The EU Sovereign SASE buyer's guide

Contents

Foreword

SASE, or Secure Access Service Edge, replaces the traditional patchwork of networking and security tools with a single cloud-delivered service. As European regulations have tightened, a variant has emerged: sovereign SASE, which keeps the data, the management, and the operations of that service in region and under local jurisdiction.

The term "sovereign SASE" is everywhere right now. Three different things are being sold under that label: cloud SASE with European data centers, private SASE with regional data residency options, and sovereign SASE with full architectural and jurisdictional independence. The first two are legitimate products. Neither is sovereign SASE in the sense that EU regulatory frameworks define sovereignty.

This guide exists because the difference matters — and because the procurement process is where it gets decided. If your RFP requirements are written around data residency rather than the four dimensions of sovereignty, you will select a product that satisfies your checklist and fails your auditor.

The guide is structured in five parts. Part One defines the category correctly. Part Two maps the regulatory landscape to specific architectural requirements. Part Three explains the deployment spectrum and how to match it to your requirements. Part Four is the procurement checklist — the questions to ask, the evidence to require, and the red flags to disqualify. Part Five provides a structured vendor evaluation framework you can use as-is or adapt for your RFP.

Part One: What Sovereign SASE actually is

The problem with the current definition

Ask five vendors to define sovereign SASE and you will get five different answers, all of which describe their own product. The working definition that has emerged in most press coverage — SASE with in-country data processing and regional data residency — is accurate as far as it goes. It does not go far enough.

Sovereign cloud initiatives promise control. In practice, that control is frequently incomplete. Even when data resides within national borders, access to that data may still be mediated by centralised security or networking products located elsewhere. Security inspection may occur outside sovereign boundaries. Policies may be authored, updated, or enforced through non-sovereign systems. Logs and telemetry — which contain sensitive operational intelligence about your network — may replicate to vendor analytics infrastructure outside your jurisdiction without your explicit knowledge or consent.

Sovereignty cannot be guaranteed by storage and processing location alone. It depends on how access is granted, where traffic is inspected, who enforces policy, and who has visibility into the logs and performance data your systems generate. If sovereignty only applies when data is at rest, it fails the moment that data moves — which is precisely when risk increases.

The European Commission's Cloud Sovereignty Framework (v1.2.1, October 2025), now the de facto evaluation standard for EU institutional tenders and increasingly referenced in NIS2 and DORA procurement assessments, makes this explicit. It evaluates "the effectiveness of sovereignty, not just where servers sit." Its eight Sovereignty Objectives — from legal jurisdiction to operational independence to supply chain transparency — define what sovereignty requires in practice.

The four dimensions of true sovereign SASE

Sovereign SASE satisfies four distinct dimensions. Each is necessary. None is sufficient alone.

Dimension 1: Data Plane Sovereignty
Traffic is inspected and threat prevention occurs within the sovereign boundary. This means security gateways, inline inspection engines, threat intelligence processing, and content filtering all execute at points of presence physically and legally within the jurisdiction. No traffic is hairpinned outside the boundary for processing — not for advanced threat analysis, not for DLP inspection, not for any security function.

This is the dimension most vendors address. In-country inspection is real and meaningful. The challenge is that data plane sovereignty, standing alone, leaves three significant gaps unaddressed.

Dimension 2: Control Plane Sovereignty
Identity validation, policy evaluation, and access decisions occur within the sovereign environment. The system that decides who can access what — the zero trust policy engine — does not rely on external infrastructure to function. If the orchestration layer, the policy store, or the identity verification system sits outside the sovereign boundary, access decisions are being made by or through infrastructure outside your jurisdiction. A US court order compelling a US-operated orchestration service to alter or expose access policies reaches your sovereign environment through the control plane even if your data never leaves Frankfurt.

Dimension 3: Management Plane Sovereignty
Administration, logging, configuration, and telemetry remain under exclusive customer or authorised-sovereign-entity authority. Your tenant configuration — the sum of your security policies, user access rules, network topology, and security posture — resides within the sovereign boundary and is accessible only to parties you have explicitly authorised. Vendor support access is brokered through in-jurisdiction enforcement points: privileged access management systems hosted within the sovereign boundary, with mandatory multi-factor authentication, time-bound access windows, session recording stored in-jurisdiction, and cryptographic credential vaulting that prevents non-EU operators from ever holding plain-text credentials.

