BSA SUBMISSION ON SAFEGUARDING THE EU'S DATA SOVEREIGNTY

Response to the European Commission's Targeted Stakeholder Consultation

Brussels, 15 September 2026

The Business Software Alliance is the global trade association of the enterprise software industry.[1] Our members build and operate the cloud infrastructure, cybersecurity tools, artificial intelligence and data-analytics platforms, and enterprise business applications (for finance, human resources, supply chain, customer relationship management, or collaboration) that companies, public administrations, and institutions across every sector run on. BSA members are headquartered across the globe, including in the European Union, and BSA is active in more than twenty markets across North America, Europe, and Asia. This submission draws on our members' direct experience delivering software, cloud, and AI services to enterprise and public-sector customers worldwide, and on their experience as targets of the barriers this consultation addresses.

BSA welcomes this consultation. Its premise -- that unjustified localisation, discriminatory treatment abroad, and inadequate safeguards for data leaving the Union deserve sustained Commission attention -- reflects what our members encounter in practice, in market after market. We would add one further premise of our own: enterprise software, cloud, and AI providers are not simply a sector alongside the others this consultation concerns; we are the delivery mechanism through which nearly every other sector accesses the digital tools it

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

depends on. Barriers that impede our members also affect every EU business, hospital, bank, and public administration that has adopted a cloud service, a security platform, or an AI tool built by a company headquartered outside its own borders, which today describes the overwhelming majority of such tools in use anywhere in the world, including within the EU itself.

This submission responds to Questions 2 through 10, in the order the questionnaire presents them. Our comments concentrate on the barriers and dependencies most specific to enterprise software, cloud computing, cybersecurity, and AI/data-analytics providers, which is a subset of the broader data-related issues this consultation addresses, but one that warrants focused Commission attention given how much of the EU's own digital and data economy runs on it.

Our submission focuses on one underlying message: sovereignty is best secured through governance, not geography. We develop this through both external and internal arguments:

First (external arguments), the EU should use its negotiating leverage to secure enforceable commitments from trading partners that they will not require data or infrastructure localisation, will not condition market access on ownership, control, or immunity from foreign jurisdiction, and will not require disclosure of source code, algorithms, or security architecture as a precondition of doing business. These commitments are the most direct answer to the barriers described in Sections Q3 through Q6 below, and they are also the type of discipline the EU's own trade agreements are best placed to deliver.

Second (internal arguments), the EU should hold its own sovereignty instruments to the same standard it is asking of others. The Cloud and AI Development Act, the Data Act, the Public Procurement Act, and national schemes such as SecNumCloud all touch on questions of ownership, origin, and control. Where these instruments condition market access on where a company is headquartered, who owns it, or whether it is immune from foreign law, rather than on the security outcomes it can demonstrate, they weaken the EU's own position at exactly the moment it is asking trading partners to abandon the same criteria. We set out this argument, and BSA's recommendations for reconciling EU sovereignty policy with EU competitiveness and EU credibility abroad, in Section Q7.3 below.

Q2. Cross-border data activity of BSA members relevant to the EU

Response: Yes.

Cross-border data movement is not incidental to how BSA members operate; it is the architecture. A cloud platform, a SaaS application, a cybersecurity service, or an AI system is, by design, delivered from distributed, often multi-region infrastructure, updated and secured through centrally managed engineering, and supported around the clock by teams working across time zones. Illustrative examples from our members' operations include:

- **Product engineering and support.** Global, follow-the-sun software engineering, quality assurance, and customer support depend on shared access to code, diagnostic data, and support tickets across borders.
- **Distributed and resilient infrastructure.** Cloud services are engineered for redundancy across multiple regions precisely so that a localised outage or disaster does not disrupt service; constraints on where data may reside work against the resilience regulators elsewhere are separately asking providers to deliver.
- **Cybersecurity operations.** Threat intelligence, malware signatures, vulnerability data, and security telemetry must move across borders in real time; detection and correlation depend on visibility across a global customer base, not a single jurisdiction's traffic.
- **AI development and delivery.** Training, fine-tuning, evaluating, and safely deploying AI models typically draws on data, compute, and engineering expertise located in multiple jurisdictions; inference for a single enterprise customer may be served from whichever region offers available capacity and the lowest latency at a given moment.
- **Enterprise customer administration.** Billing, account provisioning, licence compliance, and regulatory reporting for multinational enterprise customers are administered on a consolidated, cross-border basis.

