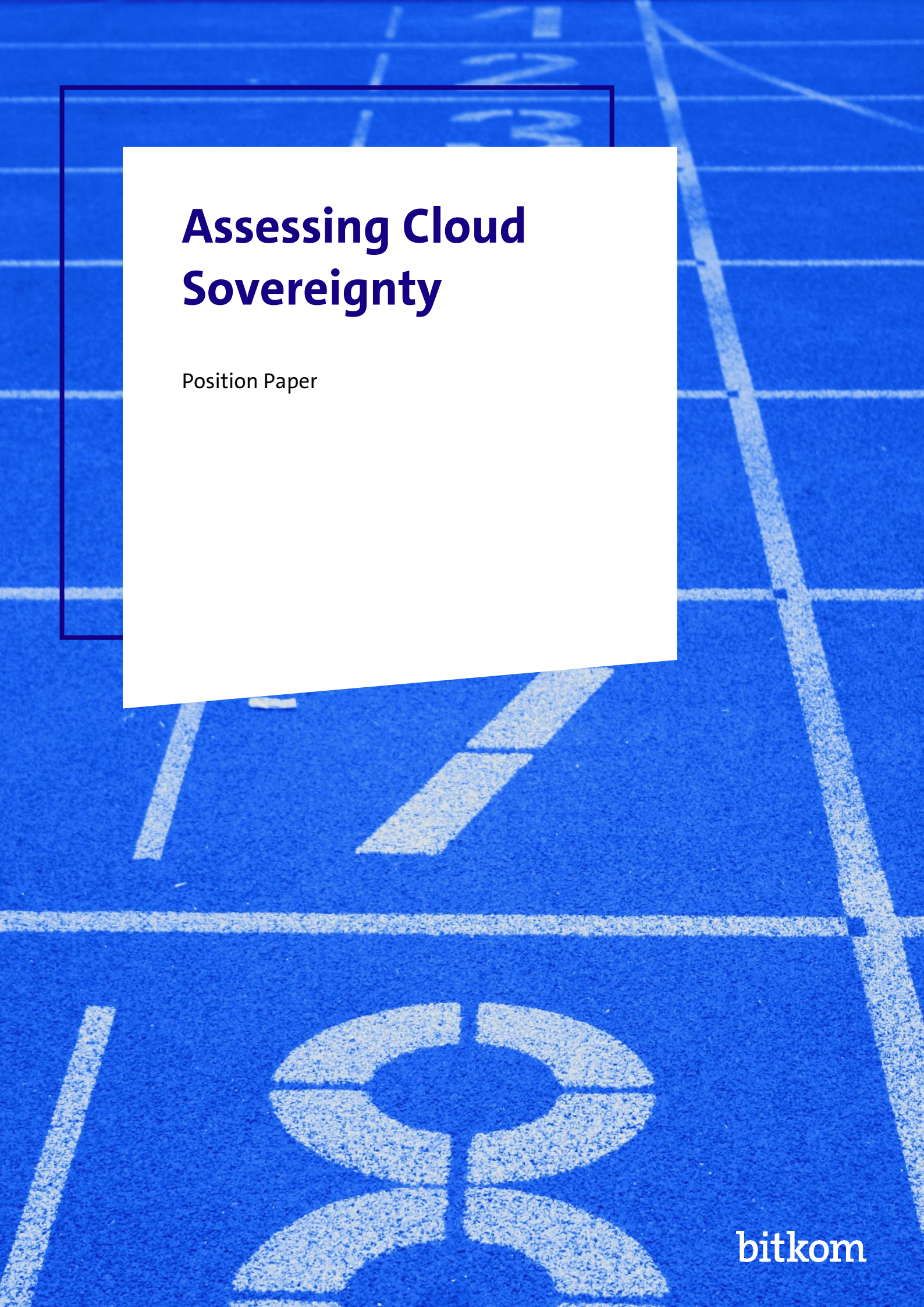

Assessing Cloud Sovereignty

Position Paper

bitkom

Bitkom Position on Cloud Sovereignty Criteria in Europe

This paper provides a perspective on approaches to defining and assessing cloud sovereignty criteria in Europe.

