Consultation Response

Safeguarding the EU's Data Sovereignty

September 2026

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the **European Commission's targeted consultation on safeguarding the EU's Data Sovereignty**. The Association for Financial Markets in Europe (AFME) is the voice of the leading banks in Europe's financial markets, providing expertise across a broad range of regulatory and capital markets issues. We represent over 150 leading global and European banks and other significant market players. Our members play a vital role in Europe's financial ecosystem, underwriting around 90% of European corporate and sovereign debt, and 85% of European listed equity capital issuances. Importantly, AFME members are market makers, providing liquidity, which is essential for ensuring financial markets can function efficiently. We also represent law firms and other associate members which advise market participants and support AFME's legal and regulatory initiatives.

AFME is registered on the EU Transparency Register, registration number 65110063986-76. We summarise below our high-level response to the consultation, which is followed by answers to the individual questions raised.

Executive Summary

International financial institutions experience significant data transfer frictional barriers between the EU and third countries. We are supportive of enhanced multilateral cooperation to ease barriers, as well as the EU taking more ambitious action to prioritise data adequacy assessments of significant markets, actively promote the adoption of international data standards (e.g. the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities), and embed free-flow of data in trade, investment, and multilateral negotiations.

Part 2- International data-related barriers or other issues

The following questions distinguish between barriers or other issues regarding the access to or use of data in third countries, and barriers or other issues regarding the transfer of data between third countries and the EU.

Q3 – In your sector or organisation, have you encountered barriers, restrictions, risks or other issues when accessing, using, sharing or transferring data within a third country?

This may include legal, technical or organisational measures that affected your ability to access, use, share, transfer or retain control over data. Examples may include authorization, licensing or certification requirements, administrative delays, forced data transfers or access, lack of transparency, discriminatory treatment, contractual or administrative restrictions, informal expectations, legal uncertainty, data leakage to third parties, public-authority or judicial access risks, or unauthorised reuse.

- X Yes
- ○ No
- ○ I don't know

Impact = 5 (very significant).

Association for Financial Markets in Europe
London Office: Level 10, 20 Churchill Place, London E14 5HJ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540
Frankfurt Office: c/o SPACES – Regus, First Floor Reception, Große Gallusstraße 16-18, 60312, Frankfurt am Main, Germany T:+ 49 (0)69 710 456 660
www.afme.eu

We observe that international banks, including European financial institutions operating internationally, do experience data-related barriers when serving markets and clients outside of the EU due to third country rules and requirements. We focus our comments here on third-country data requirements that impact cross-border data flows, as these tend to introduce both direct and indirect complications and friction for the operations of international banks. These barriers generally fall into three categories: data localisation mandates, sector-specific restrictions on cloud and outsourcing arrangements, and legal / regulatory uncertainty.

First, several important jurisdictions / markets have data localisation mandates in place. These third countries require certain categories of data to be localisation, and only transferred abroad under limited circumstances or subject to prior approval. As (non-exhaustive) examples:

- China: the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL) impose local storage obligations on operators classified as "critical information infrastructure operators," a category that has been applied broadly and has, in practice, captured some financial institutions.
- India: the Reserve Bank of India mandates that payment system data be stored exclusively in India.
- Turkey: Personal Data Protection Regulation restricts transfers abroad absent an adequacy decision or prescribed safeguard. Financial-sector information-systems rules additionally require banks' primary systems and customer-secret data to remain in Turkey, materially constraining foreign cloud and AI services
- Vietnam: the Cybersecurity Law and its implementing decree require in-country storage of certain user data by providers meeting specified activity thresholds.
- Others: while European financial institutions have largely discontinued operations in Russia, we note that Russian Federal Law No. 242-FZ requires personal data of Russian citizens to be stored on servers located in Russia before any transfer abroad.

Second, beyond outright localisation, some jurisdictions have in place requisite approval and/or security assessment requirements on outbound data transfers. While this is not directly relevant for data transfer within a country, it has significant implications for the operational set-up of international banks. As examples:

- China: the outbound transfers of "important data" or personal information above certain thresholds require a security assessment administered by the Cyberspace Administration of China (CAC), or reliance on a CAC-filed standard contract or certification mechanism. These processes introduce significant barriers to the time and certainty required for seamless cross-border transfer.
- South Korea: the Personal Information Protection Act (PIPA) restricts outbound transfers of personal data unless specific conditions are satisfied (e.g. consent, contractual safeguards, or certification), independent of the EU's own adequacy recognition of Korea, which governs transfers in the opposite direction (EU to South Korea) only.
- Nigeria: Prior approval from the Central Bank of Nigeria is required before entering into material cloud outsourcing arrangements including those with offshore providers.