These flows run in both directions, and their significance extends well beyond our own membership. Eurostat reports that **52.7% of EU enterprises used paid cloud computing services in 2025** ,more than triple the 2014 share of 17.8%, and up from 45.3% just two years earlier.[2] Among EU enterprises using cloud services, take-up is highest for e-mail (85.2%), office software (71.7%), file storage (71.5%), and security software (65.5%), with substantial and growing use of finance and accounting software (58.2%), database hosting (45.5%), enterprise resource planning (30.1%), and customer relationship management tools (27.9%). Every one of these categories depends on cross-border data flows to and from the provider delivering the service. A barrier that reaches a BSA member abroad, or one the EU erects at home, does not stop at our sector's edge, it reaches the EU manufacturer running its ERP system, the EU hospital using cloud-hosted diagnostic software, and the EU public administration relying on a cloud-based case-management system.

Q3 and Q5. Barriers, restrictions, and risks affecting the use and cross-border transfer of data

Response to Q3: Yes. Response to Q5: Yes.

[2]Eurostat, "53% of EU enterprises used paid cloud services in 2025," 3 February 2026, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260203-1.

Aggregate practical impact on our sector: 5 (very significant), assessed cumulatively. As with other respondents, our members rarely experience barriers to using data within a market separately from barriers to transferring it to the EU; a single accreditation regime, security law, or procurement rule routinely produces both effects. We set out below the typologies with a distinctly software, cloud, cybersecurity, and AI character, several overlapping with barriers other sectors report, others specific to how our members deliver services.

3.1 Sovereign-cloud and local-ownership accreditation, impact: 5

A growing number of markets have created cloud-specific accreditation or "sovereign cloud" regimes that are open, in practice, only to domestically owned or domestically controlled providers, regardless of the technical and contractual safeguards a foreign-headquartered provider can demonstrate. The Republic of Korea's Cloud Security Assurance Program (CSAP) is illustrative: as of 2025, only three non-Korean cloud providers had achieved certification, and only at the programme's Low tier, restricted to systems containing no personal information, which excludes most of the public sector in practice.[3] CSAP's Medium and High tiers, which gate access to Korea's broader digital-transformation initiatives, remain effectively closed to foreign providers, reinforced by requirements for physically separated networks, Korea-developed encryption algorithms, in-country data residency, and locally based operations personnel, requirements that diverge from internationally recognised standards without a demonstrated security benefit. Comparable dynamics recur in the Philippines' October 2025 sovereign-cloud accreditation policy, open only to domestically registered providers for a wide range of government-related data, and in cloud frameworks that confine regulated-sector customers to providers empanelled by a domestic authority.

3.2 Conditional transfer and security-assessment regimes, impact: 5

Where transfers require prior government security assessment, the process is frequently slow, discretionary, and, because it was not designed with multi-tenant cloud or SaaS architectures in mind, difficult for our members to complete in a way that matches how their services actually operate. China's Cyberspace Administration security-assessment regime, tightened further by Cybersecurity Law amendments and new certification measures that took effect on 1 January 2026, requires disclosure of transfer agreements and self-assessed risk analyses on a per-transfer basis that few standardised software or cloud products are built to produce. Vietnam's Cross-Border Transfer Impact Assessment regime, in force since January 2026, and the Ministry of Justice's July 2026 proposal for a Law on Data Security that would bar the export of "core data" outright, point toward a regional

[3] BSA, "Addressing Korea's Cloud Security Assurance Program" (7 July 2025), https://www.bsa.org/files/policy-filings/07072025bsakrcsap.pdf.

trend that would be difficult for any cloud or SaaS provider serving the market to accommodate without building segregated, market-specific infrastructure.