Status Quo

The European Commission's Cloud Sovereignty Framework (Version 1.2.1, October 2025) [1] sets out a new system to evaluate the »sovereignty« of cloud services. It defines eight Sovereignty Objectives within this framework, ranging from strategic and legal sovereignty to supply chain, technology, and operational control, and introduces five Sovereignty Effectiveness Assurance Levels (SEAL 0–4) that measure the degree of EU control. Providers are scored accordingly, and their results contribute to procurement decisions through a weighted Sovereignty Score.

The framework was recently being applied to a single, large-scale procurement procedure worth around EUR 180 million. While originating from a procurement context, the analysis focuses on the broader policy implications of applying cloud sovereignty criteria beyond individual tenders. In this regard, it may become a key reference point for upcoming initiatives such as the planned publication of the EU's Cloud & AI Development Act (CADA) and revised Regulation 2012/1025, and the ongoing review of the EU procurement directives or national policies such as Germany's sovereign cloud strategy.

The German Federal Office for Information Security (BSI) recently published »Criteria Enabling Cloud Computing Autonomy (C3A)«[2], a set of cloud sovereignty criteria grounded in the EU Cloud Sovereignty Framework. This demonstrates that approaches to sovereignty assessment are already used beyond individual procurement frameworks and suggests the increasing relevance of such criteria in shaping future approaches to digital sovereignty in Europe.

Bitkom welcomes ongoing efforts to bring greater transparency and clarity to the assessment of cloud sovereignty, as this is beneficial for both providers and users. Differing definitions, criteria, and certification approaches across jurisdictions create complexity and make it difficult to assess and compare cloud offerings in a consistent way.

[1] ↗Cloud Sovereignty Framework | European Commission
[2] ↗BSI - Presse - C3A: BSI veröffentlicht Souveränitätskriterien für Cloud-Dienste

Recent Bitkom data[3] underline both the relevance and the complexity of the issue: 78 percent of German companies express concerns about dependencies on a limited number of non-European providers, and nearly two thirds consider the location of data centres in Germany or the EU to be an important factor in provider selection. At the same time, companies are generally not willing to make trade-offs in terms of performance, functionality, or cost.

This highlights that measuring cloud sovereignty remains inherently challenging, as it encompasses a range of legal, technical, and operational dimensions, the relevance of which depends on the specific use case. A more coherent and harmonised approach at EU level can help address this fragmentation, improve comparability, and provide greater legal and operational certainty for all stakeholders.

Therefore, a European framework for cloud sovereignty can help set common guardrails that ensure a high degree of security and trust. These frameworks and their design and application should ensure an appropriate balance between sovereignty, openness, and competitiveness. Furthermore, alignment with global standards and the promotion of fair competition will ultimately determine whether these approaches empower or constrain Europe's digital ecosystem.

Challenges in Current Approaches to Measurable Cloud Sovereignty Criteria

Efforts to create transparency and comparability in assessing sovereignty are welcome, including the definition of different »sovereignty levels«. However, the practical implementation of these criteria should be as unbureaucratic and lean as possible. Overly complex compliance processes, documentation requirements, and structural separation measures could otherwise create bureaucratic hurdles that increase costs and complicate implementation unnecessarily.

As a matter of principle, any safeguards should be designed in a balanced, evidence-based, and proportionate manner, respect non-discrimination principles, and remain fully consistent with EU law. EU policy objectives, including those aimed at strengthening digital sovereignty, must be pursued in full compliance with the EU's binding international and reciprocal free-trade commitments, including obligations under the WTO GPA, GATS, and applicable bilateral and plurilateral trade agreements.

At the same time, requirements should be clearly defined and targeted, allowing for flexibility across different use cases while avoiding unnecessary complexity. Additionally, approaches should avoid excessive fragmentation across the ecosystem, as highly individualised or case-by-case assessment models may increase complexity, create legal uncertainty, and lead to additional implementation and compliance burdens for both providers and users.

