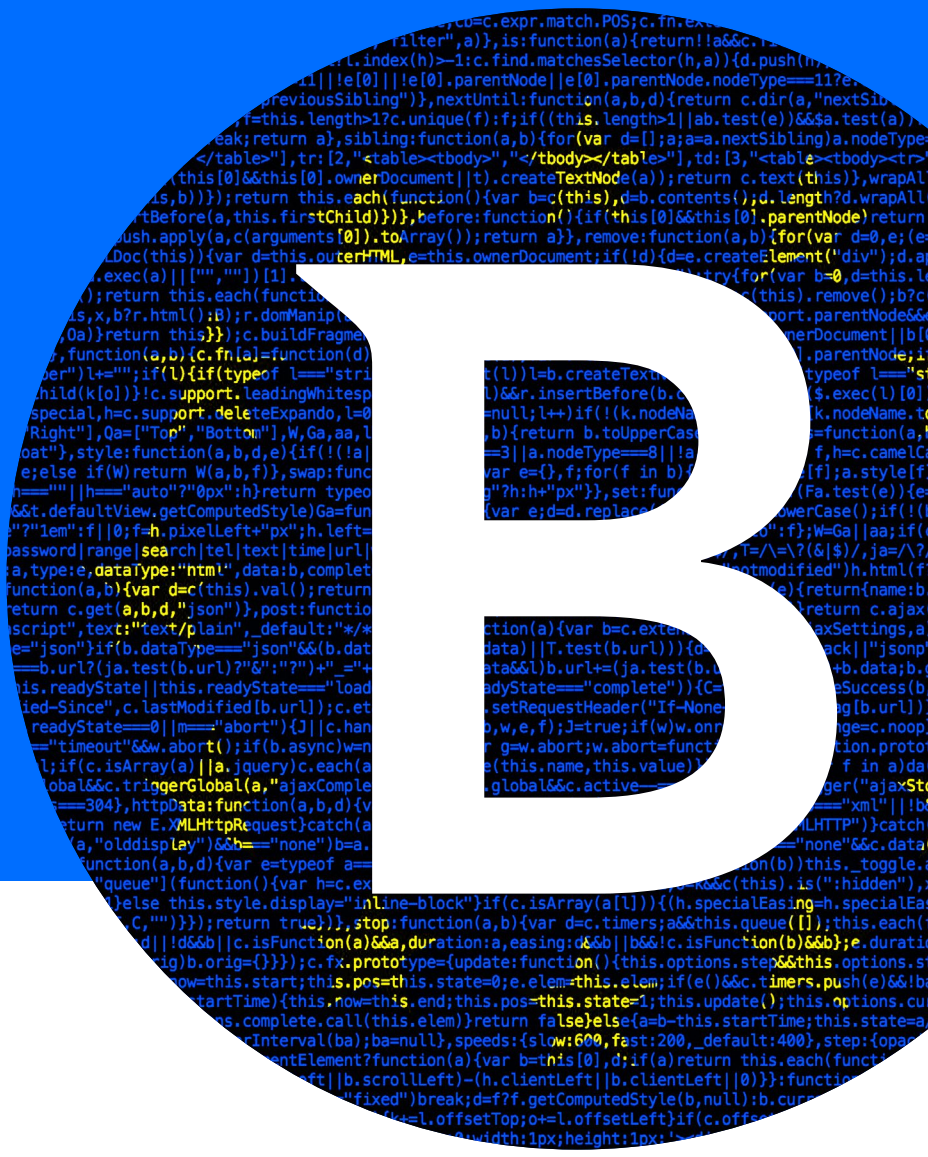
Bitdefender Global Leader In Cybersecurity

Mind the Gap: **How to Identify Cybersecurity Solutions That Are Truly EU Data Sovereignty Compliant**

WHITE PAPER



Today's cybersecurity platforms continuously collect, correlate, and analyze data across endpoints, identities, cloud infrastructure, SaaS applications, email, and networks. In the process, they touch some of an organization's most sensitive operational data, making questions of legal jurisdiction, governance, and operational control increasingly important.

As organizations place greater scrutiny on these issues, many vendors have responded by marketing their solutions as "EU sovereign" when they fall short of true sovereignty. These vendors are engaging in sovereignty washing, which gives buyers a false sense of security that their data is safe. But foreign ownership, offshore support teams, and hidden jurisdictional exposure leave buyers just as vulnerable as if the data were stored in another country entirely.

In this white paper, we'll define true data sovereignty. We'll also explore the hidden risks that sovereignty washing can expose your organization to, as well as the five questions you should ask a cybersecurity vendor to help distinguish real data sovereignty from marketing claims.