Third, we observe that some restrictions on data access, use, and transfer of data in third countries stem from requirements on outsourcing and cloud adoption. For example:

- South Korea: the Financial Services Commission, under the Electronic Financial Transactions Act, imposes reporting or prior-approval requirements before outsourcing "core" systems to cloud providers, creating friction for offshore processing of financial consumer data.
- Gulf states (e.g., Saudi Arabia, UAE, Bahrain, Qatar): Central bank frameworks, such as those administered by the Saudi Central Bank (SAMA), often require data residency for banking and customer data, with specific rules governing cloud outsourcing.
- Indonesia: the OJK requires banks to locate its Electronic Systems in a data centre and disaster recovery centre locally unless an approval is given.

Finally, regulatory uncertainty from a lack of clear definitions or thresholds is itself a material obstacle. As a clear example, China's lack of a published, precise definition of “important data” (subject to

outbound transfer approval) leaves financial institutions unable to determine with confidence which datasets trigger the CAC security assessment obligation, independent of the substantive restriction that assessment imposes.

Q4 – In the last three years, has your organisation been required, formally or informally, to provide access to non-personal data that you deem sensitive for your organisation to a public authority in a third country as a condition for market access, authorisation, certification, public procurement, security review or regulatory approval?

- o No
- X Yes, once or on isolated occasions
- o Yes, on multiple occasions
- o I don't know / no experience

Yes, financial institutions are generally required to provide access to non-personal data to a public authority as a condition for market access. In this vein, we do acknowledge that non-personal data provision is a normal course of authorisation and supervision. However, there are cases where non-personal data provision appears to exceed international norms. This is most apparent in China, where, as noted above, the cross-border transfer assessment for "important data" under the Data Security Law (with the Cyberspace Administration of China as the responsible authority) requires companies to submit non-personal but sensitive industrial, geospatial, or infrastructure-related data for governmental review before transfer; as data transfer is a continuous activity by international financial institutions, this can lead to significant market and operational friction.* Chinese cryptography and critical-infrastructure certification regimes (e.g. the Cryptography Law and MLPS 2.0) can similarly require disclosure of technical/architectural data as part of testing and certification.

*There are also examples outside the financial sector, where China's 2021 connected-vehicle data rules required European automotive manufacturers to localise vehicle data on domestically hosted infrastructure, often via joint ventures with Chinese cloud providers, as a practical condition of continued market access.

Q5 – In your sector or organisation, have you encountered barriers, restrictions, risks or other issues as regards data transfers between a third country and the EU, including where the data was generated, collected or lawfully accessed outside the EU?

Examples may include data localisation requirements, security reviews, extraterritorial governmental or judicial access of data stored in the EU, administrative delays, lack of transparency, discriminatory treatment, contractual or administrative restrictions, informal expectations, legal uncertainty.

- X Yes
- o No
- o I don't know

If yes, please provide examples, including the third country or region concerned, and rate the impact on your organisation or sector (on a scale of 1 to 5, where 1 = very limited impact, and 5 = very significant impact).

Yes, as noted above, financial institutions face barriers on both directions of EU and third-country data transfers. Greater regulatory coherence and reduced legal uncertainty are needed to support trusted and efficient cross-border data flows. Substantive barriers include:

- **Data transfer conditionality**: the EU's conditional transfer model under GDPR permits cross-border data flows subject to meeting defined safeguards (e.g., consent, adequacy, or contractual mechanisms with assessment). This requires companies to verify the legal basis for every transfer rather than treating cross-border movement as presumptively open.
- **Gaps in adequacy coverage**: major commercial destinations, such as India, still lack an EU data adequacy decision. This requires international institutions to rely on more burdensome contractual transfer mechanisms for high-volume data relationships.
- **Third-country restrictions on inbound/outbound flows**: countries such as China, Vietnam, Qatar, Saudi Arabia, and the UAE impose local processing or prior government authorisation

requirements before data can move across their borders, restricting the free flow of data back to the EU or onward to other markets. In some cases, the countries extend legal jurisdiction to residences of those countries holding accounts with European banks.

- **Growing restrictions on non-personal data**: international studies show that measures affecting cross-border flows of non-personal data have increased roughly five-fold over the past decade[1], which indicates this is a broader and worsening trend, not limited to personal data transfers.