3.3 Classification uncertainty and the definition of "transfer", impact: 5

Regimes built around undefined or elastic categories, "important data," "core data," "sensitive" or "critical" data, create particular difficulty for multi-tenant cloud and SaaS providers, who typically cannot know in advance how a regulator will classify a given enterprise customer's dataset, and who serve many customers from common infrastructure that cannot practically be re-partitioned by classification after the fact. A related and, for our members, especially consequential problem arises where "transfer" is defined to capture mere remote access. Read literally, several regimes treat viewing or processing data from outside the territory, including by a support engineer resolving a ticket, or a security analyst investigating an alert, as a regulated cross-border transfer. That definition sits in tension with how follow-the-sun engineering, global security operations centres, and centrally managed DevOps actually work, and risks converting ordinary product support into a compliance violation. In our members' experience, this is among the most disruptive barriers to ordinary service delivery: it forces providers to assess every possible access path against a maximal footprint rather than the actual, transient access involved, producing duplicative compliance obligations for what is functionally a matter of minutes.

3.4 Restrictions on cybersecurity and threat-intelligence data, impact: 4

Some jurisdictions restrict or add friction to the cross-border movement of log data, threat telemetry, and vulnerability information, including through in-country log-retention mandates. We understand the impulse behind these rules, but the effect runs against their stated purpose: detection, correlation, and attribution of cyber threats depend on visibility across a global base of signals, and confining a security vendor's telemetry to a single jurisdiction narrows exactly the picture that makes detection effective, rebutting the assumption that localisation and security move in the same direction. This is a case where the barrier does not merely raise cost; it can directly degrade the security outcome the underlying rule was meant to improve.

3.5 Emerging localisation of AI training data and model information, impact: rising

A newer and, in our assessment, fast-developing typology concerns artificial intelligence specifically. A small but growing number of jurisdictions have begun to require that data used to train or fine-tune AI models remain in-country, or that model documentation, weights, or algorithmic logic be disclosed to a regulator as a condition of deployment. Measured against the decade-long trajectory of data localisation more broadly ,which began with narrow sectoral rules and hardened, over time, into the broad, cross-sectoral regimes catalogued by the OECD and others ,we would urge the European Commission to treat AI-specific localisation as a typology to monitor and address now, in the design of its toolbox and in ongoing digital trade negotiations, rather than as a future problem to be addressed

once the pattern has become as entrenched as data localisation itself. In our members' experience, these requirements rarely arrive as standalone data laws: they are increasingly embedded inside generative-AI service regulation, AI-provider accreditation schemes, and sovereign-AI industrial policy, which a toolbox scoped only to conventional data localisation would miss. Requirements to disclose model weights or algorithmic logic to a public authority raise the same security-paradox concern set out at Q4 above: they concentrate the most sensitive possible information about a system in additional hands, without a demonstrated security benefit.

3.6 Customs duties on electronic transmissions, impact: 5, and newly elevated

The WTO moratorium on customs duties on electronic transmissions lapsed on 30 March 2026, when the Fourteenth Ministerial Conference closed without the consensus needed to renew it.[4] For enterprise software delivered electronically, licences, SaaS subscriptions, updates, and cloud-delivered services alike, this converts what had been settled multilateral practice for twenty-eight years into a live legal exposure in any market that has not otherwise bound itself. We return to this in Section 7 below; it is, in our assessment, the single most consequential adverse development in digital trade policy this year, and one squarely within the European Commission's power to help remedy.

BSA recommends that the European Commission:

- Treat cloud- and AI-specific accreditation and certification regimes as a distinct, high-priority typology in the European Commission's toolbox and negotiating mandates, alongside general data localisation.
- Give early and specific attention to AI-related data and model localisation before it hardens into the kind of entrenched, cross-sectoral regime data localisation has become.
- Treat the lapse of the WTO moratorium on customs duties on electronic transmissions as an urgent, first-order priority for restoration (Section 7).
- Recognise remote-access-as-transfer as a distinct typology, and press in negotiations for definitions of "transfer" that distinguish transient operational access under appropriate safeguards from bulk data export.

Q4. Requirements to disclose sensitive non-personal data, source code, or security architecture

Response: Yes, on multiple occasions.

