Response to the European Commission Targeted Consultation on Safeguarding the EU's Data Sovereignty

September 2026

The Global Data Alliance ("GDA" or "the Alliance") welcomes the opportunity to respond to the Commission's targeted consultation on safeguarding the EU's data sovereignty.

INTRODUCTION

The GDA shares the premise from which this consultation proceeds:

- That data is essential to Europe's competitiveness and security and is a foundational input both to artificial intelligence and to Europe's growing technological sovereignty and resilience; and

- That other countries' unjustified localisation requirements, discriminatory origin- or ownership-related preferences, or other arbitrary, disguised, or unnecessary trade barriers can threaten those objectives.

We agree with the premise that a level playing field, security, and consistency with EU values and interests can be secured alongside cross-border data flows conducted with trust.

The GDA is well positioned to assist in this assessment: our members are active across the agriculture, automotive, aviation, energy, finance, health, hospitality, manufacturing, media, software, telecommunications, and transportation sectors. Our members also include EU-based organisations and some of the most significant investors and employers in Europe. Finally, our members occupy both sides of the question this consultation asks – both as suppliers of data-driven products and services to European customers, and as users of data that must be accessed, consolidated, and analysed across borders.

This submission is organized as follows: An Executive Summary and Discussion section, followed by two Annexes: (1) an overview of GDA's cross-border data policy principles; and (2) a country-by-country analysis of cross-border data policies of interest.

EXECUTIVE SUMMARY

We welcome this consultation and share the concerns that motivate it. Unjustified data localisation mandates, discriminatory eligibility rules, and opaque government access regimes in third countries impose real and rising costs on European organisations. These are legitimate challenges that not only warrant an EU response, but also should inform how the EU designs its own cross-border data policies.

We also welcome the Commission's framing that data sovereignty does not preclude openness to trusted partners. That framing is consistent with the Declaration for European Digital Sovereignty adopted at the French-German Summit of 18 November 2025, which provides that digital sovereignty "does not mean isolation or protectionism,"

but rather ensuring that Europe can act independently and in a self-determined manner while striving for international cooperation with partners that share European values.[1]

The EU has a great deal to gain by collaborating with its allies and trading partners to promote greater cross-border access to data, services, and technology. In 2024, the EU exported €1,568 billion of services to non-EU countries, a record, generating a services surplus of €194 billion – the highest in a decade.[2] The EU is the world's largest exporter and importer of digitally deliverable services. Global exports of digitally delivered services reached approximately USD 5.3 trillion in 2025 and now account for roughly 55% of global services trade.[3] Roughly 38% of Europe's digitally deliverable services exports go to economies outside the region.[4]

Our submission makes four points:

1. **The barriers are real, documented, and systemic.** Section 4 sets out specific third-country measures – in China, India, Indonesia, the Republic of Korea, Saudi Arabia, Türkiye, the UAE, Vietnam and elsewhere – that restrict European organisations' ability to access, use, and repatriate data. These are not isolated incidents. They follow a recognisable pattern and are proliferating.

2. **Obstacles to transferring data *into* the EU deserve more attention than they receive.** Third-country export controls on data prevent EU-headquartered companies from consolidating operational, safety, quality, and compliance data at their European parent entities. This is a first-order European sovereignty problem, and it also directly impedes those companies' ability to discharge obligations imposed on them by EU law.

3. **The diagnostic test should be the character of the measure, not the nationality of the provider.** What makes a third-country measure harmful is that it conditions access on origin, ownership, or corporate structure rather than on demonstrated security and performance. That is the right test for identifying foreign barriers — and, for the same reason, it is the right constraint on the EU's own response.

4. **The EU has more leverage through coalition and trade instruments than through the unilateral imposition of its own data-related trade restrictions.** Section 6 sets out recommendations that would materially improve European organisations' position abroad while remaining true to European values and strategic priorities.

DISCUSSION

Barriers to Accessing or Using Data in Third Countries

We group the measures that our members encounter into five categories. In each case, implementing governments seek to justify the restriction on sovereignty, security, privacy, or law-enforcement grounds. Regrettably, in many

---

[1] Declaration for European Digital Sovereignty, adopted at the Franco-German Summit, Berlin (18 November 2025). The Declaration provides that digital sovereignty "does not mean isolation or protectionism", but rather that Europe should be able to act independently and in a self-determined manner while striving for international cooperation with partners that share European values. See also Global Data Alliance, Submission on the Franco-German Digital Sovereignty Initiative (23 June 2026), which develops the point at greater length.

[2] Eurostat, "EU services exports reach record high in 2024" (17 December 2025), at https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251217-1. Extra-EU exports of services totalled EUR 1 568 billion in 2024, an increase of 8% on 2023; extra-EU imports of services totalled EUR 1 374 billion (+7%); the resulting services trade balance of EUR 194 billion is the highest recorded in the past decade. The United States was the largest destination for extra-EU services exports (EUR 344 billion; 22%), followed by the United Kingdom (EUR 294 billion; 19%) and Switzerland (EUR 162 billion; 10%). Underlying dataset: Eurostat, bop_its6_tot.

[3] WTO, Digitally Delivered Services Trade Dataset, WTO Global Services Trade Data Hub, at https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm. On the 2025 estimates: global exports of digitally delivered services of approximately USD 5.3 trillion, against total services exports of approximately USD 9.6 trillion, giving a share of roughly 55% - up from approximately 43% in 2015. For comparison, the WTO recorded digitally delivered services exports of USD 4.25 trillion in 2023, equivalent to 13.8% of global goods and services exports.

[4] WTO, "WTO and OECD release expanded dataset on trade in services covering over 200 economies" (17 February 2025), at https://www.wto.org/english/news_e/news25_e/stat_17feb25_e.htm. The WTO reports that 62% of Europe's exports of digitally deliverable services were destined for economies within the region, implying that approximately 38% went to economies outside it. By contrast, North America exported 82% of its digitally deliverable services outside the region. Source: WTO estimates (2025), Balanced Trade in Services (BaTIS) dataset in the WTO Global Services Trade Data Hub.

of these cases, the measure is designed or applied in a way that is discriminatory or more trade-restrictive than necessary to achieve the stated objective.

1.1 Data localisation mandates and data transfer restrictions

These types of measures may require that data be stored, processed, or backed up within national territory, or that duplicate local copies be maintained. They may also impose restrictions on the ability to transfer data from outside the EU into the EU or to another market. As outlined in the GDA's Cross-Border Data Policy Index, these types of restrictions are especially common in the financial, health, public sector, and critical infrastructure contexts – precisely the contexts in which geographic redundancy and cross-border threat visibility matter most.[5] We offer several illustrative examples below, and a more comprehensive listing in the Annex to this submission.

Example 1.1(a) — China: outbound transfer restrictions and "important data" catalogues	
Sector	Cross-sectoral; acute in automotive, manufacturing, pharmaceuticals, financial services, and logistics
Data category	Operational and machine data; R&D and engineering data; personal and sensitive personal data; "important data" as defined under the Data Security Law
Third country	People's Republic of China
Practical impact	The Cybersecurity Law, Data Security Law, and PIPL together impose security assessment, standard contract, or certification requirements on outbound transfers, triggered at various numerical thresholds. PIPL Articles 42–43 further authorise retaliatory measures against overseas entities. The practical result is that EU-headquartered groups face material legal uncertainty if they attempt to consolidate and transfer data from Chinese operations[6].
Isolated or systemic	Systemic. The framework is comprehensive, expanding through sub-national catalogues, and applies across sectors.

