shoved into this framework. This rather downplays the ecological impact of cloud solutions rather than acknowledges them.

These critiques aside, it is a decent basis to build an assessment when writing a public tender or asking for technical specifications.

SEAL Level Definitions

Level	Name	Definition
SEAL-0	No Sovereignty	Service under exclusive non-EU control, governed entirely in non-EU jurisdictions
SEAL-1	Jurisdictional Sovereignty	EU law formally applies; limited practical enforceability; non-EU operational control
SEAL-2	Data Sovereignty	EU law applicable and enforceable; material non-EU dependencies remain
SEAL-3	Digital Resilience	EU law enforceable; EU actors exercise meaningful but not full influence
SEAL-4	Full Digital Sovereignty	Complete EU control; subject only to EU law; no critical non-EU dependencies

Sovereignty Objectives and Weights

Objective	Description	Weight
SOV-1	Strategic Sovereignty	15%
SOV-2	Legal & Jurisdictional Sovereignty	10%
SOV-3	Data & AI Sovereignty	10%
SOV-4	Operational Sovereignty	15%
SOV-5	Supply Chain Sovereignty	20%
SOV-6	Technology Sovereignty	15%
SOV-7	Security & Compliance Sovereignty	10%
SOV-8	Environmental Sustainability	5%

Microsoft Cloud Service Configurations

Microsoft offers four deployment models with ascending sovereignty features:

Configuration	Key Features
Standard Public Cloud	Azure/M365 in EU regions; standard data residency
EU Data Boundary	Customer data, support data, pseudonymized data confined to EU/EFTA
Sovereign Public Cloud	Data Guardian (EU-personnel access control - announced; not yet GA); Sovereign Landing Zones; Level 1-3 controls
National Partner Clouds	Delos (Germany), Bleu (France); operated by local entities under national security frameworks

National Partner Clouds: conflicting legal grounds

A further source of concern is the **legal ambiguity created by overlapping EU and US obligations, and the way this ambiguity shifts liability from US technology vendors onto European intermediaries rather than removing US leverage**. National partner clouds such as Delos and Bleu are incorporated under EU or national law and led by EU-based management, but they remain technically and contractually dependent on Microsoft's proprietary cloud stack, which is ultimately controlled by a US-headquartered parent company subject to the US CLOUD Act, FISA and related surveillance and disclosure regimes. This structural dependency means that, even where day-to-day operations and data centres are located in the EU and staffed by EU nationals, the underlying software, update pipelines, control planes and support channels are still within the effective reach of US jurisdiction.

In this setting, requests from foreign (e.g. US) authorities can rest on **two competing legal bases**. On the EU side, instruments such as the GDPR (Articles 44–49), the Law Enforcement Directive, sector-specific secrecy rules, and forthcoming NIS2/DORA obligations restrict or condition any disclosure of personal or sensitive data to third countries, requiring an EU-lawful basis, appropriate safeguards, and in some cases prior authorisation or notification of supervisory authorities and affected data subjects. On the US side, the CLOUD Act and FISA can oblige entities with a

sufficient US nexus (including parents, affiliates, or contractual partners) to provide data or technical assistance, regardless of where the data is stored, and can be coupled with non-disclosure orders that explicitly prohibit informing the EU customer, the local operator, or regulators of the existence or scope of the request. The result is a **genuine conflict of laws**, not a simple hierarchy that a "strong" executive can resolve by preference.

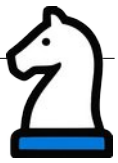
From a governance perspective, these arrangements **externalize the conflict of laws onto the European partner cloud and its management**. If local management prioritises EU law and refuses to comply with a US-based request, it may protect the immediate EU legal position of the public customer, but it simultaneously exposes the partner cloud, and potentially the upstream US vendor, to enforcement measures in the United States (e.g. contempt of court, fines, commercial retaliation). Conversely, if the partner silently facilitates access in response to US pressure, it risks violating EU data protection, secrecy and security obligations, and in sensitive domains even criminal provisions. This is not merely an abstract compliance issue: it raises the question of how far a commercial national partner will be willing to put a lucrative strategic collaboration at stake in order to resist, for example, a broadly framed "terrorism" or "national security" request. In practice, the **legal and personal risk is shifted away from the US technology provider onto the local partner entity and, ultimately, onto individual EU managers who must decide which legal order they are prepared to defy**.