For a software company, source code, algorithms, model weights, and detailed security architecture are not incidental technical detail; they are close to the entire asset. Several

[4] WTO, 14th Ministerial Conference, Briefing Note on E-commerce, https://www.wto.org/english/thewto_e/minist_e/mc14_e/briefing_notes_e/ecommerce_e.htm.

accreditation, certification, and transfer-approval regimes require disclosure of exactly this material as a condition of market access, certification, or continued operation, going well beyond what internationally recognised standards such as the ISO/IEC 27000 series require, and, in our members' experience, beyond what is necessary to assess the risk the regime purports to address. Korea's CSAP submissions and China's CAC security-assessment documentation requirements are both illustrative of accreditation processes that request architecture, configuration, and testing detail substantially exceeding internationally recognised baselines.

The security paradox

We would underline a point BSA has also made in the context of the EU's own emerging sovereignty framework: what protects an enterprise's customers is the demonstrated ability to govern, audit, and mitigate risk, not the disclosure of source code or architecture to a government authority, and not the geography of the vendor supplying it.[5] A consolidated description of a system's architecture, controls, and defences is, in the wrong hands, a blueprint for attacking it. Requiring that description be lodged with a public authority, particularly where that authority's own handling, retention, and onward-access controls are undefined, and particularly where the authority in question also performs intelligence or public-security functions, multiplies the number of parties holding the most sensitive possible map of a system's defences. We urge the European Commission to hold its own instruments to the same standard as it develops them (Section 7.3).

The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, adopted in December 2022, is the right starting template.[6] It was negotiated precisely to reduce the legal uncertainty that drives both localisation and disclosure demands, and its principles ,legal basis, legitimate aims, prior approval, defined handling, transparency, oversight, and redress ,extend naturally from personal data to the kind of sensitive non-personal and proprietary technical information our members are asked to disclose.

BSA recommends that the European Commission:

- Pursue, in FTAs and digital trade agreements, a freestanding commitment that partners will not condition market access, certification, or procurement on disclosure of source code, algorithms, cryptographic keys, or security architecture, subject to narrowly scoped judicial and regulatory exceptions.
- Extend the OECD Declaration's principles to government access to sensitive non-personal and proprietary technical information and press for wider adherence.

---

[5] BSA, "BSA Warns: Origin-Based Sovereignty Criteria Will Hurt Europe's Competitiveness," https://www.bsa.org/files/policy-filings/en06052026bsadigitalsovereigntytaskforce.pdf.

[6] OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD/LEGAL/0487 (14 December 2022), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

- Promote reliance on ISO/IEC 27000-series certification and mutual recognition as the alternative to bespoke national disclosure regimes.

Q6. Whether EU operators face less favourable conditions than domestic or other third-country operators

Response: Yes.

The mechanisms are rarely stated as nationality tests, but they function as one. Four recur most often in our members' experience:

- Ownership, control, and immunity-from-foreign-law criteria, which by construction exclude every foreign-headquartered provider regardless of its technical or contractual safeguards.
- Accreditation and empanelment limited, in practice, to domestic providers (Section 3.1 above).
- Asymmetric approval burdens, a light-touch notification for domestic hosting, a lengthy discretionary approval for the identical service hosted abroad.
- Local-content and procurement preferences that condition public-sector eligibility on domestic investment, local headquarters, or local partnership.

We would note that these criteria do not distinguish between an EU-headquartered provider and any other foreign provider: an EU cloud, software, or AI company competing for a public contract abroad faces exactly the barriers described above, on exactly the same terms as a competitor headquartered anywhere else outside that market. Origin-based tests abroad are, in that sense, symmetric in their effect on the EU's own global champions and on every other non-domestic provider. This is a reason for the European Commission to pursue their removal with urgency, and a reason for caution before the EU replicates the same logic in reverse at home, a point we develop in Section 7.3.

The BSA recommends that the European Commission:

- Establish, as a standing negotiating objective, that partners will not condition market access, certification, or procurement on ownership, control, personnel nationality, or immunity from foreign legal jurisdiction.
- Treat asymmetric procedural burdens between domestic and foreign hosting as discrimination in substance, actionable under GATS national treatment and the Government Procurement Agreement where applicable.

Q7. What the European Commission could do

We suggest six actions that the European Commission should undertake and that would have the greatest effect for global enterprise software, cloud, cybersecurity, and AI providers, and, in turn, for the EU customers who rely on them.