Approaches to defining measurable cloud sovereignty criteria may combine minimum assurance requirements with different emphases on selected sovereignty dimensions.

[3] ↗Cloud Report 2025

Depending on their design, such approaches may favour providers with fully EU-based technology stacks.
While this can contribute to ensuring secure, resilient, and compliant operations in certain contexts, approaches to assessing cloud sovereignty should be adapted to the specific use case and context.
Accordingly, sovereignty assessments may consider a range of legal, technical, and operational factors, the relative importance of which depends on the specific use case. In this context, factors such as operational resilience, adherence to open standards, and multi-cloud portability can play an important role in enabling long-term digital sovereignty.
Overall, best-practice approaches to measurable sovereignty criteria should therefore remain **context-sensitive, combining clear minimum requirements with a balanced and use-case-specific assessment of different sovereignty dimensions**. Where appropriate, this could be supported by predefined, risk-based assessment schemes for different use cases, helping to ensure consistency, reduce complexity, and provide clearer guidance for both providers and users.

In addition, methodologies for measuring cloud sovereignty should provide clear and transparent criteria. Vague definitions and insufficiently specified factors risk inconsistent or subjective evaluations, thus must be avoided to ensure comparability. Sovereignty assessments should be based on clear and transparent criteria, while keeping implementation proportionate and avoiding unnecessary administrative burdens.

While the EU Cloud Sovereignty Framework, for instance, defines eight objectives, we generally recommend prioritising those with the greatest strategic leverage, such as:

- Data & AI Sovereignty
- Operational Sovereignty
- Technological Sovereignty & Cybersecurity
- Legal Sovereignty

Furthermore, the upcoming Cloud and AI Development Act, as well as relevant initiatives at Member State level, should promote a unified, streamlined, and harmonised approach across the European cloud market. Such models should reward demonstrable control, security, interoperability, and accountability, thus recognising technical, contractual, and organisational safeguards as valid ways to manage foreign dependencies.

Sovereignty assessment models should also be aligned with existing and upcoming policies.

Europe's digital sovereignty and competitiveness will depend on strengthening European capabilities while maintaining a framework of trusted openness in the digital ecosystem, supported by clear and enforceable rules. In this context, digital sovereignty should not be understood as technological autarky, but as the ability to make informed and independent choices. While existing and emerging sovereignty frameworks represent initiatives aimed at reinforcing trusted digital infrastructure in Europe, their contribution will ultimately depend on how they are implemented and how they interact with the broader cloud and digital policy landscape.

To ensure this, sovereignty definitions should be targeted and set a clear benchmark for the wider ecosystem. At the same time, in the private sector, the ultimate choice of the most appropriate cloud service for a specific use case should remain with the user.

We believe that genuine digital sovereignty requires that entities can choose, combine, and transition between technologies that best meet their needs while being able to manage dependencies.

Beyond sovereignty considerations, performance will remain a key factor for cloud users. This may include, for example, access to best-in-class or emerging technologies (such as advanced AI capabilities), as well as considerations related to cost, scalability, and the ability to participate effectively in global innovation ecosystems.

Ultimately, strengthening Europe's cloud ecosystem should focus on enabling a competitive environment that supports technological excellence and freedom of choice, underpinned by open standards, interoperable systems, secure infrastructure, skilled specialists, and reliable, diversified value chains.

This should be complemented by a clear and proportionate framework for control over operations and data, allowing different approaches to coexist depending on the use case.

Recommendations & Summary

Cloud sovereignty criteria should be understood primarily as a customer- or use-case-specific articulation of requirements rather than a one-size-fits-all instrument. A balanced approach could therefore combine sovereign solutions for particularly sensitive or critical workloads with the flexibility to adopt advanced and innovative technologies where appropriate. Sovereignty objectives should be assessed in relation to specific use cases rather than applied as uniform market-wide requirements. Assurance levels (such as SEAL or similar constructs) should therefore be aligned with the sensitivity and operational needs of different use cases, with higher levels reserved for clearly defined security-critical domains.

