



FACT SHEET

How to strengthen your digital sovereignty and security with Myra



How to strengthen your digital sovereignty and security with Myra

With the new EU Cloud Sovereignty Framework, Europe is establishing clear criteria to identify critical dependencies in IT landscapes and develop digitally sovereign cloud strategies. In addition, the assessment catalog facilitates comparisons between providers and exposes “sovereignty washing,” where service providers advertise their services as “digitally sovereign” even though this is not actually the case.

The framework thus serves as a decision-making aid for management in companies and public authorities, as well as a blueprint for their own evaluation systems to select cloud services. In this fact sheet, you will learn how Myra meets the EU’s sovereignty criteria and helps you make your cybersecurity more digitally independent.

SEAL rating system: Myra achieves high level of sovereignty

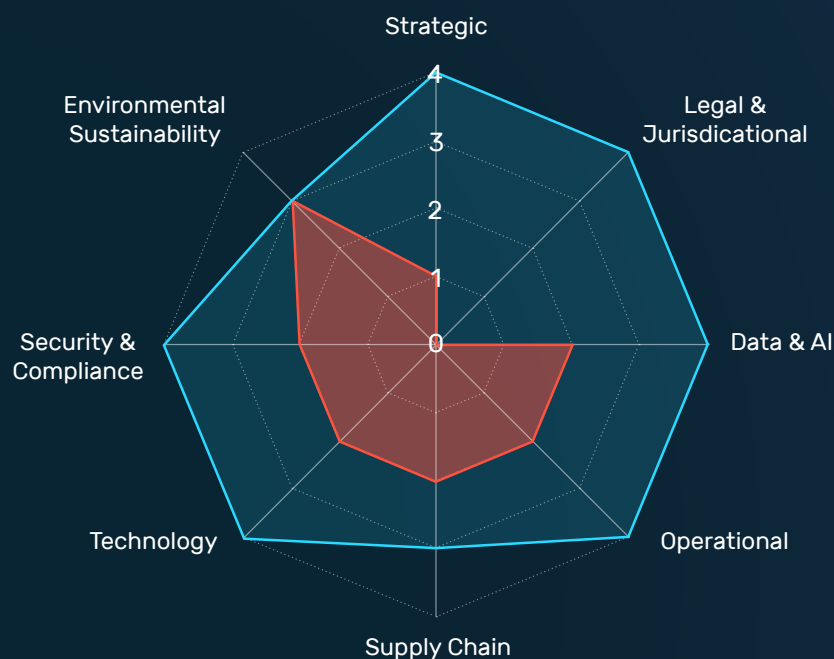
The EU Cloud Sovereignty Framework defines eight sovereignty objectives covering strategic, legal, operational, and technological aspects. These include control over data locations, protection from extraterritorial law enforcement, supply chain transparency, and technological independence for key components. The objectives are assessed using five Sovereignty Effectiveness Assurance Levels (SEAL) ranging from 0 (no sovereignty) to 4 (full digital sovereignty).

Myra meets almost all sovereignty criteria of the EU Cloud Sovereignty Framework

Comparison with typical competitors from outside the EU

● Myra Security

● Typical non-EU Provider



Methodology:

The eight sovereignty objectives (SOV-1 to SOV-8) were evaluated individually based on the influencing factors defined in the EU Cloud Sovereignty Framework v1.2.1 (as of October 2025) and assessed according to the SEAL system. The assessment of non-European competitors was carried out to the best of our knowledge and based on publicly available information and does not claim to be exhaustive or completely accurate.



“For providers outside the European Union, some of the criteria required by the Cloud Sovereignty Framework are simply impossible to meet – especially with regard to legal and jurisdictional sovereignty.

Dennis-Kenji Kipker

Professor of IT security law

& Research Director cyberintelligence.institute

Where Myra measurably stands out from non-EU providers

The following overview shows how Myra implements the objectives of the EU Cloud Sovereignty Framework.