Example 1.1(b) — Saudi Arabia: mandatory in-Kingdom hosting	
Sector	Public sector, critical national infrastructure, financial services, health, energy
Data category	All hosted information and IT systems; cloud customer data; backup and disaster recovery systems; security monitoring data; personal data
Third country	Kingdom of Saudi Arabia
Practical impact	The National Cybersecurity Authority's Essential Cybersecurity Controls require that an organisation's information hosting and storage be inside the Kingdom (ECC-1:2018, 4-2-3-3) and that cybersecurity managed services centres for monitoring and operations be located entirely within the Kingdom (ECC-1:2018, 4-1-3-2). Cloud Cybersecurity Controls (CCC-1:2020, 2-3-P-1-10 and 11) extend this to cloud storage, processing, disaster recovery, and monitoring systems. Under the Personal Data Protection Law, controllers must obtain a permit from SDAIA to transfer personal data abroad absent an approved destination or narrow exception; approvals are slow and uncertain, so most organisations

[5]Global Data Alliance, GDA Cross-Border Data Policy Index (2023), at https://globaldataalliance.org/resource/cross-border-data-policy-index/; full index at https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf.

[6] PRC Cybersecurity Law (effective 1 June 2017); Data Security Law (adopted 10 June 2021, effective 1 September 2021); Personal Information Protection Law (effective 1 November 2021), arts. 38-40 and 42-43, at http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml; CAC, Measures for Security Assessment of Cross-Border Data Transfers (effective 1 September 2022); CAC, Regulations on Promoting and Standardising Cross-Border Data Transfers (22 March 2024). On the sub-national "negative lists", see Annex II (China), describing the Tianjin Free Trade Zone list of 46 data subclasses (17 May 2024) and the Beijing Pilot Free Trade Zone list of 23 business scenarios and 198 data elements across five industries (30 August 2024). See also Global Data Alliance, Submissions in the People's Republic of China (2020-2025), at https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-china

	localise by default[7]. Separately, a 2021 policy conditions eligibility for government contracts on establishing a regional headquarters in the Kingdom.
Isolated or systemic	Systemic, and expanding as part of a declared national strategy.

Example 1.1(c) — India: sectoral localisation layered on general data protection law	
Sector	Financial services, insurance and reinsurance, public sector IT, geospatial and meteorological services
Data category	Payment system data; securities market data; insurance records and policyholder data
Third country	India
Practical impact	Multiple sectoral regulators impose localisation obligations that operate on top of, and independently of, the Digital Personal Data Protection Act. The IRDAI (Maintenance of Insurance Records) Regulation 2015 requires insurance data to be held in India; IRDAI reinsurance regulations impose storage and consent requirements on foreign reinsurer branches. The RBI Master Direction on KYC requires that the entire data and recordings of video-based customer identification be stored in systems located in India. The MeitY MeghRaj initiative requires participating cloud providers to maintain a data centre facility within India. Geospatial guidelines and the National Data Sharing and Accessibility Policy constrain cross-border use of mapping and government-owned weather data. For European insurers, reinsurers, and banks, the effect is duplicated infrastructure and an inability to run group-level risk, actuarial, and fraud models on a consolidated basis[8].
Isolated or systemic	Systemic and cumulative — the burden arises from the interaction of overlapping sectoral instruments rather than any single measure.

Example 1.1(d) — Vietnam: mandatory data localisation	
Sector	Cloud/data storage; e-commerce and payments; transport platforms; “core” and “important” data; online communications
Data category	Personal information of service users in Vietnam; user-generated account, usage, payment, email, IP-address, and telephone-number data; user-relationship data under the Cybersecurity Law
Third country	Vietnam
Practical impact	Vietnam’s 2025 Cybersecurity Law, effective 1 July 2026, requires domestic and foreign enterprises providing telecommunications, Internet, and value-added services in Vietnam that collect, exploit, analyse, or process specified user data to apply data-protection measures and store that data in Vietnam; it also provides for a local branch or representative-office requirement for foreign enterprises. Decree No. 333/2026/ND-CP, issued on 19 August 2026, specifies implementation. It requires domestic enterprises to store covered personal and user-generated data in Vietnam and establishes procedures

[7] Saudi National Cybersecurity Authority, Essential Cybersecurity Controls ECC-1:2018, controls 4-2-3-3 (hosting and storage inside the Kingdom) and 4-1-3-2 (cybersecurity managed services centres located entirely within the Kingdom); NCA, Cloud Cybersecurity Controls CCC-1:2020, controls 2-3-P-1-10 and 2-3-P-1-11; Personal Data Protection Law (Royal Decree M/19 of 2021, as amended in 2023) and its Implementing Regulations, administered by SDAIA. On the regional-headquarters condition for government contracting, see Annex II (Saudi Arabia). See also Global Data Alliance, Submissions to the Kingdom of Saudi Arabia (2020-2025), at https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-saudiarabia

[8] IRDAI (Maintenance of Insurance Records) Regulations, 2015, para. 3(9), at https://irdai.gov.in/document-detail?documentId=604674; IRDAI reinsurance regulations, imposing storage and consent conditions on foreign reinsurer branches; RBI, Master Direction on Know Your Customer (as amended, May 2021), at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12089&Mode=0, requiring that the entire data and recordings of video-based customer identification be stored in systems located in India; MeitY, MeghRaj cloud empanelment requirements, at https://ambud.meity.gov.in/; National Data Sharing and Accessibility Policy 2012, at https://dst.gov.in/sites/default/files/gazetteNotificationNDSAP.pdf; and the Digital Personal Data Protection Act 2023 together with the Digital Personal Data Protection Rules 2025 (notified 13 November 2025). See Annex II (India) for the full inventory.

	under which foreign enterprises in a broad set of digital-service sectors can be ordered to localise covered data and establish a local office after repeated non-compliance with Ministry of Public Security cybersecurity requests. The minimum storage period following an order is 24 months. For European providers and customers, these requirements can force duplicated infrastructure and local operations, constrain use of regional or global cloud architectures, and complicate cross-border security monitoring and service delivery[9].
Isolated or systemic	Systemic.

Comparable measures apply in other markets of interest to European organisations, including:

- **Indonesia —** Government Regulation 71 and Ministerial Regulation 5/2022 impose registration and public-scope obligations on electronic system operators, with blocking as the enforcement mechanism; Bank Indonesia requires certain financial transactions to be processed domestically; and Ministry of Industry Regulation 22/2020 sets local content requirements against a 35% import-substitution target, with signalled intent to extend local content rules to software and cloud services.

- **Türkiye —** the Banking Regulation and Supervision Agency requires both primary and secondary information systems to be hosted in Türkiye; a 2019 Presidential Circular on Information and Communication Security imposes loosely defined residency obligations on "strategic" government workloads that override subsequent clarifying guidelines.

- **United Arab Emirates —** the Abu Dhabi Healthcare Information and Cybersecurity Standard restricts cross-border health data flows, with consequences for research participation, remote care, medical device servicing, and insurance eligibility verification for EU citizens resident in or travelling to the Emirate.

- **Morocco** — Decree No. 2-24-921 restricts eligibility to supply qualified cloud services to providers incorporated in Morocco with their entire operational and business systems located in-country (Level 1), or to providers a majority of whose shares are held by Moroccan persons and all of whose processing and storage takes place in Morocco (Level 2). This combines a localisation mandate with an explicit shareholding test.

- **South Africa, Taiwan, Bolivia, and others —** national cloud and data policies requiring that government or financial-sector data reside on domestic infrastructure, in several cases operated by domestic vendors.

These barriers impact EU-based entities and EU-invested foreign entities in several ways. First, where a third country restricts the export of data generated on its territory, the entity that loses visibility is the European parent or affiliated. An EU-headquartered manufacturer or an EU corporate affiliate with operations in a market that maintains an “important data” catalogue or a sectoral residency mandate cannot reliably consolidate and scale that operation’s engineering, quality, safety, telemetry, or workforce data at its European headquarters. This could lead to circumstances in which the EU corporate parent (or board of directors) are responsible for governing a foreign affiliate whose operational data it cannot see.