This is the dimension that most directly affects what "only I can see my data" actually means in practice. If your vendor's operations team can access your management plane from outside your jurisdiction — even temporarily, even with good intentions — your management plane is not sovereign.

Dimension 4: Jurisdictional Sovereignty
The service is governed by and operated under applicable local law. The contracting entity is legally domiciled within the jurisdiction. No foreign legal regime can compel access to the service, its configuration, its metadata, or its operational data through the vendor.

The US CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018) is the operative risk factor in European procurement right now. It compels US-domiciled providers to produce data in their control, regardless of where that data is physically stored. The key phrase is "in their control." If a US-headquartered vendor operates your control plane, your management plane, or your support access infrastructure — even in a European data center — that infrastructure is under their control and therefore potentially within US legal reach. No data processing agreement, no standard contractual clause, no contractual sovereignty assurance changes this. It is a structural legal exposure that only an architectural and jurisdictional solution can address.

The EU Cloud Sovereignty Framework names the CLOUD Act explicitly under its SOV-2 (Legal and Jurisdictional Sovereignty) objective as a risk factor that must be assessed and mitigated. It is not background context. It is a scored evaluation criterion.

The distinction that matters most

Sovereign cloud and sovereign SASE are complementary, not interchangeable. Sovereign cloud determines where data is stored. Sovereign SASE determines how data is accessed and protected — across users, devices, networks, and applications — as it moves. Together they form a complete sovereignty model. Separately, each leaves a gap the other cannot fill.

An organisation that has invested in sovereign cloud but uses a US-operated SASE platform to secure access to that cloud has data sovereignty at rest and a significant sovereignty gap in motion. The sovereign cloud investment is not wasted — it is incomplete.

Part two: The regulatory landscape and what it requires

Why the regulatory pressure is compounding

EU enterprises are not facing one sovereignty requirement. They are facing a layered and increasingly aligned set of obligations from multiple regulatory frameworks, each of which translates directly into specific architectural requirements for SASE. Understanding which framework applies to your organisation — and what it specifically requires — is the starting point for any sovereign SASE procurement.

NIS2 Directive (EU 2022/2555 — transposed nationally by October 2024)

NIS2 expanded the scope of critical infrastructure sectors significantly. Eleven sectors are now covered, including energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, ICT service management, public administration, and space. Management bodies are personally liable for cybersecurity failures.

The operative articles for SASE procurement:

- **Article 20 (Governance accountability):** Management bodies must approve and oversee cybersecurity measures. This creates demand for unified, auditable policy management with clear role-based access control and segregation of duties. Multi-vendor or stitched architectures that make governance visibility difficult create a direct Article 20 compliance gap.
- **Article 21(2)(a–j) (Risk management measures):** Covers risk policy, incident detection and response, business continuity, supply chain security, secure acquisition, effectiveness assessment, cryptography, access control, and multi-factor authentication. Each is a discrete procurement checklist item.
- **Article 21(2)(d) (Supply chain security):** Explicitly requires ICT supply chain controls, auditable subprocessor access, and data processed within EU-governed operational environments. Vendors with non-EU support teams accessing EU infrastructure without sovereign enforcement controls fail this article.

- **Article 23 (Incident reporting):** 24-hour early warning, 72-hour incident notification, and one-month final report to national CSIRTs. Buyers require tamper-evident timestamped logs and pre-built reporting workflows to support these timelines. Log storage outside the sovereign boundary creates a chain-of-custody problem for incident reporting.
- **Article 26 (Jurisdiction and territoriality):** Operations, data processing, and support must be governed under EU law. US-headquartered vendors contracting as a US entity, with operations governed under US law, have a structurally difficult argument to make here.

What NIS2 requires in a SASE deployment: In-boundary traffic inspection; unified policy management with RBAC and audit trails; supply chain documentation for all subprocessors; tamper-evident log storage within EU jurisdiction; incident reporting workflows with sub-72-hour capability; MFA across all access; and an EU-governed support model with documented access controls.

DORA (Regulation EU 2022/2554 — effective January 17, 2025)

DORA is in force. It applies to financial entities — banks, insurers, investment firms, crypto-asset service providers, payment institutions — and critical ICT service providers designated as systemically important. Unlike GDPR, DORA targets operational resilience, not primarily data protection. It cares whether ICT systems can be demonstrated to be secure, resilient, and auditable across the full supply chain.

