GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

POSITION PAPER ON DIGITIAL SOVEREIGNTY INQUIRY OF THE FRANCO-GERMAN DIGITAL SOVEREIGNTY TASK FORCE

CONSULTATION ON A COHERENT EUROPEAN APPROACH TO DIGITAL SOVEREIGNTY

June 2026

The Global Data Alliance (GDA)[1] offers this public position paper on recent digital sovereignty inquiries from the Franco-German Digital Sovereignty Task Force.

The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA member companies are active in all industrial sectors and depend on cross-border access to information and data transfers to create jobs across the European Union (EU). GDA members are active across the agriculture, automotive, aviation, energy, finance, health, hospitality, manufacturing, media, software, telecommunications, transportation, and other EU sectors in the EU.

GDA welcomes the work of the Franco-German Digital Sovereignty Task Force and supports the EU's ambition to strengthen its digital resilience, competitiveness, and technological capability. The underlying concerns that motivate this consultation are legitimate. Concentrated dependencies on a narrow set of providers — regardless of their nationality or place of establishment — do create genuine economic and security risks, not only for public administrations but for the broader economy.

The question the Task Force must answer, however, is not *whether* to strengthen Europe's digital foundations, but *how*. The GDA's strong view is that genuine digital sovereignty is best achieved through openness, trust, and strong standards — not through geographic exclusion, origin-based discrimination, or prescriptive nationality criteria.

This view is well grounded in the EU's own stated objectives. The **Declaration for European Digital Sovereignty** from the French-German Summit of 18 November 2025 explicitly 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 striving for international cooperation with its partners that share European values and principles." The GDA strongly endorses this framing.

The GDA urges the Task Force to build a sovereignty framework on three pillars: **(1) trust and accountability, not nationality**; **(2) risk-based and technology-neutral governance**; and **(3) open, interoperable standards that secure access to the world's best technology**. Critically, any indicators used to measure digital sovereignty must function as positive assessments of contribution — not as de facto origin-based eligibility thresholds that disadvantage non-EU providers regardless of the quality, security, or competitiveness of their services.

Dimensions of Digital Sovereignty

1. Enforcement Capability (Q1–Q2)

The GDA supports the principle that EU institutions, Member States, and other users of digital services should have meaningful visibility into — and oversight of — their digital supply chains. Transparency about jurisdictional exposure and material dependencies is a reasonable and workable tool for managing digital risk. However, enforcement approaches must be grounded in proportionality and genuine risk assessment, not in reflexive geographic exclusion.

Specifically:

- Jurisdictional transparency requirements — where proportionate and clearly scoped — are workable and can improve oversight without creating unnecessary administrative burdens on providers or procurers.
- Blanket legal exclusions of non-EU access to sensitive data conflate sovereignty with isolation. The EU already possesses robust enforcement tools: the GDPR, NIS2, the Data Act, and the AI Act collectively provide a comprehensive framework for data protection and security enforcement. These instruments should be leveraged and, where necessary, clarified — not supplemented by parallel, duplicative requirements.
- Any data sovereignty framework should define the scope of 'sensitive data' with precision. In modern cloud and SaaS environments, customer content, identity data, metadata, logs, telemetry, support data, backups, and AI-related processing data serve different purposes and carry materially different risk profiles. Enforcement requirements should identify, with specificity, which data categories and processing activities they cover.

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

The GDA strongly supports investment in European digital capabilities, including in AI, cloud computing, cybersecurity, and advanced computing. Building European technological expertise is a legitimate and important policy objective. However, the Task Force should be clear that "mastery" of key technologies does not mean — and should not require — developing or deploying exclusively European solutions.

