Business Software Alliance's
Response to the Digital Sovereignty Task Force

Stakeholder Consultation on Digital Sovereignty

June 2026

About BSA

The Business Software Alliance (www.bsa.org) is the global trade association of the enterprise software industry, representing companies that are leaders in artificial intelligence, cybersecurity, cloud computing, and other cutting-edge technologies. We work in over 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation.

BSA members[1] are global companies headquartered across the US, Canada, Europe, Asia-Pacific, and beyond, operating at the forefront of Europe's digital transformation.

BSA's Overall Position

BSA welcomes the work of the Franco-German Digital Sovereignty Task Force and supports the EU's ambition to strengthen its resilience, competitiveness, and technological capability. The concerns underpinning this consultation are legitimate: concentrated dependencies on a small number of providers, regardless of their nationalities or place of establishment, do create genuine risks — not just for public administrations, but across the wider economy, given that much of the legislation being discussed will apply far more broadly.

How Europe responds to those concerns, and which concrete criteria it retains to define sovereignty, matters enormously. BSA believes that genuine digital sovereignty is best achieved through openness, trust, and strong standards — not through isolation, geographic exclusion, or prescriptive origin-based requirements. As BSA's November 2025 paper "Keeping the Door Open: The EU's Path to Digital Sovereignty" sets out, what matters for Europe's sovereignty is the ability to govern, audit, and mitigate risk, not the geographic origin of each element. BSA's position is aligned with the recent conclusions of the European Transport, Telecommunications and Energy Council of December 5, 2025, whose section V is titled "reinforcing digital sovereignty in an open

[1] *BSA's members include: Adobe, Akamai, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systèmes, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.*

manner", emphasising the need for "close cooperation with (...) international partners (...) to ensure diversified, secure, resilient and trusted digital supply chains". Finally, BSA's views are aligned with the Declaration for European Digital Sovereignty from the French-German Summit of 18 November 2025 which provides that "Digital sovereignty does not mean isolation or protectionism; it means ensuring that Europe can act independently and in a self-determined manner based on international law, its own laws, values, and security interests, while thriving to international cooperation with its partners that share European values and principles".

BSA therefore urges the Task Force to adopt a trust-based, risk-based model that rewards demonstrable security, interoperability, and accountability, and that recognises technical, contractual, and organisational safeguards as valid ways to manage dependencies.

Section 1: Dimensions of Digital Sovereignty

1. Enforcement Capability (Q1–Q2)

BSA assessment: Partially suitable

BSA supports the principle that public bodies and organisations should have meaningful oversight of their digital dependencies. However, enforcement approaches should be grounded in risk and proportionality, not blanket jurisdictional exclusion.

- Jurisdictional transparency requirements are a reasonable and workable tool, provided they are proportionate and do not place excessive administrative burden on providers or procurers.
- Blanket legal exclusions of non-EU access to sensitive data risk conflating sovereignty with isolation. The EU should instead rely on strong contractual, technical, and legal safeguards — such as encryption and access controls — rather than geographic exclusion.
- BSA members already follow GDPR, NIS2, Data Act and other frameworks that provide robust enforcement mechanisms. These existing tools should be leveraged before new, duplicative requirements are imposed.

- Digital sovereignty frameworks should define the scope of "data" with precision. In modern SaaS services, customer content, identity data, metadata, logs, telemetry, support data, backups, and AI-related processing data serve different purposes and carry different risk profiles. Any data localization requirement should precisely identify the data categories, processing activities, access restrictions, retention expectations, and sub processor limitations in scope.

2. Capability to Design, Deploy and Use Technologies (Q3–Q4)

BSA assessment: Partially suitable, with important qualifications

BSA strongly supports investment in European digital capabilities, including in AI, cloud, cybersecurity, and quantum computing. However, "mastery" of technologies should not be interpreted as requiring Europe to develop or deploy exclusively European solutions.

- Global software companies are essential partners in Europe's digital transformation. BSA members invest substantially in European data centres, employ thousands of digital professionals across Member States, and deliver skills programmes in cybersecurity, cloud, and AI. The digital solutions offered support the competitiveness of European companies and the delivery of European objectives in the built environment, infrastructure, water, manufacturing industries, among others.
- Requiring organisations to transition exclusively to European technology competencies is impractical, costly, and would reduce security and innovation. Open-source is one valuable tool but should not be mandated as the default.
- Policy should focus on building capability, scale and choice, not on restricting the origin of technologies deployed.