The operative articles for SASE procurement:

- **Article 5 (Governance):** Management body accountability for ICT risk with RBAC and segregation of duties across all ICT functions. Unified platform visibility is directly advantaged — fragmented multi-vendor architectures create governance gaps that DORA auditors flag.
- **Article 9 (Protection and prevention):** Zero trust network access with continuous posture assessment, localized control plane with access decisions contained within sovereign boundaries. Access decisions made outside the sovereign environment are a documented risk under DORA's protection requirements.
- **Article 28 (Third-party ICT risk):** Oversight of technology providers including contractual requirements, audit rights, concentration risk assessment, and exit strategy documentation. Any SASE vendor whose own management plane is a third-party ICT dependency outside EU jurisdiction creates a recursive DORA compliance problem.
- **Article 29 (ICT concentration risk):** Financial entities must have operational transparency and reduced dependency on globally shared infrastructure. Vendors operating globally shared control planes are a concentration risk flag under DORA's own framework.
- **Article 30 (Key contractual provisions):** EU-governed operations, localized data processing, verifiable operational access controls, audit rights. A buyer contracting with a US entity for core ICT services faces difficulty defending Article 30 compliance. EU legal entity contracting matters here — not as a preference but as a compliance factor.

What DORA requires in a SASE deployment: All three planes (data, control, management) within sovereign boundaries; EU-governed contracting entity; documented ICT concentration risk assessment for all third-party dependencies; operational audit rights; exit strategy and data portability plan; RBAC and segregation of duties with audit trails; Threat-Led Penetration Testing (TLPT) telemetry retained in-jurisdiction.

Germany KRITIS (Kritische Infrastrukturen, IT-SiG 2.0)

Germany's critical infrastructure framework designates ten sectors — energy, water, transport, health, finance, food, IT and telecommunications, media, government, and space — as subject to heightened cybersecurity obligations under the BSI (Bundesamt für Sicherheit in der Informationstechnik).

Key requirements for SASE procurement:

- **State-of-the-art technical and organisational measures (TOMs):** BSI guidance defines current best practice. Generic "cloud-native" security architectures without in-country control plane governance do not satisfy the TOMs standard for KRITIS-designated operators.

- **Mandatory incident reporting:** Stricter timelines than NIS2 minimums. Pre-built SIEM integrations with tamper-evident audit trails and automated reporting workflows are a functional requirement, not a nice-to-have.
- **Attack detection systems (IT-SiG 2.0):** Real-time IDS/IPS, UEBA with MITRE ATT&CK framework mapping, and continuous monitoring across IT and OT environments — with all detection telemetry remaining within German or EU infrastructure.
- **What KRITIS requires in a SASE deployment:** BSI C5-aligned architecture; all detection and telemetry within German or EU jurisdiction; in-country data residency for logs and operational data; no replication to non-EU analytics backends; documented supply chain with bill-of-materials for all software components; OT/ICS protocol awareness for energy, water, and transport sector operators.

GDPR and the CLOUD Act problem

GDPR Chapter V restricts international transfers of personal data from the EU to third countries. Remote access to EU infrastructure from outside the EEA constitutes a "transfer" under GDPR and EDPB guidelines — even if the data is not physically moved. This means vendor support access from India, the US, or any non-EEA country to EU-hosted SASE infrastructure triggers GDPR transfer obligations and controls.

Standard contractual clauses (SCCs) are the operative fallback mechanism, but they require Transfer Impact Assessments (TIAs) and create ongoing documentation obligations. The better architectural solution is to route all non-EU support access through an EU-hosted privileged access management system — a sovereign enforcement point — that governs, logs, and time-bounds all access from outside the EEA. This eliminates the transfer problem structurally rather than managing it contractually.

Contracting through an EU legal entity — one that processes personal data under EU law, with EU-based data controllers — further reduces GDPR transfer risk. For EU public sector buyers and increasingly for regulated enterprises, this is becoming a hard requirement rather than a preference.

EU Data Act (Regulation 2023/2854 — fully effective January 12, 2027)

The EU Data Act targets cloud lock-in. It requires providers to facilitate switching between services, phases out egress charges for data portability, and mandates API and format portability for configurations, policies, and telemetry. Buyers are beginning to require exit strategy documentation and portability commitments in vendor contracts because from January 2027, non-compliance will be an enforceable obligation.