The compounding problem is that EU law increasingly requires European companies to do exactly what third-country measures prevent. Obligations to identify and address adverse impacts across global value chains, to report on sustainability performance at group level, to maintain product traceability and execute cross-border safety recalls, to run group-wide financial terrorist financing, sanctions, or other criminal law screening, and to manage ICT third-party risk across the group all presuppose that a European parent can gather and analyse data from its non-EU operations[10]. Third-country localisation mandates combined with data transfer restrictions therefore do not only harm European competitiveness; they directly impede compliance with European law.

[9] Vietnam, Law on Cybersecurity (2025), effective 1 July 2026; Decree No. 333/2026/ND-CP (19 August 2026). See Annex II (Vietnam), and Global Data Alliance, Submissions in Vietnam (2020-2025), at https://globaldataalliance.org/resources-results/?pub_type=&location=loc-vietnam.

[10] See in particular Directive (EU) 2022/2464 (Corporate Sustainability Reporting Directive), requiring consolidated group-level sustainability reporting that covers subsidiaries established outside the Union; Directive (EU) 2024/1760 (Corporate Sustainability Due Diligence Directive), requiring identification and mitigation of adverse impacts across a company’s own operations, those of its subsidiaries, and its chains of activities; Regulation (EU) 2022/2554 (DORA), requiring group-wide ICT third-party risk management

1.2 Discriminatory certification, licensing, and procurement conditions

These measures condition certification or procurement eligibility on criteria unrelated to the security or performance of the service — the supplier's nationality, ownership structure, the citizenship of its personnel, or its immunity from foreign legal process.

Example 1.2(a) — Republic of Korea: the Cloud Security Assurance Program (CSAP)	
Sector	Public sector (central, provincial, and local government, including public universities and health institutions); financial services
Data category	All data associated with public-sector information systems; personal credit information; location and cartographic data
Third country	Republic of Korea
Practical impact	CSAP, elevated from administrative guidance to legal requirement by a March 2022 revision to the Cloud Computing Promotion Act, imposes several requirements that do not track international practice: physical network separation (rather than logical separation, the recognised standard for isolating sensitive workloads in multi-tenant environments); mandatory use of Korean-developed encryption algorithms (ARIA, SEED) in place of internationally recognised algorithms; physical data residency in Korea; and local operations and management personnel. The 2023 three-tier reform has not resolved the problem: because any system containing personal information as broadly defined under PIPA is classified Medium or High, the Low tier covers only a narrow subset of public systems. To date only a small number of non-Korean providers have achieved CSAP certification, and only at the Low tier. Separately, Korea maintains a uniquely restrictive licensing regime for cartographic and location-based data, and has never approved a licence to transfer such data abroad. In financial services, the Financial Services Commission prohibits overseas processing of personal credit information and has historically required cloud systems to sit on servers located in Korea; network segregation rules have been interpreted by the Financial Supervisory Service to treat global support access as a violation.[11]
Isolated or systemic	Systemic and structural. Successive reforms have been piecemeal; the core eligibility architecture is unchanged.

We highlight Korea because it is the clearest available illustration of a general point that bears directly on this consultation: an eligibility framework built on residency, national encryption standards, and local personnel produces near-total foreign exclusion in practice even where it is not framed as exclusion in law. Three certifications, all at the lowest tier, after a decade of the programme's operation is the measurable outcome.

The Korean framework is also being consolidated rather than relaxed. In April 2026 the Ministry of Science and ICT and the National Intelligence Service announced that CSAP and the separate NIS security verification would be merged into a single NIS-led public cloud security verification framework, with revised National Cloud Computing Security Guidelines, a one-year grace period, and full implementation in the second half of 2027. The technical criteria, the relationship to Korea's National Network Security Framework, and the treatment of foreign providers

---

and incident reporting; Regulation (EU) 2023/988 (General Product Safety Regulation) and Regulation (EU) 2023/1115 (Deforestation Regulation), each requiring traceability and, in the former case, cross-border recall capability; and Regulation (EU) 2024/1624 together with Directive (EU) 2024/1640 (the anti-money-laundering package), requiring group-wide policies, controls and procedures, including information sharing within the group. Each of these obligations is imposed on the European parent and each presupposes that the parent can obtain data from operations located outside the Union.

[11] Cloud Computing Promotion Act, as revised in March 2022, elevating CSAP from administrative guidance to a legal requirement; KISA, Cloud Security Assurance Program certification criteria and the 2023 three-tier (Low/Medium/High) classification scheme; Personal Information Protection Act; Credit Information Use and Protection Act, art. 17; Regulation on Supervision of Electronic Financial Transactions, art. 14-2-8; and the FSC no-action letter on whether direct access by an overseas trustee to a domestically located server violates art. 15(1)(5) of the Regulation on Supervision of Electronic Financial Transactions, at https://better.fsc.go.kr/fsc_new/replyCase/OpinionDetail.do?stNo=11&muNo=86&muGpNo=75&opinionIdx=2261. See Annex II (Republic of Korea) for the fuller account, including the September 2024 National Intelligence Service indication that encryption requirements would be relaxed up to the Medium tier, which has not been reflected in any formal amendment to CSAP.

all remain unresolved. There have also been reports of proposals to extend CSAP beyond public procurement into a private-sector certification mechanism, which would widen the reach of the criteria described above rather than narrow them. We encourage the Commission to seek clarity on these points before the framework is settled, since the design choices are being made now.

1.3 Third-country government access to sensitive data

The consultation asks specifically about risks linked to third-country access to sensitive data transferred across networks. We address this question in relation to personal data and non-personal data below.

In terms of personal data protection, the central question is whether government access regimes are grounded in law and subject to independent oversight. Putting aside the legitimate exceptions and limitations for national security or intelligence gathering purposes that many economies (including EU member states) maintain, there is an emerging international legal consensus regarding appropriate safeguards – a consensus that is perhaps best represented by the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, adopted in December 2022.[12] Presumptively, economies that have subscribed to that OECD Declaration should not be considered to represent a "high risk" in this context. Relevant safeguards include whether:

(1) There are legal protections against unlawful governmental acts of search and seizure;
(2) Access is authorised by published law rather than administrative discretion;
(3) Access is generally subject to prior or subsequent independent review;
(4) Affected parties have meaningful redress;
(5) Providers may publish transparency reporting; and
(6) Providers may seek review or redress (either administratively or judicially).

In terms of non-personal data protection, the central questions relate to standards of trade secret protection, and whether governmental acts of misappropriation are subject to challenge and legal redress.

Assessed against those markers, several of the regimes described above present acute risks. For example, China's PIPL Articles 42–43 authorise retaliatory measures against overseas entities on national security or public interest grounds, with no independent review. "Important data" designations under China's Data Security Law are made administratively, at national and sub-national level, without publication requirements or challenge mechanisms. Under both of these laws, the presumptive ability of the Chinese government to access personal data is not subject to significant due process constraints. Similar concerns arise in jurisdictions such as Vietnam.[13]

Finally, we underscore that mitigations that actually reduce exposure are technical and contractual rather than jurisdictional: encryption with customer-controlled key management, data minimisation and even residency by design where the sensitivity of the workload warrants it, and published transparency reporting. Each of these is verifiable by audit, each can be written into a procurement specification, and each is available from European and non-European suppliers alike[14].

---

[12] OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD/LEGAL/0487 (adopted 14 December 2022), at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487. The Declaration was adopted by OECD members and the European Union, and its common principles address legal basis, legitimate aims, approvals, data handling, transparency, oversight and redress. It is the closest thing to an agreed international benchmark against which government access regimes can be compared, and it has the advantage for present purposes of being a standard the EU itself has subscribed to.