From a sovereignty standpoint, this shows that national partner cloud constructions do not eliminate extraterritorial exposure; they **relocate it one organizational layer away from the US vendor, while preserving the underlying dependency on US-controlled technology and legal frameworks**. The residual uncertainty around how such conflicts would be resolved in concrete cases, and who would bear the consequences, is fundamentally at odds with the level of predictability and exclusive legal control implied by SEAL-4 for SOV-1 (Strategic Sovereignty) and SOV-2 (Legal & Jurisdictional Sovereignty).

Additionally, Delos Cloud and Microsoft signed a **Memorandum of Understanding** granting Delos legal rights to access and use Microsoft cloud software code if a government outside Europe restricts Microsoft's services for specific customers. Delos and Bleu also formed a **Franco-German mutual assistance alliance** for crisis scenarios including military conflict or large-scale cyberattacks.

SEAL Assessment by Sovereignty Objective

SOV-1: Strategic Sovereignty (15%)



Contributing Factors: Corporate ownership, governance location, EU financing sources, alignment with EU strategic priorities, resilience against service withdrawal.

Configuration	Assessment	SEAL Level
Standard Public Cloud	US corporate ownership; governance in Redmond; no EU board authority	SEAL-0 to SEAL-1
EU Data Boundary	Same ownership structure; EU operational commitments	SEAL-1
Sovereign Public Cloud	European advisory board; EU datacenter investment; no governance transfer	SEAL-1 to SEAL-2
National Partner Clouds	Local entity operation (SAP/Orange-Capgemini); EU governance for operations	SEAL-3

Even through National Partner Clouds, local entities can at best offer resistance and try to retain oversight in what the parent (US-based) company is doing. At no point will a Microsoft server (be it Azure as a host, or Microsoft Cloud services) be able to claim complete EU control.

SOV-2: Legal & Jurisdictional Sovereignty (10%)

Contributing Factors: Governing legal system, exposure to non-EU extraterritorial laws, channels for foreign authority data access, IP jurisdiction.

Configuration	Assessment	SEAL Level
Standard Public Cloud	Subject to US CLOUD Act; US courts can compel disclosure	SEAL-1
EU Data Boundary	Same legal exposure; EU data residency does not affect jurisdiction	SEAL-1 to SEAL-2
Sovereign Public Cloud	Data Guardian (announced; not yet GA) adds procedural friction; legal exposure unchanged	SEAL-2
National Partner Clouds	Local operator subject to EU law; Microsoft technology layer remains US-controlled	SEAL-2

Note: Extraterritorial laws

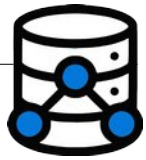
Multiple extraterritorial laws impact the legal jurisdiction. These laws apply to Microsoft regardless of data location, operational controls, or local partnerships. Procedural mitigation (Data Guardian, legal challenges) reduces risk but does not eliminate legal exposure. The fact that Microsoft testified it "cannot guarantee protection from valid US court orders" in the French Senate in July 2025, acknowledges this as a risk.

- **CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018):** Requires US-based companies and their subsidiaries to provide data stored on servers regardless of whether the data is stored in the US or on foreign soil. It applies to any provider of electronic communications or remote computing services subject to US jurisdiction.

- **FISA Section 702**: Requires US providers to give warrantless access to non-US citizens' data under vague "national security" pretexts. This applies regardless of data location and operates in secrecy. Affected entities may never be notified.
- **Executive Order 12333**: The foundational authority for NSA signals intelligence collection. Unlike domestic surveillance, overseas collection has no judicial oversight and limited congressional oversight. It permits bulk collection of foreign communications including those of EU citizens.
- **Patriot Act**: Also requires companies to hand over data at the request of US authorities regardless of physical location.

As much as Microsoft promises to object against possible requests, not only are they often bound to act – they are also bound to a gag order, not allowing to inform you of these invasions into domestic laws.

SOV-3: Data & AI Sovereignty (10%)



Contributing Factors: Customer cryptographic control, data access auditability, EU-confined processing, AI model governance under EU control.