The practical implication for SASE procurement: any architecture where your tenant configuration, security policies, and operational logs are stored in a vendor-operated management plane creates a portability constraint that the EU Data Act directly addresses. The exit cost — in time, in operational disruption, and in the loss of historical telemetry — is a compliance risk, not merely a commercial inconvenience.

Part three: The deployment spectrum — matching model to requirements

Not every organisation needs the same level of sovereign architecture. The right model depends on your regulatory obligations, your operational capacity, your risk tolerance, and your strategic timeline.

The following spectrum — built on a single unified platform — covers the full range from cloud-delivered simplicity to fully air-gapped operational independence. The critical characteristic is that all four tiers run on the same platform, the same policy engine, and the same management interface. Moving from one tier to another does not require a platform change, a retraining investment, or a re-architecture of your security policies.

Tier 1: Unified SASE

Standard cloud-delivered SASE running on a shared global network of 100+ points of presence. Includes the full security stack. Best fit for enterprises with no sovereignty mandates or only light regulatory requirements. Traffic is inspected at the nearest location, while management runs on the vendor's shared infrastructure.

- **Appropriate for:** Enterprises operating primarily outside heavily regulated sectors; multinational organisations where the EU entity has a light sovereignty footprint; cloud-first organisations prioritising operational simplicity over jurisdictional independence.

- **Not appropriate for:** Any NIS2 Essential Entity, DORA-regulated financial entity, KRITIS-designated operator, or public sector buyer subject to EU institutional procurement standards.

Tier 2: Private SASE

Dedicated infrastructure reserved for a single customer within the vendor's locations. Better isolation and performance than the shared model, with options to keep data in a specific region. Management of the service, however, still runs on the vendor's infrastructure.

- **Appropriate for:** Enterprises needing tenant isolation and performance guarantees; organisations with data residency obligations but without strict jurisdictional sovereignty requirements; customers transitioning toward sovereign architecture who need an interim step.

Tier 3: Sovereign SASE as a Service

A fully managed sovereign service. Everything, including data handling, control, and management, runs on dedicated infrastructure in a sovereign EU data center, operated under EU law and contracted through an EU legal entity. Vendor support is only possible through an in-region access control system, and teams outside the EU have no direct access to the infrastructure.

This model delivers sovereignty without requiring the customer to build or operate infrastructure. It is the correct model for NIS2 Essential Entities, DORA-regulated organisations that require sovereignty but lack the resources or appetite to manage their own sovereign infrastructure, and regulated mid-market enterprises that need jurisdictional compliance with managed service simplicity.

- **Appropriate for:** EU regulated enterprises in financial services, healthcare, energy, and government-adjacent sectors; organisations subject to DORA, NIS2, KRITIS, or GDPR transfer restrictions; buyers who need EU legal entity contracting; organisations that want sovereign architecture without the capital expenditure of building sovereign infrastructure.

Tier 4: Sovereign SASE on-premises

Software deployed, hosted, and operated entirely on customer or partner infrastructure. Air-gapped capable — zero external vendor connectivity required for operation. Full feature parity with cloud deployments. Suitable for national telcos and service providers who want to deliver sovereign SASE as a managed service to their enterprise customers; national ministries of defence and classified government environments; and very large, complex, globally regulated enterprises with the resources to operate their own sovereign infrastructure.

- **Appropriate for:** National telcos and service providers; ministries of defence; banking; intelligence agencies; critical national infrastructure operators requiring full operational independence; very large regulated enterprises with dedicated security operations teams.

Matching model to regulatory requirement:

Regulatory obligation	Minimum appropriate tier
No specific sovereignty mandate	Tier 1 or 2
GDPR transfer compliance (operational)	Tier 3 (EU legal entity + JumpServer governance)
NIS2 Essential Entity	Tier 3 minimum; Tier 4 for highest criticality
DORA-regulated financial entity	Tier 3 minimum
KRITIS-designated operator	Tier 3 (BSI C5 aligned); Tier 4 for highest KRITIS criticality
EU CSF SEAL-2	Tier 2 with EU DC
EU CSF SEAL-3	Tier 3
EU CSF SEAL-4	Tier 4
Defence / classified / air-gap	Tier 4 only

Part four: The procurement checklist

These questions are structured around the four sovereignty dimensions plus EU Data Act portability. They should be submitted as formal RFP requirements. Acceptable responses are those backed by documentary evidence — architecture diagrams, responsibility matrices, legal entity documentation, certification scopes. Marketing assertions without supporting documentation should be treated as non-compliant responses.