3. Economic Value Creation Capability and Capacity (Q5–Q6)

BSA assessment: Partially suitable — significant concerns around implementation

BSA shares the EU's ambition to develop a competitive European digital economy. As the Draghi report underlines, accelerating AI and cloud adoption in European industry is critical to competitiveness. However, BSA has significant concerns about the approach proposed under this dimension.

- Linking sovereignty assessments to the territorial anchoring of value creation — including share of EU employment, location of R&D — risks functioning as a "buy European" mandate by the back door. This would undermine competition, raise costs for public administrations, and reduce choice.
- BSA members make substantial investments in Europe. Many operate major European data centres, hold large EU-based workforces, and contribute to local ecosystems. This investment is made because Europe is an attractive market, not because of mandate — and that attractiveness must be preserved.
- Public procurement frameworks should be designed around outcomes — security, performance, interoperability, value for money — not the geographic origin of service providers or location of corporate headquarters.
- Additionally, Documenting and reporting the share of EU-generated value added within a global technology product or service is operationally complex - if not impossible. Isolating and attributing value creation at a territorial level would create disproportionate compliance burdens, particularly for companies that already contribute substantially to the European digital economy.

4. Data Protection (Q7)

BSA assessment: Partially suitable, provided implementation is risk-based and technology-neutral

BSA strongly supports high data protection standards for sensitive data. The EU already has the most comprehensive data protection framework in the world, and BSA members follow GDPR, NIS2, and related obligations.

- Technical and organisational measures — encryption, pseudonymisation, access controls, contractual safeguards, and data localisation options — are effective and proportionate tools for managing extraterritorial risks.
- Mandatory use of specific privacy-enhancing technologies should be approached carefully: mandating particular technical solutions can create lock-in, reduce flexibility, and quickly become outdated as technology evolves.
- Trust is built through accountability and transparency, not through nationality. Protection against extraterritorial access can be effectively addressed through strong contractual, legal, and technical safeguards, applied proportionately according to the sensitivity of the data. European businesses should be able to opt for enhanced controls where needed rather than forcing all companies, including Saas, into the highest-cost model based on risks.

5. Substitutability and Interoperability of Systems (Q9–Q10)

BSA assessment: Particularly suitable — this is the most effective lever for sovereignty

BSA regards interoperability and open standards as the cornerstone of genuine digital sovereignty. Requirements in this area directly address lock-in risks and empower users to exercise real choice.

- The EU should promote open, internationally recognised technical standards — such as ISO 27001 — rather than developing parallel or exclusive European frameworks. This strengthens sovereignty while maintaining global connectivity.
- Modular system architectures and documented software bills of materials are practical, effective measures that BSA members can implement and support.
- Open-source solutions have an important role to play but should not be mandated. What matters is that systems are designed to avoid unilateral dependencies and vendor lock in (e.g. with multi-cloud environments) — this can be achieved through open standards, contractual switching rights, as well as technical interoperability and portability requirements.
- Standardisation cooperation with global partners — through ISO, IEC, and other international bodies — should be a priority to prevent fragmentation and ensure European standards carry global weight.

6. Infrastructure Resilience (Q11–Q12)

BSA assessment: Suitable, provided "trusted international partners" is interpreted broadly and based on risk criteria

BSA supports the development of resilient, trustworthy critical IT infrastructure. However, resilience is best achieved through diversity and redundancy — not through geographic restriction.

- Multi-cloud and hybrid approaches, combining European and international providers within a clear governance framework, offer more robust protection and resilience than geographic exclusivity. A single European cloud stack would itself create a dangerous concentration risk.
- The criteria for "trusted international partners" should be based on demonstrable security standards, legal safeguards, contractual commitments, and technical measures — not on the country of origin of the provider.
- BSA members building and operating European data centres and distributed Points of Presence already contribute directly to European infrastructure resilience. This investment is most effective when it takes place in a competitive, open market.