Several considerations are critical here:

- The global technology ecosystem is deeply interdependent. GDA members are among the most significant investors in Europe's digital economy: they operate major European data centres, employ thousands of digital professionals across EU Member States, and deliver skills programmes in cybersecurity, cloud computing, and AI. Their products and services support the competitiveness of European companies across industries — from automotive manufacturing to pharmaceutical R&D.
- Policy should focus on building European capability, scale, and choice — not restricting the provenance of technologies deployed. The two are not in tension: a Europe that has invested deeply in digital skills, infrastructure, and innovation will be better placed to make informed, sovereign choices about the technologies it deploys — wherever those technologies originate.
- Open-source solutions are a valuable tool for auditability and interoperability, but should not be mandated as the default. What matters is whether systems are designed to be secure, interoperable, and free from unilateral lock-in — outcomes that can be achieved through multiple approaches.

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

The GDA shares the EU's ambition to develop a strong, competitive European digital economy. The Draghi Report's finding that accelerating AI and cloud adoption in European industry is critical to Europe's competitiveness reflects a reality that GDA members understand directly: they are among the most important investors in European digital infrastructure, and Europe's continued attractiveness as a market depends on sound, forward-looking policy.

However, the GDA has **significant concerns** about linking sovereignty assessments to territorial anchoring of value creation — measured through indicators such as share of EU-based employment, R&D location, or headquarters location.

- Such indicators, when used as thresholds or eligibility criteria, risk functioning as a "buy European" mandate by another name. The effect would be to disadvantage providers that are not majority-EU-headquartered, regardless of the quality, security, interoperability, or competitiveness of the services they provide. This would reduce competition, raise costs for public administrations, and limit European companies' access to globally leading technology.
- Public procurement frameworks should be designed around outcomes — security, performance, interoperability, service quality, and value for money — not the geographic origin of service providers or the location of corporate headquarters.
- Documenting and reporting the share of EU-generated value added within a global technology product or service is operationally complex, if not impossible for most companies. Isolating and attributing value creation at a territorial level within globally integrated supply chains would create disproportionate compliance burdens, particularly for companies that already contribute substantially to the European digital economy.

4. Data Protection (Q7)

The GDA strongly supports high data protection standards. The EU already operates the world's most comprehensive data protection framework — the GDPR — and GDA members comply fully with GDPR, NIS2, and related obligations. Ensuring that these standards are rigorously enforced and consistently applied across Member States is a more effective path to data sovereignty than layering additional parallel requirements.

- Technical and organisational measures — encryption, pseudonymisation, access controls, contractual safeguards, data localisation options, and regular audits — are effective, proven, and proportionate tools for managing extraterritorial risks.
- Trust is built through accountability and transparency, not through nationality. Protection against extraterritorial access is most durably addressed through strong contractual, legal, and technical safeguards, applied proportionately according to the sensitivity of the data involved.
- European businesses — including SMEs — should be able to opt into enhanced controls where warranted by their specific risk profile, rather than all organisations being forced into the highest-cost compliance model on the basis of worst-case scenarios.

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

The GDA regards interoperability requirements and open standards as the **cornerstone of genuine digital sovereignty**. Unlike origin-based criteria — which address the nationality of a provider but not the quality of the service — interoperability requirements directly address the lock-in risks that sovereignty is intended to mitigate. They empower European organisations to exercise real choice: to switch providers, combine technologies, and retain control over their data and systems.

- Modular system architectures and documented software bills of materials are practical, effective measures that GDA members can implement and support. They enhance auditability, facilitate provider switching, and reduce dependency risks.
- Open-source solutions have an important role to play but should not be mandated as the default. What matters is that systems are designed to avoid unilateral lock-in — through open standards, contractual switching rights, and technical interoperability and portability requirements.
- Multi-cloud and hybrid approaches, which GDA members are well placed to support, offer more robust resilience than any single-provider or single-origin model.
- Standardisation cooperation with global partners — through ISO, IEC, and other international bodies — should be a priority. Without international alignment, the risk is a patchwork of bespoke European requirements that raises costs and, ultimately, serves no one well.

6. Infrastructure Resilience (Q11–Q12)

The GDA supports the development of resilient, trustworthy critical IT infrastructure. Distributed, redundant, and geographically diverse infrastructure is essential to Europe's digital resilience. However, the Task Force should be clear that resilience is achieved through **diversity and redundancy — not through geographic restriction.**

- A single European cloud stack — concentrated among a small number of European providers — would itself create a dangerous concentration risk. True resilience requires access to multiple providers, technologies, and architectures.