Section A: Data Plane Sovereignty

1. **Where does traffic inspection occur for all inline security functions — including advanced threat protection, DLP, and RBI — for users accessing EU-hosted applications?**

   What you are looking for: Documented confirmation that all inline security processing occurs at PoPs within the EU, with no functions that hairpin traffic outside the jurisdiction for processing. Ask for a data flow diagram showing the inspection path for each security service.

   Red flag: Any function that routes traffic to a non-EU processing facility for analysis, even temporarily.

2. **Can the full security stack — NGFW, SWG, CASB, ZTNA, DLP, ATP, RBI — be deployed and operated entirely within the sovereign boundary?**

   What you are looking for: Confirmation that the sovereign deployment variant offers full feature parity with the vendor's standard cloud offering. Ask for a feature parity matrix comparing the sovereign variant to the standard offering.

   Red flag: Any features listed as "not available at launch," "cloud-only," or "requires cloud connectivity" in the sovereign deployment variant.

Section B: Control Plane Sovereignty

3. **Where does your orchestration and policy evaluation layer run? Specifically: does your management portal, SASE orchestrator, or equivalent operate on your own cloud infrastructure, a third-party cloud, or on customer/partner infrastructure?**

   What you are looking for: The answer to this question is in the vendor's own product documentation. Ask them to provide their deployment architecture diagram and their licensing/ordering guide showing the location of each component.

   Red flag: Any confirmation that the orchestration layer, management portal, or policy evaluation system runs on vendor-operated cloud infrastructure outside the customer's sovereign environment.

4. **Can your platform evaluate and enforce security policies without connectivity to your corporate infrastructure? For how long, and under what degraded-mode conditions?**

   What you are looking for: The ability to operate indefinitely without external vendor connectivity — for both normal operations and incident response. Air-gap capable platforms have no dependency on vendor connectivity for any function.

   Red flag: Any response indicating that connectivity to vendor infrastructure is required for policy synchronisation, identity verification, threat intelligence updates, or any other operational function.

5. **What happens to policy enforcement if connectivity to your orchestration layer is disrupted for 24 hours? 72 hours? Indefinitely?**

   What you are looking for: Documented behaviour under connectivity loss. Acceptable responses describe local caching of policies, local identity verification, and continued enforcement without degradation. This is directly relevant to DORA's business continuity and resilience testing requirements.

   Red flag: Any response indicating that policy enforcement degrades or fails under vendor connectivity loss.

Section C: Management Plane Sovereignty

6. **Who at your organisation has access to our tenant configuration, security policies, metadata, and logs? Under what conditions, through what controls, and subject to what legal framework?**

   What you are looking for: A documented access model showing: role definitions for vendor staff who can access customer environments; the technical controls governing that access (MFA, session recording, time-bound access, credential vaulting); the legal jurisdiction governing that access; and the process by which access is authorised, logged, and reviewed.

   Red flag: Any response indicating that access is governed by the vendor's internal policies without a documented customer-facing access model. Any response indicating that support staff have persistent access to customer environments.

7. **Are logs, telemetry, and audit records stored exclusively within the sovereign boundary? Are they replicated to any non-EU analytics, SIEM, or monitoring infrastructure?**

   What you are looking for: Confirmation that all logs, metadata, telemetry, session records, and audit trails are stored within the EU and are not replicated to non-EU infrastructure for any purpose — including vendor analytics, threat intelligence sharing, or product improvement.

   Red flag: Any replication of log data to non-EU infrastructure, including for purposes described as "aggregate" or "anonymised." GDPR guidance from the EDPB does not accept anonymisation as a basis for unrestricted international transfer.

8. **How is vendor support access from outside the EU governed? Specifically: is there a sovereign enforcement point (privileged access management system) operating within the EU through which all non-EU access is brokered?**

   What you are looking for: An EU-hosted PAM/JumpServer architecture with: no direct SSH or RDP access from non-EU infrastructure to EU environments; mandatory MFA for all access sessions; session recording stored within the EU in immutable or WORM format; credential vaulting ensuring credentials are never exposed to non-EU operators; time-bound, approval-based access with dual-control requirements for high-risk actions; and an EU-resident approver in the access authorisation chain.

   Red flag: Any response indicating that support staff can access EU infrastructure directly from outside the EU without brokering through a sovereign enforcement point. "We use VPN" is not an equivalent control.