Configuration	Assessment	SEAL Level
Standard Public Cloud	Microsoft-managed encryption; EU region storage	SEAL-1 to SEAL-2
EU Data Boundary	Data confined to EU/EFTA; Microsoft retains key access by default *(Microsoft reserves the right to transfer data outside the EU Boundary for "coordinated global security response" scenarios)*	SEAL-2
Sovereign Public Cloud (L2)	Customer-Managed Keys via Azure Key Vault Managed HSM	SEAL-2 to SEAL-3
Sovereign Public Cloud (L3)	Confidential Computing; data encrypted during processing	SEAL-3
National Partner Clouds	Local key management; confidential computing available	SEAL-3

Note 1: Metadata

Confidential Computing and Customer-Managed Keys in Azure primarily protect **payload data**, but **telemetry, logs, identities, traffic patterns, and access metadata** remain visible to Microsoft's control plane and often leave the confidential enclave. That metadata is typically processed in centralised Microsoft services (Azure AD / Entra ID, Defender, Sentinel, M365 telemetry) that was already classified under US jurisdiction in SOV-2. This means that if your metadata is significant, this check would negatively impact the SEAL-level.

Note 2: CoPilot processing location

Microsoft 365 Copilot expands in-country processing for Copilot Interactions to 15 countries by the end of 2026, including Switzerland. Yet, at this moment it is not available.

Note 3: "Harvest Now, Decrypt Later" (HNDL) Gap

This document discusses encryption (Customer-Managed Keys, Confidential Computing) as if current encryption provides permanent protection. However:

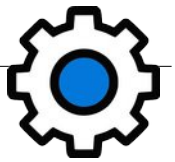
- Adversaries can intercept and store encrypted data today, waiting for quantum computing capabilities to mature.
- Once quantum computers reach sufficient capability, algorithms like Shor's will break current RSA and ECC encryption schemes.
- This means even data protected with today's strongest encryption (including Confidential Computing) may be compromised in the future if copies were captured.
- Furthermore, if implementation flaws in the cryptographic vault arise, a swift upgrade will not solve this, as older backups will be controlled by adversaries.

This fundamentally undermines the SOV-3 rating for Customer-Managed Keys and Confidential Computing. Taking this in account will also require an open source and auditable hypervisor stack.

Note 4: Authentication and IAM

Microsoft's Entra ID (formerly Azure AD) processes authentication and identity metadata centrally, and this service is **not covered by Confidential Computing enclaves** even in the Sovereign Public Cloud configuration.

SOV-4: Operational Sovereignty (15%)



Contributing Factors: Migration portability, EU operator capability, EU talent availability, EU-based support, source code/documentation access, subcontractor control.

Configuration	Assessment	SEAL Level
Standard Public Cloud	Microsoft-managed operations; limited customer operational control	SEAL-1
EU Data Boundary	Same operational model; geographic data restriction only	SEAL-1
Sovereign Public Cloud	Data Guardian (announced; not yet GA) requires EU personnel for access; support from EU locations	SEAL-2
National Partner Clouds	Local partner operates infrastructure; Microsoft provides technology	SEAL-3
Azure Local (on-premises)	Customer operates infrastructure; disconnected operation possible (currently in public preview)	SEAL-3 to SEAL-4

Maximum Achievable: SEAL-3 to SEAL-4 with Azure Local in fully disconnected mode. However, Azure Local still depends on Microsoft for software updates and security patches, creating residual dependency.

SOV-5: Supply Chain Sovereignty (20%)

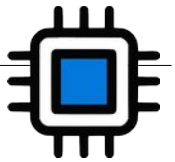
Contributing Factors: Hardware manufacturing origin, firmware jurisdiction, software development location, vendor dependency, supply chain visibility.

Configuration	Assessment	SEAL Level
All known Microsoft Configurations	Hardware: Intel/AMD (US), NVIDIA (US/Taiwan), storage (Asia)	SEAL-0 to SEAL-1*
	Firmware: Proprietary, US/Asian development	
	Software: Windows, Azure, M365 developed in US	
	Supply chain: Not auditable at component level	

Structural Limitation: Supply chain sovereignty is Microsoft's weakest dimension. No configuration changes hardware or software provenance. Even National Partner Clouds use Microsoft-developed software on globally-sourced hardware.