- GDA members building and operating European data centres and distributed points of presence already contribute directly to European infrastructure resilience. This investment is most effective — and most durable — when it takes place in a competitive, open market that rewards performance and accountability.

The GDA also notes the importance of avoiding requirements that would limit cross-border redundancy. Cybersecurity and operational resilience depend on the ability to distribute data and processing across geographies. Requirements that mandate concentration within EU borders may paradoxically increase vulnerability.

Indicators of Economic Value Creation

The GDA has **substantial concerns** about this section of the consultation. While framed 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. The GDA urges the Task Force to resist this approach and to design any indicators around genuine contribution, not geographic provenance.

Q1–Q2: Relevance of Proposed Indicators

The GDA recognises that contributions to EU-based employment, local ecosystem development, and technological capability are meaningful dimensions of economic value. However, these factors should function as **positive indicators of contribution** — not as eligibility thresholds or minimum requirements that exclude providers who do not meet them.

Additional indicators the GDA considers more relevant for assessing genuine contribution include:

- Compliance with EU regulatory frameworks, security certification status, and demonstrated ability to deliver secure, trusted, 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 that build EU digital capabilities at scale;
- Participation in global research, open-source, and innovation ecosystems that benefit European users and industries; and
- Supply chain resilience, diversification, and the ability to provide continuous and reliable service to European customers.

Q3–Q4: Location of Registered Office and Data Hosting

The GDA 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 deeply interconnected. What matters is compliance with EU law, adherence to 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 may be relevant as a factor for specific high-sensitivity use cases, but should not be applied as a blanket requirement. Mandatory EU data localisation for all digital services would:

- Fragment the Digital Single Market;
- Harm cybersecurity by eliminating geographic redundancy and limiting cross-border threat intelligence sharing;
- Increase the costs of maintaining state-of-the-art security solutions; and
- Weaken resilience and failover capacity by limiting options for alternative storage and rapid recovery in the event of outages, cyber incidents, or data loss.

Q5–Q11: Workforce, R&D, and Subcontracting Thresholds

The GDA 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 may be incompatible with the EU's international trade commitments, including under the WTO Government Procurement Agreement.

Where indicators of this kind are used at all, the GDA recommends that they be applied only as positive scoring criteria in procurement evaluation — never as eligibility thresholds — and only where genuinely relevant to the sensitivity and risk profile of the specific procurement in question.

Conclusion

The GDA stands ready to work constructively with the Franco-German Digital Sovereignty Task Force and with the European Commission to help develop a sovereignty framework that is ambitious, coherent, and workable — for European institutions, for European industry, and for the globally integrated technology ecosystem that underpins Europe's digital economy.

The GDA's members — headquartered across the globe, operating at scale across every sector of the European economy — have a direct and enduring stake in Europe's digital success. The cross-border data flows that underpin agricultural precision, automotive connectivity, clinical research, energy

management, financial services, and supply chain optimisation all depend on a regulatory environment that is open, predictable, and built on trust.

The GDA believes that Europe's digital sovereignty is most effectively secured through:

- Strong, internationally recognised standards and interoperability requirements that empower users to exercise genuine choice;
- Risk-based, technology-neutral regulation that rewards demonstrable security, accountability, and compliance — not geographic origin;
- Public procurement frameworks designed around outcomes — performance, security, interoperability, and value — not the nationality or place of establishment of the provider;
- Open and responsible cross-border data flows, maintained as a structural feature of the European digital economy rather than treated as a vulnerability to be managed through localisation;
- Partnership between European institutions and globally invested technology companies that are already deeply committed to Europe's digital future; and
- International cooperation — including through the US-EU digital trade framework and global standards bodies — to prevent fragmentation and ensure that Europe's approach carries global weight.

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 is genuinely open, trusted, and resilient — and that the world looks to as a model.

[1] The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, see https://www.globaldataalliance.org