Additional Criteria and Remarks (Q13)

BSA wishes to highlight the following additional considerations:

- Regulatory coherence and simplicity: The digital sovereignty agenda must be pursued consistently with the EU's simplification agenda — the two are currently pulling in opposite directions. The existing regulatory framework — GDPR, NIS2, the AI Act, the Cyber Resilience Act — already provides a strong foundation to safeguard privacy and security. New sovereignty requirements should build on these rather than duplicate or conflict with them. Sovereignty frameworks that are overly complex, costly, or inconsistent with existing rules reduce choice, increase compliance costs, and divert investment away from growth and innovation. The upcoming tech sovereignty package should therefore be designed around simplicity and proportionality as core principles.
- Digital skills: Europe's long-term sovereignty depends on people as much as technology. Investment in digital skills — particularly in cybersecurity, cloud, and AI — must be a central pillar of any sovereignty framework.
- International alignment: Without some convergence at the international level, the risk is a patchwork of bespoke requirements that raises costs and ultimately serves no one well. The Task Force should consider how its proposals interact with international trade commitments and global standards frameworks.

Section 2: Focus on Indicators of Economic Value Creation

BSA has significant concerns about this section of the consultation. While presented as focused on "economic value creation" rather than ownership or capital origin, the indicators under consideration would in practice function as proxies for company origin — effectively disadvantaging non-European providers regardless of the quality, security, or competitiveness of their services.

Q1–2: Relevance of indicators

BSA recognises the relevance of assessing contributions to local ecosystems, technological development, and skilled employment as indicators of economic value. However, these should be used as positive indicators of contribution, not as exclusionary thresholds.

Additional indicators BSA would consider relevant include:

- Compliance with EU regulatory frameworks, security certification status, and demonstrated ability to provide secure, trustworthy, and scalable services in accordance with EU rules and values, including contractual commitments on data access, portability, and switching rights;
- Investment in innovation, cybersecurity, AI capabilities, and resilient infrastructure, including through partnerships with EU universities, research institutions, and technology companies, and through skills development programmes, apprenticeships, and educational partnerships that build EU digital capabilities at scale;
- Ecosystem multiplier effect: the economic activity generated within the EU by the provider's partner and reseller ecosystem, which in many cases significantly exceeds the provider's direct employment footprint;
- Participation in global research, open-source, and innovation ecosystems; and
- Supply chain resilience and diversification.

The assessment framework should remain technology-neutral and avoid approaches that could fragment markets, reduce interoperability, or limit access to globally competitive technologies and expertise.

Q3–4: Location of registered office and data hosting

BSA does not consider the location of a company's registered office to be a relevant or appropriate indicator of sovereignty value. The technology ecosystem is fundamentally global and highly interconnected, with many technology solutions conceived, developed, produced, and delivered through complex value chains involving multiple countries and regions. What matters is compliance with EU law, technical security

standards, and the practical ability of customers to exercise control over their data — none of which is determined by where a company is incorporated.

Data hosting location can be a relevant factor for specific high-sensitivity use cases, but should not be applied as a blanket requirement. Mandatory EU data localisation for all services would fragment the Digital Single Market, harm cybersecurity (by eliminating geographic redundancy), and weaken European firms' global reach. Moreover, requirements forcing data localisation solely for the sake of physical proximity can undermine cybersecurity and operational resilience. They may hinder cross-border threat intelligence sharing, increase the costs of maintaining state-of-the-art security solutions, and weaken resilience and failover capacity by limiting opportunities for alternative storage or rapid recovery in cases of outages, cyber incidents, or data loss.

Q5–11: Workforce, R&D, and subcontracting thresholds

BSA urges significant caution in the design of these indicators. Setting minimum thresholds for EU-based employment, R&D staff, or subcontracting expenditure as conditions for procurement eligibility would constitute a de facto origin-based restriction, regardless of how it is framed.

- Such thresholds risk being incompatible with the EU's international trade commitments, including under the WTO Government Procurement Agreement.
- They would reduce competition, drive up costs for public administrations, and may reduce rather than enhance security by limiting access to globally leading solutions.
- If indicators of this kind are to be used at all, they should be applied only as positive criteria in procurement scoring — never as eligibility thresholds — and only where genuinely relevant to the sensitivity and risk profile of the specific procurement. They should also avoid creating unnecessary administrative burdens for companies in Europe, in particular by refraining from introducing overly granular, product- or solution-level criteria.