1. Adopt a risk-based sovereignty model

- Maintain **customer's freedom of choice.**
- Evaluate sovereignty objectives **per use case**.
- Ensure that public and private buyers can select, combine, and switch providers; **support multi-cloud, portability, and open standards**.

2. Recognise the role of technical controls and supply-chain resilience in sovereignty assessments

- Sovereignty frameworks should place strong emphasis on **verifiable technical and governance controls**, such as client-side encryption, key management, auditability (enabled by source-code transparency), and transparent corporate governance structures.
- Assessments of sovereignty characteristics should consider the realities of globally integrated supply chains and consider factors such as **control, access, security, and supply-chain resilience**, alongside proportionate localisation considerations where relevant.
  Cooperation models, including joint ventures, strategic partnerships, and co-development agreements, should be recognised as a complementary instrument that can reduce specific supply-chain dependencies (such as single-source concentration or restricted access to critical components) without resorting to market exclusion, provided they are accompanied by proportionate governance arrangements covering control, access, and accountability.

3. Ensure development of fair and non-discriminatory evaluation criteria

- Design assessment levels and related metrics in a way that maintains competition and preserves customer choice across the cloud ecosystem.
- Avoid **criteria or assessment designs that may lead to unintended exclusion of providers that demonstrably meet the relevant requirements** for the given use case, thereby reducing competition and customer choice.

- Ensure that **evaluation criteria and benchmarks remain aligned with current market and technical realities**, and that assessments of all available solutions are fair, objective, evidence-based, and grounded in demonstrated capabilities.
- **Clarify governance and review responsibility**: Clearly define which authority is responsible for setting and updating award criteria, with structured involvement of industry and trade associations to ensure market alignment, technical feasibility, and sustained competition.
- Ensure procurement frameworks remain **innovation-friendly**, cost-efficient, and non-discriminatory, while at the same time maintaining security standards appropriate to the relevant risk profiles.

4. Strengthen security through modern, evidence-based approaches

- Anchor sovereignty in **secure-by-design architectures, continuous monitoring, and threat-intelligence sharing.**
  - Reflect **modern cybersecurity practices** such as zero-trust architectures, secure data processing technologies (e.g., confidential computing), and continuous threat monitoring as core elements of sovereign cloud security, alongside clear governance and jurisdictional safeguards.
- When designing data localisation requirements, consider potential trade-offs in specific use cases, including possible implications for cross-border security operations and incident response, while ensuring coherence with ongoing EU simplification efforts, including the Omnibus package and the Data Act.
- Require **certifications**, **attestations**, and **compliance artefacts** to demonstrate adherence to the »contributing factors« (if included in the assessment).
  - **Use existing certifications and compliance artefacts where possible**: Allow providers to demonstrate adherence to contributing factors through existing certifications, attestations, and recognised compliance documentation, avoiding the creation of parallel certification schemes or labels.
  - **Enable reuse of trusted assessments**: Where appropriate, allow results from recognised third-party certifications or prior assessments to be reused across comparable contexts to streamline verification processes and enable providers to demonstrate their assessed sovereignty levels efficiently.

5. Ensure open and competitive markets

- Promote market rules that **foster competition** and avoid lock-in created by restrictive licensing practices.
- Recognise that active upstream contributions and **transparent open-source development models** can contribute to a high degree of software supply-chain certainty and global resilience.
- Enable users to select solutions that best fit their **risk profile, sovereignty needs, interoperability, and fair market conditions.**
- Support a **European cloud ecosystem built on trusted openness and inclusion.**

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Lucy Czachowski | Head of AI & Cloud – Resilience and Infrastructure
P +49 3027576-320320 | l.czachowski@bitkom.org

Responsible Bitkom Committee
WG Cloud Policy & Gaia-X