9. **Can session recordings and access logs be disabled or deleted by non-EU operations staff?**

   What you are looking for: Confirmation that session recordings and audit logs are immutable and cannot be modified or deleted by vendor staff, particularly non-EU operations teams.

   Red flag: Any operational capability for non-EU staff to modify, disable, or delete audit records.

10. **Who holds the root certificate authority and encryption key management for the sovereign deployment? Can keys be managed by customer-operated HSMs?**

    What you are looking for: BYOK (Bring Your Own Key) or HYOK (Hold Your Own Key) support with customer or nationally operated HSM integration. The EU CSF SOV-3 requirement is explicit: only the customer, not the provider, should have effective control over cryptographic access to their data.

    Red flag: Vendor-managed root CA or encryption keys without BYOK/HYOK option.

Section D: Jurisdictional Sovereignty

11. **What is the legal entity through which this service is contracted for EU customers? In which jurisdiction is that entity domiciled, and under which national law does it operate?**

    What you are looking for: An EU-domiciled legal entity — specifically one registered and operating under the law of an EU member state — as the contracting vehicle. Contracts with US-domiciled entities, even for services delivered in the EU, carry CLOUD Act exposure through the contracting entity itself.

    Red flag: Any response confirming the contracting entity is incorporated in the United States, regardless of the location of delivery infrastructure.

12. **Has your legal team produced a CLOUD Act exposure assessment for your EU sovereign offering? Can you share the results or conclusions of that assessment?**

    What you are looking for: A documented legal analysis confirming that the vendor's sovereign architecture materially mitigates — or eliminates — the risk of compelled access by US law enforcement through the CLOUD Act. This should address: which entity operates the control plane; whether that entity is US-domiciled; what data that entity controls; and the legal basis for the assessment.

    Red flag: Any response asserting CLOUD Act immunity without legal analysis. Any response indicating the assessment has not been conducted.

13. **Are there any circumstances under which a non-EU government could compel your organisation to alter, disable, or expose access to a customer's sovereign SASE environment?**

    What you are looking for: A specific, legally grounded response addressing both the contractual and architectural basis for the vendor's answer. The architecture — not the contract — is what provides structural protection.

    Red flag: Any response relying solely on contractual assurances without architectural mitigation. Any response that does not directly address the CLOUD Act.

Section E: EU Data Act portability and exit

14. **If we choose to move to a different SASE provider, how do we export our tenant configuration, security policies, telemetry history, and log archives? What format, what timeline, and what vendor involvement is required?**

    What you are looking for: A documented, low-friction exit process. Configurations and policies exportable in standard formats without requiring vendor involvement. Log archives exportable in full without data loss. Timeline under 30 days for complete tenant export. No dependency on the vendor's platform or staff to execute the migration.

    Red flag: Any response indicating that tenant migration requires significant vendor involvement, cannot be completed without platform access, or involves data loss for historical telemetry.

15. **Are there any technical dependencies — proprietary hardware, vendor-specific firmware, non-standard protocol implementations — that would increase the cost or complexity of migrating to a different provider?**

    What you are looking for: A software-centric architecture running on standard hardware with well-documented, non-proprietary APIs. No dependency on vendor-specific appliances, firmware, or protocol implementations that would create exit costs.

    Red flag: Proprietary hardware requirements (specific vendor appliances, vendor-branded edge devices) without standard hardware alternatives.

16. **Under the EU Data Act, what is your documented commitment to portability, switching facilitation, and egress cost elimination? When will you be in full compliance with the January 2027 requirements?**

    What you are looking for: A specific, time-bound commitment to EU Data Act compliance with documentation of current portability capabilities and a roadmap to full compliance by January 2027.

    Red flag: Any response that cannot commit to a specific EU Data Act compliance timeline, or that treats portability as a commercial negotiation rather than a regulatory obligation.

Section F: Operational resilience and support model

17. **What is the process for emergency (break-glass) access to our sovereign environment — for example, during a major incident requiring vendor involvement outside normal support procedures?**

    What you are looking for: A documented break-glass procedure that maintains sovereign governance even under emergency conditions. Acceptable responses describe: a pre-approved emergency access protocol; dual-control authorisation with an EU-resident approver; immediate post-incident audit and review; and automatic access revocation after a defined period.

    Red flag: Any emergency access procedure that bypasses the sovereign enforcement point, disables session recording, or requires the customer to grant temporary unrestricted access to vendor staff.