* **Note:** Hardware and Firmware will remain a problem, independent of the software or operating system running on these machines. While Open Source Hardware is not a factor at this point, it may very well become relevant in the future.

SOV-6: Technology Sovereignty (15%)



Contributing Factors: Open APIs/standards, open-source availability, architectural transparency, EU independence in computing capabilities.

Configuration	Assessment	SEAL Level
Standard Public Cloud	Proprietary APIs; vendor lock-in through Azure-specific services	SEAL-1
EU Data Boundary	Same technology stack	SEAL-1
Sovereign Public Cloud	Sovereign Landing Zone uses Azure landing zone accelerator (open deployment)	SEAL-1 to SEAL-2
National Partner Clouds	Same underlying technology; local operational wrapper	SEAL-2

Structural Limitation: Microsoft's core platform (Windows, Azure, M365) is proprietary. Source code is not available for customer audit or modification. Standards-based APIs exist but core services remain proprietary.

Maximum Achievable: SEAL-2. Full technology sovereignty (SEAL-4) would require open-source foundations, which Microsoft does not provide.

SOV-7: Security & Compliance Sovereignty (10%)

Contributing Factors: EU/international certifications, GDPR/NIS2/DORA adherence, EU-based SOC operations, breach reporting, patch autonomy, audit access.

Configuration	Assessment	SEAL Level
Standard Public Cloud	ISO 27001, SOC 2, extensive certifications; GDPR compliance	SEAL-2
EU Data Boundary	Same certifications; EU-confined compliance scope	SEAL-2 to SEAL-3
Sovereign Public Cloud	Customer Lockbox; EU-based security monitoring	SEAL-3
National Partner Clouds	Local SOC operations; BSI/SecNumCloud certification targeted	SEAL-3 to SEAL-4

Note: Extraterritorial laws and NIS2/DORA

The legal ambiguity discussed in SOV2, may render these systems unable to fulfil timely incident reporting and transparency obligations to EU regulators and data subjects. If a lawful access event is both (a) security-relevant from an EU perspective and (b) subject to a US gag order, the EU operator might technically be in breach of its own obligations without even knowing.

SOV-8: Environmental Sustainability (5%)

Contributing Factors: Energy efficiency, circular economy practices, carbon/water disclosure, renewable energy sourcing.

Configuration	Assessment	SEAL Level
All Microsoft Configurations	Commitments: 100% renewable by 2030; carbon negative by 2030	SEAL-2 to SEAL-3
	Microsoft's 2024 sustainability report showed a ~29% increase in Scope 1+2+3 emissions since 2020, driven largely by data centre construction and AI expansion.	
	Transparency: Annual sustainability reporting	

Microsoft has strong sustainability commitments but current trajectory shows increasing emissions. EU autonomy in energy sourcing will vary by datacenter location and will impact local peak energy availability.

Workload Classification Guidance

Based on the assessment, Microsoft services are appropriate for:

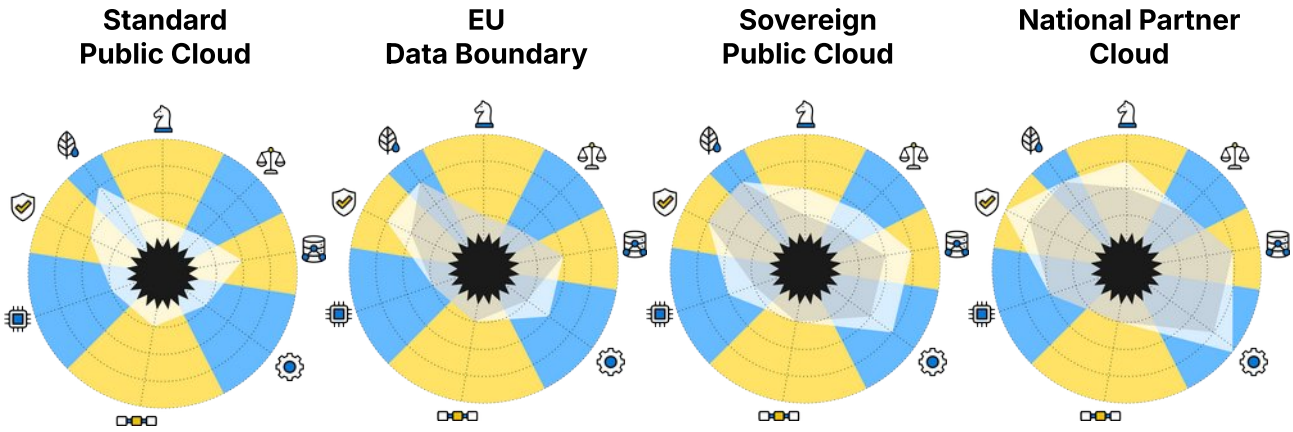
Data Classification	Required SEAL	Microsoft Capability	Recommendation
Top Secret	SEAL-4 all objectives	Cannot achieve (SOV-2, SOV-5, SOV-6 gaps)	Not suitable
Secret	SEAL-3 most objectives	Achievable for SOV-1, SOV-3, SOV-4, SOV-7; gaps in SOV-2, SOV-5, SOV-6	Conditional; assess risk tolerance
Confidential	SEAL-2–3	Achievable with Sovereign Public Cloud	Suitable with appropriate controls
Internal	SEAL-1–2	Achievable with EU Data Boundary	Suitable
Open	SEAL-0–1	Achievable with Standard Public Cloud	Suitable

Gap Analysis: What Microsoft Cannot Provide

Organizations requiring the following should evaluate alternatives:

1. **Complete legal immunity from US jurisdiction**: No Microsoft configuration eliminates exposure from extraterritorial intelligence laws.
2. **Auditable supply chain**: Hardware and core software provenance remains non-EU and non-transparent
3. **Open-source foundations**: Microsoft's platform is proprietary; source code not available
4. **Full operational independence**: Even Azure Local requires Microsoft for software updates
5. **EU-developed AI models**: Microsoft's AI stack (Copilot, Azure OpenAI) uses US-developed models

Conclusion



Legend: mapping the SEAL-levels for all 8 SOV domains in white. Light gray shows comparison with previous offering.

Objective	Weight	Standard	EU Boundary	Sovereign Public	National Partner	Maximum
SOV-1 Strategic	15%	SEAL-0–1	SEAL-1	SEAL-1–2	SEAL-3	**SEAL-3**
SOV-2 Legal	10%	SEAL-1	SEAL-1–2	SEAL-2	SEAL-2	**SEAL-2**
SOV-3 Data/AI	10%	SEAL-1–2	SEAL-2	SEAL-2-3	SEAL-3	**SEAL-3**
SOV-4 Operational	15%	SEAL-1	SEAL-1	SEAL-2	SEAL-3	**SEAL-3**
SOV-5 Supply Chain	20%	SEAL-0–1	SEAL-0–1	SEAL-0–1	SEAL-1	**SEAL-1**
SOV-6 Technology	15%	SEAL-1	SEAL-1	SEAL-1–2	SEAL-2	**SEAL-2**
SOV-7 Security	10%	SEAL-2	SEAL-2–3	SEAL-3	SEAL-3–4	**SEAL-4**
SOV-8 Environmental	5%	SEAL-2–3	SEAL-2–3	SEAL-2–3	SEAL-2–3	**SEAL-3**

According to analysis by BeLbre, Microsoft cloud services can meet sovereignty requirements for **Confidential, Internal, and Open** data classifications. They do not meet full sovereignty requirements for **Secret and Top-Secret** classifications due to structural gaps in SOV-2, SOV-5, and SOV-6. The relevance of SOV-8 is questionable with regards to data sovereignty but has been kept in account because it is part of the EC framework.

The SEAL-4 level on SOV-7 will only be achieved though if BSI/SecNumCloud certification is achieved and if the **US legislation gag orders** are considered as neglible.

BeLibre recommends organisations to implement **stratified procurement**: If needed, Microsoft services can be used for lower-classification workloads; European providers or self-hosted open-source for higher-classification workloads requiring SEAL-3+ across all objectives.

***Document Status**: Technical assessment based on EU Cloud Sovereignty Framework v1.2.1 (October 2025), Microsoft public documentation, and independent analysis. SEAL assignments represent framework-based evaluation, not official certification. Current as of February 6, 2026.*