Q6 – For the third countries that are most critical for your sector, do EU operators face less favourable conditions than domestic operators or operators from other third countries in relevant data-related markets?

- o Yes
- o No
- X I don't know

If yes:
Please identify the third country or region concerned, and the conditions considered less favourable.

We do not have sufficient information to comment on this question.

Q7 – What could the European Commission do to help address the barriers or other concerns identified above?

Please explain which type of actions would be most useful for your organisation or sector, and why. Examples could include guidance for companies on cross-border data risk assessment and safeguards, practical tools to support the transfer of data to the EU, sectoral exchanges on recurring barriers, or follow-up with third countries where systemic obstacles are identified.

There are significant steps the European Commission could take to help address barriers above, including:

- o **Expanding and streamlining outcome-based adequacy and equivalence pathways:** to support greater cross-border data flows between the EU and significant markets, the Commission should prioritise adequacy assessments for commercially significant markets that have not yet received a positive adequacy decision (e.g. India). Should the data protection frameworks of these countries be found to misaligned with the EU framework, the Commission should leverage the adequacy and equivalence assessments as channels to identify possible further safeguards in order to support cross-border data flows. Establishing data sharing arrangements with a greater number of third countries and significant markets would reduce operational inefficiency for international institutions, as well as improve reliability, certainty and predictability for lawful transfers, rather than leaving companies to default on contractual mechanisms that are more burdensome and less scalable.
- o **Promoting wider adoption of government-access safeguards**: international standards, such as the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, adopted by OECD members and the EU in December 2022, establish a useful international baseline on common safeguards for government access to private-sector data for national security and law enforcement purposes, explicitly framed as supporting data free flow with trust. In its discussions and negotiations with third countries, the Commission should promote broader third-country adoption or equivalent commitments as a confidence-building measure, particularly with jurisdictions where government access uncertainty (rather than formal transfer bans) is the primary source of risk.
- o **Considering to provide practical guidance on assessing cross-border data-transfer risks and implementing safeguards**, including for complex outsourcing, cloud and intra-group arrangements, with the aim of improving the consistent interpretation and application of EU requirements, reducing legal uncertainty and compliance costs, and supporting reliable,

[1] OECD Trade Policy paper No. 295, A Preliminary Mapping of Measures Affecting the Cross-Border Flow of Non-Personal Data

scalable data flows. Such guidance should be developed collaboratively with industry participants.

Q8 – Would cooperation between the EU and third countries or international organisations be useful for addressing international data-related challenges faced by your organisation or sector?

- X Yes
- o No
- o I don't know

II. **If "yes"**: What measures could the EU take in such international cooperation or in what format should the EU advance such international cooperation to help your organisation or sector in the data-related issues?

Yes, on balance there is a strong policy case for the EU to deepen cooperation, and existing initiatives suggest this is already the direction of travel rather than a novel proposition. International standard-setters have warned that excessive fragmentation erodes both resilience and interoperability and, for example, the G20 goals for more efficient international payments. As noted above, in servicing international markets, many European institutions face data localization requirements and untransparent "important data" or security-review regimes. These barriers are structural and unlikely to be resolved through unilateral EU action or company-by-company negotiation. Multilateral or bilateral cooperation would provide the opportunity to address these barriers at the regulatory-framework level rather than leaving individual companies to negotiate market access on unequal terms.

Several existing mechanisms illustrate the direction that could be pursued by enhanced multilateral cooperation:

- **Adequacy decisions and data partnerships**: the EU's adequacy findings (e.g., with Japan, South Korea, the UK) and ongoing dialogues with other partners have reduced transfer friction and could be extended or used as a template for new partnerships, giving European companies smoother data flows than competitors from jurisdictions without such arrangements.
- **The EU–US Data Privacy Framework**: this partnership demonstrates that negotiated, government-to-government arrangements can resolve transfer barriers that company-level compliance efforts cannot.
- **Plurilateral trade instruments**: the WTO Joint Statement Initiative on e-commerce, and frameworks like the Global Cross-Border Privacy Rules (Global CBPR) system, offer avenues for the EU to push for common baseline rules on data flows, localisation, and government access, potentially reducing the leverage third countries currently have to impose conditions market-by-market.
- **Digital/data provisions in bilateral trade agreements** - increasingly used by jurisdictions, including the EU, to embed data-flow and non-localisation commitments directly into trade terms. These provisions could be expanded to resolve the "important data"/non-personal data access issues raised in earlier questions.
- **Voluntary and interoperable mechanisms**: the EU should promote voluntary tools, such as model contractual clauses, certifications, codes of conduct and common technical standards. These can help enable organisations to demonstrate that they maintain robust safeguards for cross-border data sharing and facilitate trusted international data flows. For example, the joint guidance on Standard Contractual Clauses (SCC) developed by the European Commission and ASEAN for data transfers helps to support cross-border data transfers. Such mechanisms should complement, rather than replace, enforceable legal protections and adequacy arrangements.