7.1 Negotiate enforceable no-localisation, no-forced-transfer, and no-disclosure disciplines

The European Commission has more negotiating opportunity in 2026 than it has had in a decade: the EU-CPTPP digital trade agreement, under active work following the March 2026 MC14 agreement to accelerate it; the Canada-EU Digital Trade Agreement, under negotiation since March 2026; and a substantial pipeline of FTA negotiations with India, the Gulf Cooperation Council, and partners in Africa and Latin America. In each, we would urge the European Commission to press specifically for a freestanding discipline against mandatory disclosure of source code, algorithms, and security architecture, not folded generically into data-flow language, but named and negotiated in its own right, on the model of the source-code protections already found in agreements such as CPTPP and USMCA. A discipline that addresses data localisation but not forced disclosure would leave our members' most acute exposure untouched.

7.2 Champion risk-based, outcome-based, technology-neutral criteria and international standards

In bilateral engagement and in multilateral standards work alike, the European Commission should press partners to assess cloud, software, and AI providers against demonstrated security outcomes and accountability, audit rights, incident response, encryption, contractual safeguards, rather than nationality, ownership, or headquarters location. Cooperation through ISO and IEC, and in particular the ISO/IEC 27000 series and the work of ISO/IEC JTC1 SC27 and SC38, should be prioritised over parallel national accreditation schemes, with mutual recognition of certification as the practical mechanism for reducing duplicated compliance burden.

7.3 Apply the same standard to the EU's own instruments, the credibility condition

The Commission should pursue a pragmatic approach to sovereignty: one grounded in effective control, security, accountability, and resilience — not solely in data location. Trusted cross-border data flows are critical to Europe's own competitiveness — they underpin cybersecurity, cloud services, AI, research, and global business operations alike. The EU's strongest argument against foreign localisation and disclosure mandates is that it does not maintain equivalent measures itself. That argument is only as strong as the EU's own record, and several current and forthcoming instruments bear directly on it. The Cloud and AI Development Act, published in June 2026, would establish graduated Union assurance levels conditioning public-sector procurement eligibility and would introduce a "Union added value" criterion in procurement scoring; BSA has previously raised concerns that provisions of this kind risk limiting market access based on ownership structure rather than security outcomes, and risk granting authorities broad discretion to tighten sovereignty

requirements over time without a correspondingly clear risk basis.[7] Article 32 of the Data Act and Articles 86 to 91 of the European Health Data Space Regulation each contain provisions that, depending on interpretation, can operate as de facto localisation requirements. National schemes such as France's SecNumCloud, which conditions its highest qualification level on immunity from non-EU legal jurisdiction, and proposals from national sovereignty task forces to link procurement eligibility to corporate headquarters location, European research-and-development workforce thresholds, or subcontracting geography, raise the same concern in a different form.[8] As BSA has argued, geographic origin is not, by itself, a meaningful proxy for security or trustworthiness. What protects Europe is the ability to govern, audit, and mitigate risk, not where a company files its corporate papers. Criteria based on headquarters location, ownership, or workforce nationality raise costs, narrow the pool of eligible providers, reduce EU public bodies and enterprises access to best-in-class security and AI tools, and risk sitting in tension with the EU's own WTO and Government Procurement Agreement commitments, without a demonstrated corresponding security gain.

This is not only a public-sector concern. In our members' commercial experience, origin- and immunity-based criteria enacted for public procurement do not stay confined to that context: private-sector customers increasingly invoke the same criteria — SecNumCloud's immunity requirement, CADA's "Union added value" scoring among them — as a reference point for demanding local-only processing or origin-based exclusion in ordinary contract negotiations, regardless of whether any government-access risk or transfer-mechanism gap actually exists. EU-internal origin criteria therefore have a market-shaping effect well beyond procurement, and weaken the EU's own hand exactly when it asks trading partners to abandon the same logic.

These are not the only respects in which the EU's own framework falls short of the standard we are asking others to meet. EU-based organisations also face a fragmented internal landscape — divergent interpretations by national data protection authorities, persistent uncertainty around EU-US data flows, and overlapping national cloud certification and localisation requirements — that drives up compliance cost and, in places, drifts from the GDPR's own risk-based design toward restricting transfers on the basis of hypothetical rather than demonstrated risk. Operationalising the GDPR's own Chapter V tools — Standard Contractual Clauses and Binding Corporate Rules — more consistently across Member States would do as much to strengthen the Single Market as any new instrument.