Defining True Data Sovereignty

True data sovereignty means that your organization governs, controls, and owns its data, with governance structured to minimize exposure to foreign extraterritorial legal access and keep data primarily subject to the laws of the jurisdiction you choose.

The European Commission's Cloud Sovereignty Framework, published in October 2025, provides buyers with a way to cut through vendors' claims about European data sovereignty. It scores providers against eight Sovereignty Objectives and rates them on a five-level scale (Sovereignty Effectiveness Assurance Levels, or SEAL), running from SEAL-0 (no sovereignty) to SEAL-4 (full digital sovereignty).

THE EIGHT SOVEREIGNTY OBJECTIVES ARE:

- SOV-1: Strategic sovereignty
- SOV-2: Legal and jurisdictional sovereignty
- SOV-3: Data and AI sovereignty
- SOV-4: Operational sovereignty
- SOV-5: Supply chain sovereignty
- SOV-6: Technology sovereignty
- SOV-7: Security and compliance sovereignty
- SOV-8: Environmental sustainability

A provider's overall SEAL rating is determined by its lowest score across all dimensions. That means buyers should not focus only on areas where a provider performs well. A single non-sovereign dependency, such as a SOC under foreign jurisdiction, a non-EU-managed encryption key, or an unauditable subcontractor, can reduce the provider's overall assurance level.

Their supply chain matters too; a vendor's evaluation and score must include its full chain of subcontractors and suppliers, not just the prime contractor. The vendor itself may have good sovereignty practices, but any chain is only as strong as its weakest link. Vendors must examine and account for the sovereignty practices of every link in their supply chain.

The Problem: **Sovereignty Washing in Cybersecurity**

Many vendors that claim "EU data sovereignty" aren't being 100% forthcoming, falsely equating European hosting with European sovereignty. Instead of being truly EU sovereign and only subject to EU jurisdiction and EU data rules, they may:

- Operate data centers in Europe while being headquartered elsewhere. This issue subjects your data to another country's laws; even though it's hosted in Europe and subject to EU jurisdiction, the company's non-EU headquarters means it's also under the jurisdiction of another country.

- Offer regional data residency without disclosing that your data can still be accessed by staff, systems, or legal orders originating outside the EU, thereby undermining your operational controls.

- Partner with local cloud providers while the underlying platform, support escalation, or parent company remains non-EU-controlled, meaning your data is subject to foreign extraterritorial access requirements.

EU hosting is not the same thing as EU sovereignty. Your data can be hosted on a server located in the EU, but if your provider is headquartered elsewhere, they're ultimately subject to non-EU laws, and so are any data and systems you host with them.

Phishing and Credential Theft: **The Quiet Entry Point**

Sovereignty washing is not just a labeling problem. It can expose your business to regulatory penalties, legal orders you never agreed to, and disruptions you cannot control.

1 Regulatory exposure:

If your data or systems are hosted with a non-sovereign provider, another country's jurisdiction may impose restrictions. For example, while GDPR protections will still apply, extraterritorial legal access can create conflicting obligations or control gaps, leaving your organization's data exposed. You are also putting your business at risk of falling out of compliance with NIS2, DORA, and national frameworks.

2 Unauthorized data access:

A non-sovereign vendor can be subject to legal orders outside the EU. Encryption reduces that risk only when the customer controls the keys and the provider cannot access, decrypt, or be compelled to use them. Buyers should confirm who holds the keys, who can initiate decryption, and which legal orders apply.

3 Operational dependency:

Non-sovereign providers remain subject to the laws, sanctions, and political decisions of their home country, not just the country where your data is stored. That means that during geopolitical or legal disruption, your service continuity depends on a decision made outside the EU. Being able to escalate a potential issue, send or receive service updates, or tap into incident response resources may be difficult or impossible, leaving your business without information or recourse during an already-tense time.

4 Loss of control:

With a non-sovereign provider, you have limited visibility into data access, AI usage, or other important system behaviors. They aren't required to disclose how your data moves through their systems or who touches it. Limited visibility can leave your organization unable to prove who accessed data, where monitoring occurred, or how AI systems handled information during audits, regulatory reviews, and vendor risk assessments.

5 Business continuity:

Organizations depend on cybersecurity platforms to maintain business operations during an incident. Losing access to your security services, support, or incident response due to geopolitical events affecting your non-sovereign provider poses operational risks that extend beyond cybersecurity concerns.