[13] We recognise that some voices raise concerns about US authorities, in particular Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the Clarifying Lawful Overseas Use of Data (CLOUD) Act. Contrary to these stated concerns, however, the CLOUD Act does not create new surveillance authority; it clarifies the reach of existing compulsory process, establishes a mechanism for providers to challenge orders that conflict with the law of another jurisdiction, and creates a framework for executive agreements under which partner governments obtain reciprocal benefit. Section 702 operates on the basis of individualised targeting decisions, subject to annual certification and to judicial approval of targeting and minimisation procedures, and is overseen by the Foreign Intelligence Surveillance Court, the Privacy and Civil Liberties Oversight Board, and the Congress. Like the EU, the United States is also an adherent to the OECD Declaration.

[14] These controls are already expressed in internationally recognised, auditable standards that apply without reference to the nationality of the supplier: ISO/IEC 27001:2022, including Annex A controls 5.30 (ICT readiness for business continuity) and 8.14 (redundancy of information processing facilities); ISO/IEC 27017 and ISO/IEC 27018 on cloud-specific controls and the protection of personal data in public cloud; ISO/IEC 27031 on ICT readiness for business continuity; and ISO 22301 on business continuity management systems. Expressing resilience, exit and continuity requirements in this form has two advantages over a nationality test:

1.4 Overly broad data classification

Several EU trading partners have originated new data classifications that unduly restrict cross-border data access or transfers. This includes concepts such as "important data" and "core data" (China), "sovereign data" (Nigeria), "strategic interests of the state" (Kenya), "Regulatory Data" (India, securities sector), and "Core Data" and "Important Data" under Vietnam's draft Data Security Law, published in August 2026, which would require classification, risk assessment and transfer decisions to be filed with the Ministry of Public Security and would apply an automatic classification uplift based on aggregation alone.[15] Because the categories are elastic, companies cannot determine ex ante whether a given dataset may lawfully leave the jurisdiction. Likewise, as discussed below, many jurisdictions automatically treat health- or finance-related data as "sensitive" or "highly sensitive," and impose broad data localisation mandates or transfer restrictions to any such data. Such measures have a disproportionate impact on EU-based financial service providers, biopharmaceutical companies, and medical technology firms (among others).

1.6 Sector-specific restrictions

Financial services and banking face among the strictest and most widespread sectoral requirements, with regulators in India (Reserve Bank of India payments directive), Indonesia (OJK), Nigeria (Central Bank of Nigeria), Saudi Arabia (SAMA), Türkiye (BDDK and CBRT), Chile (CMF RAN 20-7), Mexico (CNBV), Pakistan (State Bank of Pakistan), and China all requiring some form of local storage or processing.[16] Health data faces localisation in the UAE and South Africa, among others. Public-sector and government data faces localisation in Brazil, Bolivia, Nigeria, the Philippines, South Africa, Türkiye, and Pakistan.

Restrictions are also particularly pronounced in relation to health data. The UAE prohibits the storage or processing of patient health data outside the country by default, and the Abu Dhabi Healthcare Information and Cybersecurity Standard extends that restriction to cloud deployment; Taiwan reportedly expects medical records to be held domestically and has moved to bar transfers of clinical-trial and pharmacy data in some cases; Vietnam's Decree 102/2025/ND-CP on medical data management applies extraterritorially and imposes strict consent and cross-border assessment requirements; and India, Türkiye and Kenya each treat health records as a category warranting residency or transfer restriction[17]. For EU-based

---

compliance can be verified by an accredited third party, and the same requirement can be applied to European and non-European providers on identical terms.

[15]See Annex II to this submission for the underlying measures in each jurisdiction, and Global Data Alliance, Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers (30 October 2025), at https://globaldataalliance.org/wp-content/uploads/2025/10/10302025gdante.pdf. On "important data" and "core data", see the PRC Data Security Law and the associated national and sub-national catalogues, and Vietnam's Law on Protection of Consumer Data in the Digital Environment; on "sovereign data", see NITDA's 2019 Nigeria Data Sovereignty guidelines and the draft National Cloud Policy 2025, at https://nitda.gov.ng/wp-content/uploads/2025/10/National-Cloud-Policy-2025-Oct2-2025.pdf; on data affecting the "strategic interests of the state", see Kenya's Data Protection (General) Regulations, at https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf; on "Regulatory Data", see SEBI, Cybersecurity and Cyber Resilience Framework (August 2024), at https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html; and on "critical" and "sensitive" data, see Pakistan's draft Personal Data Protection Bill (2023), s. 27(1), at https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf.

[16]See Annex II to this submission for the measure-by-measure detail, and Global Data Alliance, Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers (30 October 2025). The principal instruments are: India - RBI, Storage of Payment System Data, DPSS.CO.OD No. 2785/06.08.005/2017-2018 (6 April 2018), at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0; Indonesia - Bank Indonesia Regulation (PBI) 23/7/2021 and OJK Regulation No. 9/POJK.03/2016; Nigeria - Central Bank of Nigeria guidelines; Saudi Arabia - NCA Essential Cybersecurity Controls ECC-1:2018, 4-2-3-3, and SAMA payment-processing requirements; Türkiye - BDDK Regulation on Banks' Information Systems and Electronic Banking Services, art. 11(4) (Official Gazette No. 31069, 15 March 2020), and the CBRT Communiqué on Information Systems of Payment and Electronic Money Institutions, art. 21 (Official Gazette No. 31676, 1 December 2021); Chile - CMF, Recopilación Actualizada de Normas, ch. 20-7; Mexico - CNBV rules under the Fintech Law (2021); Pakistan - State Bank of Pakistan, Framework on Outsourcing to Cloud Service Providers (2023), at sbp.org.pk/bprd/2023/C1-Annix-A.pdf; and China - the Cybersecurity Law, Data Security Law and PIPL, as described in Annex II.

[17] UAE Federal Law No. 2 of 2019 concerning the Use of Information and Communication Technology in Healthcare; Abu Dhabi Healthcare Information and Cybersecurity Standard - see Global Data Alliance, Comments on the Abu Dhabi Healthcare Information and Cybersecurity Standard (2024), at https://globaldataalliance.org/wp-content/uploads/2024/10/10162024gdaabdhealthdata.pdf; Vietnam, Decree No. 102/2025/ND-CP on Medical Data Management (in force 1 July 2025), at https://chinhphu.vn/?pageid=27160&docid=213607; and, on Taiwan, Chambers & Partners, Taiwan Data Protection & Privacy Guide (2025), at https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/taiwan, reporting the 2024 TFDA draft rule restricting transfers of clinical-trial and pharmacy data to specified jurisdictions. See Annex II.

biopharmaceutical companies, medical technology firms, and clinical research organisations, the cumulative effect is that data generated at trial sites, in post-marketing pharmacovigilance, and in device servicing cannot be consolidated for analysis. That degrades the demographic representativeness of clinical evidence, delays safety-signal detection, and impedes the regulatory submissions that EU law itself requires.

Two further measures should be recorded in this category. South Africa's Health Information Regulations under the Protection of Personal Information Act, in force since 6 March 2026, prohibit a responsible party from transferring a data subject's health information to a third party in a foreign country unless one of the section 72(1) requirements is met; the regulations reach insurers, medical schemes and their administrators, managed healthcare organisations, pension funds and employers. In Brazil, the Ministry of Health launched a phased Sovereign Cloud for the SUS health system in August 2026, beginning with the national health-data network, on the stated basis that covered health data will be stored and processed in Brazil under Brazilian jurisdiction. Both measures affect European insurers, reinsurers, medical technology firms and clinical research organisations directly.

Such cross-border data restrictions present particular challenges in the financial and health context, precisely because data localisation mandates and transfer restrictions tend to *exacerbate* operational risk, *worsen* regulatory blind spots, *undermine* cross-border innovation and product safety testing, and *inhibit* supervisory access to information.

Implications for the Design of Any EU Response

We offer the following observations in a spirit of support for the Commission's objectives.