Sovereignty Objective	Implementation by Myra
Strategic Sovereignty (SOV-1)	• Myra is an owner-managed company with exclusively European shareholders from the DACH region • Headquarters and seat of the entire management in Germany • No critical dependencies on customers or partners outside the EU • The protection services are developed and operated autonomously from Germany on our own hardware, independently of service providers
Legal & Jurisdictional Sovereignty (SOV-2)	• Myra is subject solely to German and European law • No possibility for non-EU authorities to force access to data or systems • No risk of usage restrictions due to international regulations • Creation of intellectual property, development, and operation exclusively in Germany in accordance with EU law
Data & AI Sovereignty (SOV-3)	• Myra customers always have full control over their data, its storage location and encryption, as well as insight into data access • Option for exclusive processing of data in German data centers – in full compliance with EU law such as the GDPR • Myra does not depend on any non-European technologies to provide its services

Sovereignty Objective	Implementation by Myra
Operational Sovereignty (SOV-4)	• Code and technical documentation are in-house developments, without dependencies on proprietary solutions • “Buy European first” purchase policy: Where available, Myra sources technology or services from Europe; Myra generally purchases from retailers in Germany • Operation, maintenance, and operational support are carried out exclusively by specialists from Germany and are subject solely to EU law • No vendor lock-in: Myra is not dependent on suppliers and could switch to other hardware or alternative data centers at any time
Supply Chain Sovereignty (SOV-5)	• Myra uses only standardized hardware and therefore does not risk vendor lock-in • “Buy European first” purchase policy: Where available, Myra sources technology or services from Europe; Myra generally purchases from retailers in Germany • More than 85% of the total code used to provide services is developed in-house in Germany or based on open source; the rest is BIOS/firmware from hardware manufacturers • Full transparency across the entire supply chain, including audit rights, in accordance with regulatory requirements such as DORA
Technology Sovereignty (SOV-6)	• Myra is its own hyperscaler with an independent global network of its own hardware • Support of open standards for integrations via Rest API, Terraform, Kubernetes, and others • Customers can flexibly adapt provided integrations independently of Myra • Full transparency for customers regarding the functionality and architecture of services, including data flow
Security & Compliance Sovereignty (SOV-7)	• Myra’s technology and the protection services it provides have been comprehensively tested, audited, and certified: BSI ISO 27001 based on IT-Grundschutz, BSI C5 Type 2, critical infrastructure certification in accordance with Section 8a (3) BSI Act, PCI DSS, IDW-PS 951 Type 2 (ISAE 3402), ISO 9001, Trusted Cloud • Legally compliant adherence to the strictest data protection and security requirements in accordance with GDPR, NIS-2, DORA, and other EU regulations • SOC operation from Germany under EU law • Customers have direct access to log files and monitoring functions

Sovereignty Objective	Implementation by Myra
Environmental Sustainability (SOV-8)	• The defense infrastructure is operated entirely with renewable energies (environmental management system according to ISO 14001, energy management system according to ISO 50001) • Myra has a core interest in operating its solutions as energy-efficiently as possible in order to reduce its carbon footprint and save costs (example: optimizing TLS/SSL encryption by changing the cryptography library has significantly reduced energy consumption and greatly reduced the carbon footprint) • Long hardware life cycle thanks to redundant infrastructure; decommissioned hardware continues to be used in internal test systems • In cooperation with ClimatePartner, Myra compensates for unavoidable emissions by supporting recognized climate protection projects

Why you should act now

Even though there are no legal obligations yet, we recommend that decision-makers take action now. The framework shows that the issue of “digital sovereignty” is at the top of the political agenda in Brussels. It is therefore high time to address this issue.

Analyze your IT landscape and reduce critical dependencies by gradually switching to digitally sovereign solutions. A good place to start is with areas that are highly business-critical but relatively easy to migrate, such as cloud-based application and infrastructure security. For highly critical areas that require greater migration effort, it is advisable to initialize the transition phase as soon as possible in order to tackle this in the next step.

Here's how you benefit from digitally sovereign cybersecurity with Myra:

- 1. Reliable cyber resilience:** Fail-safe availability and data security in line with European laws and values – without risks from political influence or foreign law
- 2. Preservation of data sovereignty:** Compliance with EU data protection standards builds trust and protects both customer and business data, for example thanks to GDPR-compliant TLS termination
- 3. Less regulatory effort:** More efficient implementation and verifiable compliance with national or European cybersecurity requirements such as NIS-2, DORA, or the Cyber Resilience Act (CRA)
- 4. Robust supply chain:** No abrupt price increases or access restrictions due to tariff wars, trade barriers, or other geopolitical developments

Made in Germany



Myra protects what matters. In the digital world.

Would you like to learn more about how our sovereign solutions can strengthen your digital independence, minimize your costs, and protect your web applications from malicious attacks? Our experts will be happy to advise you individually and develop a customized solution for your organization. Schedule a non-binding consultation today.

**Critical digital dependencies cost your freedom of action.
A non-binding consultation costs nothing.**

Myra Security GmbH



+49 89 414141 - 345



www.myrasecurity.com



info@myrasecurity.com