The main caveat is that multilateral cooperation often takes significant time to negotiate and is highly dependent on reciprocal political will from third countries whose regulatory approach may not be compatible with EU objectives; it is therefore better framed as a necessary but partial and slow-acting remedy, rather than a complete solution to resolve market-access frictions at-pace.

Q9 – To what extent should the EU consider adopting measures in response where a third country imposes restrictions on access to, use of, or transfer of data by EU organisations that are not applied to domestic organisations?

- o To a great extent
- X To some extent
- o To a limited extent
- o Not at all
- o I don't know

While we view that there is a reasonable policy case for the EU to consider countermeasures, particularly where restrictions are demonstrably asymmetric (i.e., third countries limit European companies' data access/transfer while their own companies operate freely in the EU market), we view that – as a strong principle – any actions should prioritise the commercial interests of EU-based institutions, rather than jeopardise introducing more barriers through countermeasures.

We do view, however, there exist reasonable means with which the EU might seek to more fully embed reciprocal data transfers in trade and investment negotiations with third countries as well as multilateral discussions. For example, the EU could consider:

- **Conditionality in trade and investment agreements**: inserting binding non-discrimination and data-flow clauses (rather than best-efforts language) into new and renegotiated trade agreements, with dispute-resolution mechanisms specific to data-market treatment.
- **Coordinated diplomatic/multilateral escalation**: raising specific instances through WTO channels or coordinated démarches with like-minded trade partners facing similar restrictions, to increase collective leverage rather than acting unilaterally.

Q10 – Are existing channels sufficient for stakeholders in your sector to report or raise international data-related challenges with the European Commission or Member States, where appropriate? If not, what improvements would be useful, including as regards confidentiality, follow-up or sector-specific expertise?

For this question, international data-related challenges may include barriers to accessing or using data in third countries, difficulties transferring data to the EU, risks linked to third-country access to sensitive data, or relevant data-related dependencies.

Yes, there are existing channels; however, these are only partially sufficient, and currently fragmented and underused.

For example, the EU offers several routes for participants to raise data-related concerns, including through the Market Access Database and Market Access Advisory Committee, which allows businesses flag trade barriers (including digital/data issues) to the European Commission. Separately, DG TRADE's complaint mechanisms and Chief Trade Enforcement Officer office handle formal trade-barrier complaints; and business associations abroad (e.g., the European Chamber of Commerce in China) informally aggregate and relay company concerns. Member States also run their own bilateral channels via embassies and trade agencies.

The main criticism, however, is that there exists is no single, well-publicised entry point specifically for businesses to flag and report data-related barriers, companies (especially SMEs) often don't know which channel to use, and many are reluctant to file complaints for fear of retaliation in markets where they still need to operate.

We therefore recommend the following improvements:

- **Confidential/anonymised reporting options** to alleviate market retaliation concerns. We would also support a dedicated, single-entry EU-level reporting mechanism for data-specific barriers, with clear triage to the right authority. If EU-level reporting is difficult to implement, we recommend the EU to publish a list of aggregated Member State authorities / mechanisms to which issues can be reported.

- **Formalised use of private-public forums** as aggregators, with a structured feedback loop to the European Commission. This should complement firms' ability to directly reach out to authorities.

- **Better outreach and awareness**, particularly for SMEs.

- **Regular stocktaking** (e.g., an annual data-barriers report) to capture informal, recurring pressures systematically rather than only when companies choose to complain.

Q11 – Please provide any further comments, evidence, practical examples, studies or data that may support your views, including on wider data-related dependencies or vulnerabilities in your sector or organisation.

Where possible, please identify the sector, data category, economic-security relevance and third country or region concerned.

No proposed answer.

Q12 – Would you like to be contacted for future consultations, workshops or other stakeholder engagement activities related to data policy?

X Yes
o No