2.1 The EU's leverage depends on the coherence of its own position

The measures documented in Section 1 share a common design feature: they condition access on origin, ownership, nationality, corporate structure, or immunity from foreign legal process, rather than on demonstrated security and performance. That common feature is the basis on which the EU can credibly challenge them — in bilateral engagement, in trade negotiations, and in the WTO.

That leverage is diminished to the extent the EU adopts instruments built on the same design feature. Where EU frameworks gate the highest assurance levels on ownership, control, or headquarters criteria rather than on security posture, they supply third countries with both a template and a defence. Regrettably, these features are increasingly present in regulatory frameworks like the Cloud & AI Development Act proposal, the Industrial Accelerator Act proposal, and the Public Procurement Act proposal.

A request that Korea align CSAP with international practice, or that Vietnam narrow its in-country hosting mandates, is harder to press if the answer available is that the EU applies analogous criteria.

This is not an argument against EU investment in European technological capability. Non-discriminatory grants, subsidies, tax incentives, government-backed loans and guarantees, high-performance computing investment, deepening of the digital single market, regulatory simplification, and promotion of open standards are all available, effective, and consistent with international obligations. The distinction we draw is between measures, on the one hand, that actually build European capability, capacity, and resilience, and measures, on the other, that exclude best-in-class technology on the basis of origin.

2.2 Third countries are watching the EU's choices

Trade bodies in Australia, Canada, and Japan have already publicly raised concerns about exclusion from European technology promotion initiatives[18]. Those are trusted partners whose alignment the EU needs in order to press the barriers described in Section 1. The composition of the coalition the EU can assemble against the foreign data barriers described in this submission depends in substantial part on whether those partners see the EU as a defender of open digital markets or as another participant in their restriction.

[18] Foo Yun Chee, "Australia, Canada, Japan trade bodies fret over being left out in made-in-Europe drive", Reuters (Brussels, 8 June 2026). See also the joint letter, "Plea for transatlantic ties, not technological autarky" (on file with the GDA).

RECOMMENDATIONS

1. **Define "data leakage" precisely.** The term should be confined to unlawful exfiltration, compelled disclosure or transfer of proprietary source code or trade secrets, mandatory public release of sensitive data without due process, and transfers in breach of applicable law. It should not capture ordinary, lawful, contractually governed commercial transfers, which are the mechanism by which European companies operate globally. A broad definition would classify routine intra-group operations as a sovereignty threat.

2. **Adopt an outcome- and risk-based test for third-country data risk.** Assess providers' encryption and key management architecture; providers' access controls and logging safeguards, as well as contractual commitments to remain accountable for high standards of data protection and security; and providers' policies to resist unlawful government access requests and to notify customers; . Use adherence to the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities as a structuring reference. These criteria are verifiable; nationality is a proxy that is neither necessary nor sufficient.

3. **Assess whether to establish a standing EU inventory of third-country data barriers.** The EU does not publish on an annual and systematic basis a catalogue of foreign data-related trade barriers comparable to the annual US National Trade Estimate exercise[19]. Doing so would give the Commission an evidentiary base for negotiation, allow prioritisation by economic impact, and make the problem visible to Member States, Parliament, and EU business stakeholders.

4. **Prioritise cross-border data and open digital market provisions in trade negotiations.** Ongoing and prospective negotiations — including with India and Indonesia, and in the context of the EU's wider engagement in the Indo-Pacific — are the most direct available instrument for addressing the measures in Section 1. Provisions should, at minimum: prohibit restrictions greater than necessary to achieve a legitimate public policy objective; prohibit less favourable treatment of cross-border transfers relative to domestic ones; prohibit sectoral carve-outs that exclude financial services; prohibit the application of origin-based criteria in certification, procurement, or market access provisions for digital technologies; and require transparent, published, reviewable administration of any approval regime.

5. **Expand adequacy and interoperability infrastructure.** All of the following would reduce friction for European organisations operating in third markets: additional adequacy decisions, a pathway to achieve interoperability between EU transfer mechanisms and Global Cross-Border Privacy Rules Forum mechanisms, and alignment with the ASEAN Model Contractual Clauses..

6. **Commission an EU-specific economic assessment.** No study exists that models the cost to EU GDP, productivity, and employment of: (a) third-country data restrictions that impact European industries; and (b) the costs to EU industries of EU-side sovereignty requirements, including compliance and switching costs. The Oxford Economics work referenced in Annex I provides a methodology but covers Asia-Pacific only. An EU equivalent would materially improve the evidence base for any subsequent proposal.

7. **Enforce and simplify existing instruments before creating new ones.** The GDPR, NIS2, the Data Act, DORA, and the Cybersecurity Act already provide a comprehensive framework for data protection, security, resilience, and switching. Consistent enforcement across Member States, and simplification where instruments overlap, would deliver more than an additional parallel layer of requirements — and would avoid compounding the fragmentation that European organisations already navigate.

8. **Publish the evidence base.** We understand that individual responses will not be published. We would encourage the Commission to publish an anonymised synthesis of the barriers identified. Doing so would

[19] The US exercise is conducted under s. 181 of the Trade Act of 1974, 19 U.S.C. 2241, and proceeds by annual public solicitation of stakeholder evidence. See, e.g., USTR, Request for Comments on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report, 90 Fed. Reg. 44448 (15 September 2025), at https://www.federalregister.gov/documents/2025/09/15/2025-17782/request-for-comments-on-significant-foreign-trade-barriers-for-the-2026-national-trade-estimate. For an illustration of the resulting evidentiary record on cross-border data measures specifically, see Global Data Alliance, Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers (30 October 2025). The GDA would be glad to assist the Commission in scoping an equivalent EU instrument.

strengthen the EU's hand in bilateral engagement, allow stakeholders to corroborate and supplement the record, and support parliamentary and Member State scrutiny of any resulting proposal.

CONCLUSION

European organisations face real, documented, and systemic barriers to accessing, using, and repatriating data in third countries. Those barriers impose costs on European competitiveness, and – because EU law increasingly imposes group-level duties that presuppose global data access – they impede compliance with EU law itself.

The design feature that makes those foreign measures objectionable is that they condition access on origin, ownership, and nationality rather than on demonstrated security and performance. That is the standard by which the EU can most effectively challenge them, and it is the standard we encourage the Commission to apply to its own instruments. Durable digital sovereignty is best achieved through capability, collaboration, resilience, and trust – all backed by risk management frameworks and relevant technical and contractual controls. GDA stands ready to provide further technical expertise, case studies, and economic analysis as the Commission develops its assessment. We would welcome the opportunity to discuss this submission with the relevant services.

ANNEX I

ANNEX I – OVERVIEW OF CROSS-BORDER DATA POLICY AND STATISTICS

The GDA has published a set of Cross-Border Data Policy Principles to help inform domestic and international policymaking in relation to measures that have an impact on cross-border data transfers.[20] The principles are summarised and excerpted below:

- Principle 1: Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders
- Principle 2: Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices
- Principle 3: Any rules impacting cross-border data transfers should be non-discriminatory
- Principle 4: Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary
- Principle 5: Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices
- Principle 6: Countries should work together to create compatible trust-based frameworks support the seamless and responsible movement of information across borders

Principle 1: Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders

A **presumption favoring the movement of data across digital networks** reflects the reality of international economic relations today: Data moves seamlessly and securely across globally or regionally distributed cloud-based digital networks that do not match up neatly with national boundaries.[21]

Digital networks lie at the heart of our interconnected global economy. They support millions of daily transactions occurring all over the world, across every sector and at every stage of the value chain, including at the R&D, product design, regulatory approval, manufacturing, finance, marketing, sales, and post-sale service stages. Countries should not disturb the longstanding practice and presumption that data can move seamlessly and responsibly across these networks.