In our November 2025 recommendations to the European Commission, BSA set out five principles that should guide the EU's sovereignty agenda, and we commend them again here as the standard the European Commission should apply to CADA's implementing

[7] "BSA Raises Concerns About Key Elements of the EU Cloud and AI Development Act," https://www.bsa.org/news-events/news/bsa-raises-concerns-about-key-elements-of-the-eu-cloud-and-ai-development-act.

[8] BSA, "BSA Warns: Origin-Based Sovereignty Criteria Will Hurt Europe's Competitiveness," https://www.bsa.org/files/policy-filings/en06052026bsadigitalsovereigntytaskforce.pdf.

measures, to the forthcoming Public Procurement Act, and to any future instrument in this space:[9]

- **Interoperability first.** Adopt internationally recognised standards, the ISO/IEC 27000 series in particular, rather than developing parallel, EU-only certification frameworks.
- **Risk-based, technology-neutral regulation.** Apply flexible rules proportionate to actual risk, on the model the EU itself used for the AI Act, rather than blanket categorical restrictions.
- **Trust frameworks over exclusion.** Build transparent certification and mutual-recognition mechanisms that reward demonstrated compliance, rather than excluding providers by origin.
- **Smart, narrowly scoped procurement.** Reserve ownership- or location-based sovereignty requirements for a narrowly and objectively defined set of highly critical use cases, defence, national security, and comparable essential state functions, rather than applying them as a general default.
- **Invest in skills, not just rules.** Fund cybersecurity, cloud, and AI training through public-private partnerships as a durable complement to any regulatory measure.
- **Align with the GDPR.** Ensure new instruments — the Cloud and AI Development Act in particular — recognise the full range of lawful GDPR Chapter V transfer mechanisms and do not impose requirements beyond what adequacy decisions already provide; alignment of this kind increases legal certainty and keeps EU organisations' access to global technology intact.

We do not suggest that legitimate sensitivities, defence, national security, law enforcement, cannot justify heightened requirements in narrowly defined circumstances. We do suggest that the further such requirements drift from those circumstances toward a general default, the more they cost the EU in access to the best available tools, and the less credible the EU's own case becomes when it asks trading partners to abandon exactly this kind of criterion. Sovereignty measures that lose this discipline become, in practice, a source of market fragmentation and a barrier to innovation — the opposite of what they are meant to protect.

7.4 Reduce the EU regulatory compliance burden directly

Several of the most useful steps require no third-country agreement at all: expanding and accelerating the EU's adequacy network, which remains by far the most operationally effective transfer mechanism available to our members; publishing and periodically updating Commission assessments of third-country legal frameworks to reduce duplicated

[9] BSA, "Keeping the Door Open: The EU's Path to Digital Sovereignty" (13 November 2025), https://www.bsa.org/files/policy-filings/11132025eudigisov.pdf.

private-sector transfer-impact-assessment effort; pursuing practical interoperability between the EU Standard Contractual Clauses, the ASEAN Model Contractual Clauses, and the Global Cross-Border Privacy Rules system; and ensuring that EU certification schemes for cloud services, including the European Cybersecurity Certification Scheme for Cloud Services, are calibrated to risk and grounded in international standards rather than functioning as a parallel sovereignty test. Expanding adequacy benefits EU-headquartered providers with global operations exactly as much as non-EU ones, and remains the single most effective step available to reduce the duplicated third-country legal analysis our members currently repeat, market by market, for conclusions that differ little in substance.

The Commission should also reduce the practical uncertainty that still surrounds these mechanisms: streamlining the approval of Binding Corporate Rules, clarifying when the Commission's Standard Contractual Clauses (SCCs) apply to a given transfer, and providing guidance on when supplementary measures are necessary.

7.5 Extend the toolbox explicitly to AI and algorithmic-disclosure barriers

As the announced anti-data-leakage toolbox and fair-treatment guidelines take shape, we would ask the European Commission to make clear that their scope extends to barriers affecting AI training data, model information, and algorithmic-disclosure mandates, not only to data localisation in the conventional sense (Section 3.5 above). In parallel, the European Commission should pursue interoperable international AI governance, through the OECD AI Principles, the G7 Hiroshima AI Process, and the Global Partnership on AI, as the alternative to a world in which each major market imposes its own, incompatible AI-data residency and disclosure requirements.