18. **What is your business continuity and disaster recovery architecture for the sovereign deployment? Where are recovery systems located, and under whose jurisdiction?**

    What you are looking for: Active-active or active-passive HA within the sovereign boundary. Backup and recovery infrastructure located within the EU. Recovery procedures that do not require connectivity to non-EU vendor infrastructure. Recovery time objectives that satisfy DORA's ICT continuity requirements.

    Red flag: Disaster recovery infrastructure located outside the EU, or DR procedures that require connectivity to non-EU vendor infrastructure for restoration.

19. **For OT-dependent KRITIS sectors (energy, water, transport): does your sovereign SASE deployment support OT protocol inspection and IT/OT segmentation within the sovereign boundary?**

    What you are looking for: Deep packet inspection for OT protocols including Modbus, DNP3, IEC 60870-5, and PROFINET. Purdue Model-aware network segmentation. Passive OT asset discovery. All OT monitoring and telemetry retained within the sovereign boundary.

    Red flag: Any response indicating that OT inspection requires connectivity to a cloud-based threat intelligence or analytics platform outside the sovereign boundary.

Part five: Vendor evaluation framework

The following framework is designed to translate procurement checklist responses into a structured, comparable evaluation. It maps to the EU Cloud Sovereignty Framework's SEAL methodology and can be submitted as an evaluation annex to a formal RFP.

Scoring approach

Each dimension is scored 0–3:

- **0 —** Does not meet requirement: The vendor's architecture or legal structure cannot satisfy this dimension. No contractual assurance resolves the gap.
- **1 —** Partially meets requirement: The vendor satisfies some elements of this dimension but with documented gaps or caveats.
- **2 —** Meets requirement with conditions: The vendor satisfies this dimension subject to specific contractual or operational conditions that must be verified.
- **3 —** Fully meets requirement: The vendor satisfies this dimension architecturally, with documentary evidence, without requiring contractual workarounds.

Evaluation dimensions and weighting

Dimension	Checklist questions
Data plane sovereignty	Q1, Q2 — 15%
Control plane sovereignty	Q3, Q4, Q5 — 20%
Management plane sovereignty	Q6, Q7, Q8, Q9, Q10 — 20%
Jurisdictional sovereignty	Q11, Q12, Q13 — 25%
EU Data Act portability	Q14, Q15, Q16 — 10%
Operational resilience	Q17, Q18, Q19 — 10%

The weighting places highest combined emphasis on control plane, management plane, and jurisdictional sovereignty (65% combined) reflecting the EU Cloud Sovereignty Framework's own scoring, which places the heaviest weight on strategic, legal, operational, and supply chain sovereignty objectives.

Conclusion: Architecture determines sovereignty

Data residency is a necessary condition for sovereignty. It is not a sufficient one.

The regulatory frameworks governing EU enterprises in 2026 — NIS2, DORA, KRITIS, GDPR, and the EU Cloud Sovereignty Framework — have converged on a definition of sovereignty that goes significantly beyond where servers sit. They require control plane independence, management plane exclusivity, operational governance under EU law, and jurisdictional insulation from foreign legal compulsion. These are architectural requirements. They cannot be satisfied by contractual assurances, data processing agreements, or the presence of a data center in Frankfurt.

The procurement checklist and evaluation framework in this guide are designed to surface the architectural reality behind vendor sovereignty claims. Every question in Section D — jurisdictional sovereignty — has a binary answer: either the contracting entity is EU-domiciled or it is not, either the management plane is outside US legal reach or it is not. Vendors who have genuinely built for sovereignty will welcome these questions. Vendors who have marketed geographic residency as sovereignty will struggle to answer them with documentary evidence.

The gap between "data at rest in the right country" and "data governed by the right legal framework, accessed under the right controls, protected by architecture rather than contractual promise" is the gap that sovereign SASE exists to close. It is also the gap that a well-constructed procurement process will expose — and that this guide is designed to help you find before you sign.

Published by Versa Networks B.V., a Netherlands-based legal entity. Versa Networks offers Sovereign SASE across a full deployment spectrum — Unified SASE, Private SASE, Sovereign SASE as a Service (Germany, noris network), and Sovereign SASE On-Premises — on a single unified platform. For more information: versa-networks.com/sovereign-sase

This guide is produced for informational purposes. Nothing in this document constitutes legal advice. Organisations should consult qualified legal counsel for jurisdiction-specific regulatory assessments.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa

Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security.

Part# BG_EUSOVSASE-01.0