Cross-border data transfers are already estimated to contribute trillions of dollars to global GDP.[22] Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.[23] The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance. Many Regional Trade Agreements (RTAs) reflect this presumption.[24]

Principle 2: Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices:

---

[20] GDA Cross-Border Data Policy Principles, https://globaldataalliance.org/wp-content/uploads/2021/07/03022021gdacrossborderdatapolicyprinciples.pdf

[21] *See e.g.,* Research Institute of Economy Trade and Industry of Japan, *The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies*, p. 4 (2019), at: https://t20japan.org/wp-content/uploads/2019/03/t20-japan-tf8-4-digital-economy-economic-development.pdf

[22] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.

[23] *Ibid.*

[24] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf

The second pillar of an international policy consensus on data transfers involves **transparent, accountable, and evidence-driven regulatory practices**. Adhering to these practices helps ensure that any rules impacting cross-border data are well justified, enjoy the support and trust of the public, and do not unintentionally harm international commerce and innovation.

In the design, development, issuance, implementation, and review of measures that may impact cross-border data transfers, governments should:

- Be transparent;[25]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[26]
- Analyze that evidence according to sound, objective, and verifiable methods (including regulatory impact assessments—as discussed further under Principle 4 below);
- Provide opportunity for input from the public, experts, and interested stakeholders;[27] and
- Include other procedural safeguards and due process.[28]

A robust and thorough set of regulatory good practices to evaluate the foregoing factors can help policymakers improve the quality and effectiveness of proposed measures, and eschew unintended consequences that may be particularly pronounced when such measures unnecessarily restrict cross-border data transfers.[29]

Principle 3: Any rules impacting cross-border data transfers should be non-discriminatory

The third pillar supporting an international policy consensus on data transfers requires a **commitment to principles of non-discrimination and national treatment in terms of the nationality of persons, products, services, or technologies**. Subject to legitimate public policy limitations, a rule impacting cross-border data transfers would raise

[25] For example, governments should adopt pre-publication and final publication processes that specify implementation timelines, how various substantive concerns are addressed, the evaluation of evidence and expert input, and alternatives or other steps taken to mitigate negative impacts of the measure.

[26] For example, governments should seek out the best reasonably obtainable information relevant to the proposed policy, be transparent regarding information sources and any significant assumptions, and use sound statistical methodologies in analyzing that information.

[27] For example, governments should adopt procedural safeguards to ensure that any proposed measure that would impact cross-border data transfers is well-informed through input from experts, interested stakeholders, and the public. Such safeguards include:

- Advance publication, including an explanation of the measure's underlying objectives, the statutory or other legal basis underlying those objectives, and how the measure would achieve those objectives in light of available evidence;
- Opportunities for public comment; and
- Use of expert advisory groups, public-private consultative mechanisms, evaluation of best practices, and other means of protecting the public interest in thoughtful, deliberative policymaking.

[28] For example, governments should offer a retrospective review mechanism that allows for future enhancements or revisions of the measure, including from the perspective of cross-border data policy. The mechanism should permit the government to evaluate:

- How effective the measure has proven in achieving stated objectives;
- Whether changed circumstances or new information would justify a review of some aspects of the measure; and
- Whether there are any new opportunities to eliminate unnecessary regulatory burdens.

[29] Commentary on good regulatory practices in relation to cross-border data policy includes: OECD, *Trade in the Digital Era* (2019), http://www.oecd.org/going-digital/trade-in-the-digital-era.pdf; World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, White Paper (2020), p. 18 https://www.jmfrri.gr.jp/content/files/Open/Related%20Information%20/WEF_May2020.pdf ("[P]olicy-makers should ensure that domestic measures affecting data are enacted in a transparent manner that allows opportunities for broad stakeholder input; are evidence-based and consider the technical and economic feasibility of requirements; require the publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and are targeted and proportionate, and restrict trade as little as possible."); UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (2016), at: https://unctad.org/system/files/official-document/dtlstict2016d1_summary_en.pdf (recommending that the impact on smaller businesses be assessed with respect to proposed data protection legislation and data flow restrictions); Indian Council for Research on International Economic *Relations, Regulatory Burden on Micro, Small and Medium Businesses Due to Data Localisation Policies*, (Sept. 2019), at http://icrier.org/pdf/Regulatory-Burden.pdf; OECD, *Going Digital: Shaping Policies, Improving Lives* (2019), Molinuevo & Saez, Regulatory Impact Assessment Toolkit, The World Bank (2014), at: https://openknowledge.worldbank.org/bitstream/handle/10986/17255/9781464800573.pdf?sequence=1; ICTSD, Advancing Sustainable Development Through Services Regulation (2017)

concerns if it distorted the market or altered conditions of competition based on the national origin of the persons, the products or services, or the technologies involved. In some cases, concerns may also arise if data transfer rules are designed to provide economic advantages to transfers within a country's borders, and to domestic persons, their products or services, or their technologies, than are afforded to cross-border transfers and non-national persons, products, services, or technologies. Likewise, countries should refrain from discriminatory treatment among sectors, for example by blocking or impeding data transfers in particular sectors.

For the foregoing reasons, any rules relating to cross-border data transfers should not modify conditions of competition or serve protectionist ends by:

- Discriminating against foreign persons, products, or technologies;
- Treating data transfers into or out of the country less favorably than data transfers within the country; or
- Discriminating among different technologies.

Such measures should also not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade. As outlined above and in many trade agreements negotiated to date, principles of non-discrimination and national treatment are critical to advancing an international policy consensus on data transfers.[30]

Principle 4: Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary

The fourth pillar underlying an international policy consensus on data transfers should embody a commitment to **specifically tailor any rules that would impact cross-border data transfers to legitimate and justified policy objectives and to refrain from imposing restrictions on data transfers that are greater than necessary**.

This standard is reflected in many trade agreements negotiated to date[31] and in the administrative and regulatory processes adopted by many governments. As part of their administrative and regulatory practice, governments typically evaluate costs, benefits, and reasonably available alternatives as part of their assessment of whether proposed rules are necessary to achieve a specific public policy objective. Often referred to as regulatory impact assessments, these regulatory evaluations are particularly salient to data transfer restrictions, which can result in excessive economic costs and impacts. Such assessments should evaluate from a cross-border policy perspective:

- The particular public policy outcome that the proposed measure is intended to achieve;
- Whether the cross-border data restrictive features of the proposed measure are needed to achieve that outcome;
- Whether other regulatory or non-regulatory alternatives could feasibly address that need or achieve that outcome with fewer data transfer restrictions;
- The potential impacts of various alternatives over time (e.g., economic, social, environmental, public health, and safety effects) on the government, enterprises, and other persons who depend upon the ability to access technologies and transfer data across borders;
- The grounds for concluding that a particular policy alternative is preferable to others.

As a matter of international and domestic law, this type of assessment is critical to evaluate the disruptive potential of data transfer restrictions in an international commercial ecosystem. Regulatory impact assessments can help answer questions for policymakers in the process. For example, policymakers sometimes underestimate the costs of transfer restrictions, while overestimating their benefits. Policymakers also sometimes lack adequate information regarding non-regulatory solutions—e.g., evidence regarding internal controls that companies have adopted to keep data secure and private and to make it readily available in response to valid investigatory or regulatory requests. In some cases, there has been little substantiation or quantification of the risks that the measure purports to address,

[30] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[31] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf

and little analysis of whether the proposed measure (and its most restrictive aspects) are necessary and proportionate to address any such risks.[32]

This analysis is important because **how** data is protected is typically more salient than **where** it is stored.
As outlined above and in many agreements negotiated to date, rules impacting cross-border data transfers should be necessary to achieve a legitimate and justified public policy objective and impose no more restrictions on data transfers than necessary.

Principle 5: Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices

The fifth pillar incorporates the accountability model, first established by the Organisation for Economic Co-operation and Development (OECD) and subsequently endorsed and integrated into other legal systems and privacy principles.[33] This model provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data transfers. Under legal frameworks that adopt the accountability model, organizations are required to implement procedures to ensure that data they transfer outside of the country continues to be protected, regardless of where it is stored.