7.6 Use the toolbox transparently, and sequence engagement before response

The diagnostic value of the anti-data-leakage toolbox and fair-treatment guidelines will depend on the transparency and discipline with which they are used. We would ask the European Commission to publish the objective criteria underlying these instruments before applying them; to exhaust structured bilateral engagement before contemplating any response measure; to consult affected EU stakeholders, including EU cloud and software customers, who would absorb the first-order cost of many response measures, before deployment; and to assess explicitly the effect of any contemplated measure on EU downstream digitalisation.

Q8. Whether cooperation with third countries or international organisations would be useful, and in what form

Response: Yes.

Cooperation changes the default; bilateral pressure resolves individual measures one at a time. We would highlight four fora in particular.

8.1 WTO

- Restore the moratorium on customs duties on electronic transmissions, whether multilaterally, plurilaterally, or through the Agreement on Electronic Commerce, and pursue a durable rather than a rolling solution.
- Bring the Agreement on Electronic Commerce into force and pursue the addition of cross-border data-flow, localisation, and source-code disciplines to it over time, building the necessary coalition through the EU-CPTPP process.
- Use WTO transparency mechanisms, Trade Policy Reviews, Committee notifications, specific trade concerns, systematically to raise cloud accreditation and data localisation measures.

8.2 OECD

- Press for wider adherence to the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, and for extension of its principles to sensitive non-personal and proprietary technical information.
- Use the OECD AI Principles and the Global Partnership on AI as the vehicle for interoperable AI governance, reducing the incentive for nationally siloed AI-data rules.
- Sustain and expand the OECD's data localisation mapping work as an authoritative, regularly updated public inventory.

8.3 Standards bodies

Cooperation through ISO and IEC, in particular ISO/IEC JTC1 SC27 (the ISO/IEC 27000 series) and SC38, should be prioritised over parallel or exclusive national frameworks, with mutual recognition of certification as a concrete, near-term deliverable.

8.4 Digital partnerships and adequacy

The EU's digital partnerships and regulatory dialogues, and its adequacy decisions, remain the most powerful trust-building instruments the EU possesses. Cloud- and AI-specific accreditation barriers, and not only classic data-transfer barriers, should be explicitly and consistently on the agenda of each, with a feedback loop to industry on outcomes.

Q9. The extent to which the EU should consider response measures where a third country discriminates against EU organisations

Response: To some extent, with the conditions set out below.

BSA recognises the legitimacy of the underlying concern. Where a third country restricts EU organisations' access to, use of, or transfer of data in ways not applied to its own organisations, the EU is entitled to respond, and we do not counsel passivity. We do counsel

care, for reasons that bear directly on our members' interests and, more broadly, on the EU's own digital and AI ambitions.

Reciprocal localisation would be self-defeating. Economic modelling of data localisation within the EU's own single market found that if all Member States imposed economy-wide localisation requirements, the cost would run to approximately €52 billion annually, or 0.37% of EU GDP ,roughly six times the benefit of removing the more limited restrictions that exist today ,and that this loss could rise toward 0.8% of EU GDP as the volume of data-dependent economic activity continues to grow.[10] A reciprocal EU localisation mandate, imposed in response to a foreign measure, would generate a closely analogous cost ,borne by EU businesses and public bodies before it is felt by the target of the response.

Reciprocal localisation would also cut against the EU's own sovereignty and AI objectives. Much of the compute capacity, model diversity, and specialised security tooling the EU is trying to build domestic capacity around today is most efficiently accessed through globally distributed infrastructure, including infrastructure operated by EU-headquartered providers with global operations. An EU measure that fragments access to that infrastructure in the name of sovereignty would narrow, not widen, the EU's own strategic options.

Precedent runs both ways. An EU instrument that conditions access on origin or on immunity from foreign law supplies a template to precisely the governments whose measures this consultation exists to address, and, per Section 7.3, some EU and Member State instruments already move in this direction.