Specifically, for each of the questions:

- **(Q5)** The presence within the European territory of critical support functions such as maintenance, operations, or level 3 support can be a relevant indicator for certain highly sensitive or critical use cases where users require stronger assurances regarding service continuity, operational control, and responsiveness. In these contexts, users may expect not only secure and trusted technologies, but also transparency, governance safeguards, and enforceable guarantees regarding continuity of service. However, the location of support functions alone should not be treated as a standalone criterion for measuring technological value added or digital sovereignty. What matters most is whether providers can ensure resilient, secure, and reliable services through objective technical, contractual, and operational safeguards.

- **(Q6)** No specific minimum threshold should be imposed. The location of employees alone is not a reliable measure of technological value creation in Europe, particularly in a globally interconnected technology ecosystem.

- **(Q7)** No specific minimum threshold should be imposed. R&D and innovation increasingly rely on global collaboration and access to international expertise. What matters most is the quality of innovation and the contribution to Europe's technological capabilities, rather than the geographic location of R&D personnel alone.

- **(Q8)** No specific minimum threshold should be imposed. Core technologies are increasingly developed through global and collaborative ecosystems, particularly in AI, cloud computing, cybersecurity, and open-source software. Rigid localisation requirements risk discouraging investment and limiting access to trusted expertise and innovation. Technological sovereignty should instead focus on strengthening Europe's resilience, capabilities, and competitiveness without creating unnecessary compliance burdens or barriers to growth.

- **(Q9)** The location of engineering teams within the EU should not, on its own, be considered a defining measure of technological value creation or digital sovereignty. The digital economy is global, and companies need access to international talent and expertise to innovate and compete effectively. Broad localisation requirements risk limiting access to critical skills and reducing competitiveness. Where sovereignty concerns are relevant, they should apply only to genuinely sensitive or strategic use cases. What matters most is how software and digital services are developed, secured, governed, and maintained, alongside continued investment in Europe's skills and innovation ecosystem.

- **(Q10)** No specific minimum percentage should determine whether a digital service contributes significantly to the creation of technological value added in Europe. A rigid quantitative threshold based on the location or ownership structure of first-tier subcontractors would not accurately reflect the realities of the global and interconnected technology ecosystem, nor would it lead to stronger cybersecurity, resilience, or innovation outcomes. Instead, the assessment should focus on whether providers can demonstrate robust governance, oversight, and risk management across their supply chains, regardless of where specific subcontracting activities are performed.

- **(Q11)** BSA does not consider mandatory open-source licensing to be an appropriate indicator of sovereignty. Open-source can contribute to transparency and auditability, but security and trustworthiness are achieved through rigorous processes, certification, and accountability — not through licensing models. Open-source software also reflects the global and collaborative nature of today's digital economy. Contributors from around the world continuously develop, test, maintain, and improve widely used technologies, bringing broader expertise, stronger peer review, and faster identification and remediation of vulnerabilities. What matters most is therefore not where contributors are located, but how software is developed, secured, governed, and maintained.

Conclusion

BSA stands ready to work constructively with the Digital Sovereignty Task Force to develop a sovereignty framework that is ambitious, coherent, and workable. BSA fully supports the Declaration for European Digital Sovereignty from the French-German Summit of 18 November 2025 which provides that "Digital sovereignty does not mean isolation or protectionism; it means ensuring that Europe can act independently and in a self-determined manner based on international law, its own laws, values, and security interests, while thriving to international cooperation with its partners that share European values and principles".

In that regard, we believe that Europe's digital sovereignty is best secured through:

- Strong, internationally recognised standards and interoperability requirements;
- Risk-based, technology-neutral regulation that rewards demonstrable security and accountability;
- Public procurement frameworks designed around outcomes, not geographic origin;
- Partnership between European institutions and global technology companies that are already deeply invested in Europe's digital future; and
- International cooperation to prevent fragmentation and ensure Europe's standards carry global influence.

Europe's greatest strength has always been its ability to set high standards that others choose to follow. The Task Force has an opportunity to build a sovereignty framework that the world looks to as a model — open, trusted, and genuinely resilient.

* * *

For more information, please contact:
Thomas Boué: thomas@bsa.org