Accountability models comport with a general view that the standards of protection applicable to data in the country of origin should continue to attach to the data as it is transferred across digital networks, including to data centers in other jurisdictions. When data subjects in the country of origin can be assured that the data protections they expect in the country of origin also apply in countries to which the data is subsequently transferred, it obviates one frequent claimed basis for data localisation measures.

Wherever possible, countries developing rules that impact data transfers should support and rely upon international consensus-based standards, rather than advance unique, single-country standards that may be incompatible with international standards. Such an approach helps facilitate accountability by increasing alignment among countries and reducing the risks of regulatory inconsistency among countries.

Principle 6: Countries should work together to create compatible trust-based frameworks support the seamless and responsible movement of information across borders

The sixth pillar is for governments to take steps to build interoperable systems that facilitate an international consensus on data transfers.

Continuing to enjoy the transformative benefits enabled by the seamless and responsible movement of data requires a commitment to digital trust. Building digital trust requires both domestic and international action. That means domestic and international legal frameworks help economies realize the benefits of cross-border data transfers and cloud-based technology without sacrificing expectations of privacy,[34] security,[35] and safety.[36] In the international context, this may include:

---

[32] *See e.g.,* OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Art. 12 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf ("Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.")
[33] *See* OECD, *Guidelines governing the protection of privacy and transborder flows of personal data*, Arts. 14-18 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[34] Ensuring continued benefits from cross-border data transfers depends on users' faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of cloud-based technologies, providers must be free to move data across borders in an efficient and commercially viable manner.
[35] Users must be assured that governments and enterprises understand and properly manage the risks inherent in storing and running applications in the cloud. This requires implementing cutting-edge cybersecurity solutions without being required to use specific technologies.
[36] Laws online must provide meaningful deterrence and clear causes of action to deal with online threats and cybercrime. Legal systems should provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud.

- **Cross-Border Interoperability Mechanisms:** An important complement to international regulatory convergence efforts are mechanisms that ensure that different national legal regimes are "interoperable"—i.e., compatible—with one another. In the context of personal information protection, such mechanisms may include (among other things) private codes of conduct; contractual arrangements; certifications, seals, or marks; white-listing or mutual recognition arrangements; and participation in government programs. These coordination mechanisms help bridge current gaps in international privacy norms while facilitating the safe and secure transfer of personal information.

- **International Frameworks Regarding Regulation of Data Transfers and Localisation:** Another trust-building mechanism involves negotiating agreements to prohibit unnecessary data transfer restrictions and data localisation mandates. Thus, these agreements reaffirm the core principle that the seamless and responsible movement of information across digital networks is foundational to a healthy, integrated global economy. These agreements also can more precisely define the relationship between rules impacting data transfers and specific policy objectives. Overall, these agreements support legal certainty, helping grow digital trust, economic development, and technological innovation.[37]

[37] To date, many countries have made, or are negotiating, such commitments under international agreements, including under the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CP-TPP), the Digital Economy Partnership Agreement (DEPA), the Australia-Singapore Digital Economy Agreement (DEA), the UK-Japan Comprehensive Economic Partnership Agreement, the WTO Joint Statement Initiative digital trade negotiations, and various other agreements negotiated by the EU. This positive trend should continue.

ANNEX II

ANNEX II – COUNTRY-BY-COUNTRY ANALYSIS

The GDA provides below a country-by-country summary of measures of concern in relation to cross-border data transfer restrictions and data localisation mandates.

National policies on cross-border data transfers and data localisation are – alongside economic profile, level of internet and broadband access, and level of computer literacy – important determinants of the ability of economies to sustain economic and scientific activity. The types of cross-border data policies that can undermine that ability take many forms. Sometimes the policies expressly require data to stay in-country. Sometimes, these policies impose unreasonable conditions on sending data abroad or prohibit such transfers outright. In other cases, the policies require the use of domestic data centers or other equipment, or the need for such data centers to be operated by local vendors. Sometimes these measures cite privacy or security as their underlying purpose, but often the measures are designed in a manner that also suggests alternative, protectionist purposes. For example, these measures may:

- Reflect a choice of policy tools that are significantly more trade-restrictive than necessary to achieve the stated public policy goal;

- Constitute unnecessary, unjustified and/or disguised restrictions on data transfers across borders, or may be more restrictive of data transfers than necessary; or

- Treat cross-border data transfers less favorably than domestic data transfers.

Such improper data localisation mandates and cross-border data restrictions are frequently imposed in several specific contexts, including in cybersecurity, privacy, health, and financial contexts. Ironically, it is precisely in these contexts that cross-border data restrictions can do the most harm.

Below, we summarise measures of concern in several economies of priority interest: Brazil, China, India, Indonesia, the Republic of Korea, Saudi Arabia, Türkiye, the UAE, and Vietnam. We also summarise measures of concern in other markets of interest: Bolivia, Canada, Chile, Japan, Kenya, Mexico, Morocco, Nigeria, Pakistan, the Philippines, South Africa, Taiwan, and Thailand.

Markets of Priority Interest

A. Brazil

We outline below issues worthy of future monitoring in Brazil's cross-border data policy landscape. Please see here for submissions on Brazil's cross-border data measures and here for its ranking in the GDA Cross-Border Data Policy Index.[38]

Personal Data Protection and Cross-Border Data: On August 23, 2024, the Brazilian Data Protection Authority (ANPD) adopted Resolution CD/ANPD No. 19/2024, establishing rules governing international transfers of personal data and approving Brazilian standard contractual clauses. The Regulation addresses adequacy decisions and transfers supported by specific contractual clauses, standard contractual clauses, and global corporate rules, while preserving the other transfer mechanisms authorized by Article 33 of the LGPD. In January 2026, Brazil and the European Union adopted mutual adequacy decisions: ANPD Resolution No. 32/2026 recognises the European Union as providing an adequate level of protection, while the European Commission adopted a corresponding adequacy decision for Brazil. As a result, personal data may now flow between Brazil and the EU without additional contractual or other transfer safeguards.[39]

Data and Server Localisation Requirements: Brazil's current federal cloud-procurement framework contains data-residency requirements for federal executive bodies and entities participating in the federal Information Technology Resources Administration System (SISP). Portaria SGD/MGI No. 5.950/2023 provides that data processed in cloud environments must be stored in data centers located in Brazilian territory. Processing may occur in data centers outside Brazil only where an updated backup copy is stored in data centers located in Brazil, subject to the other requirements of the framework. These requirements constrain the ability of covered federal entities to rely exclusively on cloud infrastructure located outside Brazil.[40]

Restrictions on IoT Permanent Roaming: Brazil continues to restrict permanent roaming for machine-to-machine (M2M) and Internet of Things (IoT) deployments. Under ANATEL's current competition guidance, a user or M2M/IoT device cannot use foreign SIMs remain connected to Brazilian networks for more than 90 days. As a result, European IoT providers may be forced to migrate devices to a Brazilian operator, local SIM, or other arrangement.[41]

Sovereign Cloud Initiatives (2026): In August 2026 Brazil advanced two public-sector cloud initiatives framed around digital sovereignty. On 11 August, the Ministry of Health and Serpro began a phased initiative to migrate strategic SUS systems and data to sovereign cloud infrastructure, beginning with CadSUS and the National Health Data Network (RNDS). Official materials state that data hosted in the sovereign environment will be stored and processed in Brazilian territory and subject to Brazilian law. The government also launched the Nuvem Brasileira initiative to develop national cloud infrastructure with a first public consultation on 3 September 2026. Government statements indicate that the initiative is not intended to exclude technologies or providers based solely on foreign origin and contemplates the integration of technologies from different suppliers,[42] although the initiative is intended to increase national control over data and infrastructure.[43]

---

[38] Global Data Alliance, Submissions to Brazil (2020-2025), https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-brazil&sector=&language=&posts_filtered=1; Global Data Alliance, Cross-Border Data Policy Index (2023), https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf.