The objective is removal of the foreign measure, not the imposition of a symmetrical one. Where the European Commission does proceed with a response measure, BSA recommends that it be:

- A last resort, deployed only after documented, good-faith bilateral or plurilateral engagement has failed.
- Evidence-based and disclosed, to the extent confidentiality permits, against the published objective criteria contemplated by the Data Union Strategy.
- Targeted at the specific measure, not the sector or the market, to minimise collateral cost to EU downstream digitalisation.
- Never in the form of reciprocal data or infrastructure localisation, or origin-based exclusion, for the reasons set out above.
- Time-limited, with sunset and mandatory review, and withdrawn promptly on removal of the triggering measure.

[10]ECIPE, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States," https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/.

- Coordinated with like-minded partners wherever possible, which is both more likely to change the foreign measure and less exposed to a charge of unilateralism.

Q10. Whether existing channels are sufficient for stakeholders to raise international data-related challenges

Response: Existing channels are useful but not sufficient.

Five specific difficulties are most salient for our members:

- Cloud, software, and AI barriers rarely present as classic market access barriers. They surface as cybersecurity certification schemes, cloud accreditation regimes, procurement scoring criteria, or AI governance rules, administered by technical regulators rather than trade ministries. A channel organised around tariffs, SPS, and TBT does not naturally capture them, and firms are often unsure whether a cloud accreditation scheme or an algorithmic-disclosure rule is even in scope.
- Confidentiality concerns suppress reporting. A vendor reporting a barrier in a market where it is mid-certification, defending a tender, or negotiating with a regulator has direct commercial exposure. A credible, non-attributable reporting pathway, including through industry associations, is essential, and BSA is willing to serve as such a channel.
- The most consequential barriers are informal, verbal guidance, unwritten expectations, and administrative delay, and current channels are least equipped to record barriers with no published measure to cite.
- Sector-specific expertise is unevenly distributed. Assessing whether a cloud accreditation framework or an AI algorithmic-disclosure requirement constitutes a disguised restriction requires technical expertise alongside trade expertise, and firms report that the quality of engagement varies considerably depending on who receives the report.
- Feedback is limited. Firms and associations that invest in preparing a detailed submission frequently hear nothing about what happened to it, which depresses future reporting more than any other single factor.

The BSA recommends that the European Commission:

- Establish a dedicated cross-border data and digital services barrier intake within the Single Entry Point, with an explicit scope statement covering cybersecurity certification schemes, cloud accreditation regimes, procurement scoring criteria, and AI governance and algorithmic-disclosure measures alongside conventional localisation and transfer barriers.

- Provide a robust, non-attributable confidentiality pathway, including an option for reporting through industry associations on an aggregated basis; BSA is willing to serve as such a channel, and this submission is offered in that spirit.
- Convene a standing sectoral expert group on cloud, software, and AI-related data barriers, bringing together DG CNECT, DG TRADE and DG GROW with industry, and feeding recurring findings into negotiating mandates and the toolbox.
- Close the loop: report back to reporting stakeholders, at least annually, on what was raised, with whom, and to what effect.

Conclusion

The premise of this consultation is sound, and BSA's members experience the underlying problem directly: unjustified localisation, discriminatory treatment abroad, and inadequate safeguards for data leaving the Union impose real costs, in market after market. For global enterprise software, cloud, cybersecurity, and AI companies, those costs are frequently sharper than for other sectors, because the barriers described in this submission strike at what our companies most directly sell, source code, algorithms, and the architecture of trust that underpins a security or AI product, and because so much of the rest of the EU economy depends on the tools our members deliver.

The most effective response available to the European Commission is also the most consistent with the Union's own tradition: to use the EU's negotiating weight to secure binding commitments from partners against localisation, forced transfer, and forced disclosure, and, in parallel, to ensure that the EU's own sovereignty instruments are held to the same risk-based, outcome-based, technology-neutral standard. Sovereignty secured through governance, the demonstrated ability to audit, control, and mitigate risk, is durable. Sovereignty pursued through geography is not, and it is expensive, for the EU's own businesses and public bodies, in the meantime.

BSA stands ready to support the European Commission in this work, and to provide technical input, evidence, and market intelligence from our member companies as the Commission's toolbox, guidelines, and negotiating agenda take shape.

* * *

For further information, please contact:
Thomas Boué, Vice-President and Director General Policy – EMEA
thomas@bsa.org