The Sovereignty Checklist

Use the checklist below to evaluate the core requirements behind a sovereignty claim. Each row helps buyers compare vendor proof against signs of sovereignty washing.

What to Check	Green Light (Real Data Sovereignty)	Red Flag (Sovereignty Washing)
Legal Jurisdiction	✓ Fully governed by EU law, with no exposure to foreign extraterritorial access	✗ Subject to non-EU jurisdiction, such as the CLOUD Act, even if EU-hosted
Data Control	✓ You hold the encryption keys, with full auditability of access	✗ The provider holds the keys, or access oversight is unclear
Data Residency	✓ Data is exclusively processed in the EU, with no fallback outside it	✗ Data sits in the EU but may be processed or accessed elsewhere
Operational Control	✓ EU-based teams run, maintain, and secure the platform independently	✗ Support, updates, or escalation rely on a non-EU vendor
Technology Stack	✓ Transparent and interoperable, built on open standards	✗ Proprietary stack controlled by a non-EU vendor
Supply Chain	✓ High transparency and auditability, minimal critical non-EU dependencies	✗ Hidden reliance on non-EU infrastructure, firmware, or software
Security Operations	✓ SOC, monitoring, and response are fully under EU jurisdiction	✗ Security operations are accessible or controlled from outside the EU
Continuity & Autonomy	✓ Service continues independently of any non-EU provider	✗ Updates or continuity are lost if the foreign vendor withdraws

Note:

- Green Light - *Real Data Sovereignty*
- Red Flag - *Sovereignty Washing*

How to Identify a True Data Sovereign Solution

As sovereignty claims become more common, how can you tell whether a vendor is truly EU-sovereign or just hosting services in Europe and calling it something more? Cybersecurity buyers should prioritize solutions that deliver:

1 EU jurisdiction:

Choose a provider that can demonstrate it is governed entirely by EU law and has no exposure to foreign authorities. Request governing-law documentation, ownership details, and confirmation that no non-EU parent can override operational or legal decisions.

2 EU operational control:

Insist on a provider whose security operations, support, and governance are controlled within Europe. Ask where SOC staff are located, which legal regimes govern them, and whether support escalation ever moves through a non-EU parent, vendor, or subcontractor.

3 Certified sovereign infrastructure:

Select a provider that hosts on trusted European cloud infrastructure backed by recognized sovereign cloud certifications and governed under EU jurisdiction. Certifications such as ANSSI SecNumCloud, Spain's ENS High, or equivalent sovereign cloud qualifications provide stronger evidence than data residency claims alone. Ask for certification documentation, the certification scope, and current audit reports showing which services, regions, and providers the certification covers.

4 End-to-end sovereignty:

Ensure the provider offers sovereignty across data, operations, technology, and supply chain. Review supplier and subcontractor disclosures, including hardware origin, firmware provenance, and audit rights for critical sub-suppliers.

5 Questions Every Buyer Should Ask

Before investing in a cybersecurity solution, ask these five questions. A vendor's inability or unwillingness to answer questions or provide product documentation should be seen as a warning sign rather than a formality worth overlooking. Solid providers should be able to document their answers and provide tangible proof of their claims.

1. Headquarters location:
Is your company headquartered and governed exclusively in the EU, and can you demonstrate that no foreign parent can override your operational or legal decisions?

2. Laws:
Which laws govern access to my data beyond GDPR? Specifically, are you subject to the U.S. CLOUD Act, FISA 702, or any equivalent extraterritorial instrument?

3. Encryption keys:
Who holds the encryption keys for my data, and under what legal circumstances could you or any third party decrypt it without my explicit authorization?

4. SOC location:
Where is your SOC located, and are all staff monitoring my environment subject solely to EU law?

5. Supply chain:
Can you provide a full supply chain disclosure, including hardware origin, firmware provenance, and sub-supplier audit rights, all the way to the component level?

When evaluating a cybersecurity platform, you must look beyond where data is stored. True cybersecurity sovereignty applies to the platform itself, including the security data it collects, processes, and uses during threat detection, investigation, and response. It combines data sovereignty, technical sovereignty, and operational sovereignty to ensure your cybersecurity operations remain governed, operated, and controlled under European jurisdiction. Together, these three dimensions help your organization strengthen cyber resilience, support regulatory compliance, and reduce exposure to foreign jurisdiction and extraterritorial legal risk.

Assessing these capabilities requires legal, operational, and supplier evidence that can be difficult to gather during a vendor evaluation. If you're uncertain where a provider stands, request a free Sovereign Risk Assessment to identify potential areas of exposure before making your decision.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071

T: +40 21 4412452