[39] Autoridade Nacional de Proteção de Dados (ANPD), Resolução CD/ANPD nº 19, de 23 de agosto de 2024, https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-19-de-23-de-agosto-de-2024; ANPD, "Brasil e União Europeia reconhecem adequação mútua em matéria de proteção de dados pessoais" (23 Jan. 2026), https://www.gov.br/anpd/pt-br/assuntos/noticias/brasil-e-uniao-europeia-reconhecem-adequacao-mutua-em-protecao-de-dados-pessoais; European Commission, "The EU and Brazil conclude agreements to create the biggest area of free and safe data flows in the world" (27 Jan. 2026), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_229/IP_26_229_EN.pdf

[40] Secretaria de Governo Digital, Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, arts. 1, 3 and Annex I § 5.4.5, current text updated 19 June 2026, https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/vigentes/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023.

[41] ANATEL, Resolução nº 783, de 3 de setembro de 2025, art. 66 § 4 (defining prohibited permanent roaming as more than 90 consecutive days, including M2M/IoT devices), https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2060-resolucao-783; Chambers and Partners, TMT 2026 - Brazil, § 4.2 (reporting that foreign SIM cards may not use Brazilian networks for more than 90 consecutive days), https://practiceguides.chambers.com/practice-guides/tmt-2026/brazil

[42] Brazil, Governo Digital, "Nuvem Brasileira" (project page; market consultation held 3 Sept. 2026), https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/ambiente-tecnologico/nuvem/nuvem-brasileira; Serpro, "Soberania sem isolamento: Nuvem Brasileira busca controle sobre dependências tecnológicas" (4 Sept. 2026), https://www.serpro.gov.br/menu/noticias/noticias-2026/soberania-sem-isolamento/

43Brazil, Ministry of Health, "Ministério da Saúde inicia jornada para a Nuvem Soberana do SUS" (11 Aug. 2026), https://www.gov.br/saude/pt-br/assuntos/noticias-ms/2026/agosto/ministerio-da-saude-inicia-jornada-para-a-nuvem-soberana-do-sus.

B. China

We outline below several concerns and recommendations regarding cross-border data policies and measures in China. Many GDA members face a challenging commercial environment in China, particularly in relation to cross-border data transfers, which are subject to outright prohibitions in some contexts and significant legal uncertainty in other contexts.[44]

Please see **here** for submissions on China's cross-border data restrictions and **here** for its ranking in the GDA Cross-Border Data Policy Index.[45]

Restrictions on Cross-Border Data Transfers
The Government of China has put in place numerous laws and regulations restricting the transfers of data across borders and forcing data to be stored locally including the CSL. For GDA members that provide cloud computing services or that rely heavily upon cloud computing for their business operations, these restrictions create an uneven playing field — advantaging domestic businesses that already have local infrastructure and preventing foreign businesses from operating efficiently or at all.

***Data Security Law*:** The Data Security Law (DSL), adopted on 10 June 2021, went into effect on September 1, 2021. The DSL (a) requires the State Internet Information Department to draft rules for all "other data handlers" (i.e., not just CII operators) to restrict those other handlers' exportation of "important data"; (b) applies to "[any person] handling important data"; (c) requires the State to create a "categorical and hierarchical system for data protection" as well as "catalog of" for "important data", and to assess the "importance" of data based on broad criteria relating to: economic development, social development, national security, the public interest, and the lawful rights and interests of citizens or organizations; (d) authorizes each region and department to set a "catalog of important data" within that region and in corresponding industries and sectors; and (e) requires the State to create a "monitoring and early warning system" for important data, which will apparently help it prevent the exportation of "important data."

Following the swift enactment of the DSL, the Cyberspace Administration of China and sectoral regulators such as the Ministry of Industry and Information Technology have developed guidelines to establish the requisite frameworks for data categorization and classification under the DSL. As China works on classifying the scope of "important data" and other data classifications under the auspices of the DSL, it will be important to ensure that those categories of classification are not overbroad and do not automatically and improperly sweep in data categories, such as intra-company data transfers (e.g., of internal business and operational data) that are otherwise protected.

***Personal Information Protection Law*:** The Personal Information Protection Law (PIPL)[46] took effect on November 1, 2021. Of particular concern are requirements for *ex ante* security assessments that impact data transfers that global companies have long engaged in for their daily business operations. The PIPL also raises the following concerns:

(1) data localisation requirements for "personal information" (PIPL Art. 40) and highly restrictive data transfer provisions for "personal information" (PIPL Arts. 38-40);
(2) lack of definition or overbroad scope for key concepts that implicate data localisation requirements and data transfer restrictions, including what constitutes a "justified need," or a "large volume [of data]" (PIPL Art 40);
(3) mandates for data assessments requiring governmental notification and/or approval in conjunction with the data localisation and data transfer provisions noted above (PIPL Art. 38(1), 40);

---

[44] AmCham China, *China Business Climate Survey Report*, at: http://www.amchamchina.org/policy-advocacy/business-climate-survey/; *See generally,* GDA Cloud Scorecard – 2018 China Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_China.pdf

[45] Global Data Alliance, Submissions in the People's Republic of China (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-china&sector=&language=&posts_filtered=1

[46] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

(4) proposed data transfer "standard contracts" that, while encouraging, may not be interoperable with standard contractual clauses under the EU General Data Protection Regulation (GDPR) or other established personal data protection frameworks (PIPL, Art. 38(3));
(5) the absence from the PIPL of other internationally recognised data transfer mechanisms, such as intra-corporate binding rules, trustmarks, and regional certifications (PIPL, Art. 38);
(6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established. (PIPL, Art. 39); and
(7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43).

The GDA and 31 other global associations raised these concerns in a letter submitted to China during the drafting process, but the concerns were not addressed.[47]

***Measures for Security Assessment of Cross-Border Data Transfers*:** On September 1, 2022, the Measures for Security Assessment of Cross-Border Data Transfers of the Cyberspace Administration of China (CAC) took effect. These security assessment measures are required only for a limited subset of companies engaging cross-border data transfers – specifically:

- A critical information infrastructure operator or a personal information processor based in China (akin to a "data controller" under the GDPR) that processes personal information for 1 million or more persons;
- A transferor of "important data";
- A processor of the personal data of more than 1 million individuals; a transferor of personal information of more than 100,000 individuals; or a transferor of sensitive personal information of more than 10,000 individuals. The latter criteria apply to the period beginning on January 1 of the preceding calendar year.

CAC also issued the Guidelines on Application of Security Assessment of Cross-border Data Transfers (First Version) on August 31, 2022.[48]

Regulations on Promoting and Standardizing Cross-Border Data Transfers: On March 22, 2024, the CAC issued its long-anticipated final Regulations on Promoting and Standardizing Cross-Border Data Transfers. The Regulations, which went into effect immediately, do not appear to materially alter China's restrictive cross-border data policy regulatory landscape, but they do loosen some restrictions (e.g., on intra-company transfers of human resources data.

Negative Lists of Data Whose Transfer is Prohibited or Restricted: Throughout 2024, several Free Trade Zones published catalogues of "important data" the transfer of which is explicitly be restricted. For example, on May 17, 2024, the Tianjin Free Trade Zone published its Data Outbound Management List – Negative List of data that cannot be transferred out of China without securing the approval of the local CAC authorities via a data security assessment, securing the approval of Chinese authorities pursuant to a standard contract, or securing a personal information protection certificate.

---

[47] Multi-association Letter on Draft Personal Information Protection Law and Draft Data Security Law, June 2, 2021, at: https://www.globaldataalliance.org/downloads/en06022021gdachinadslpip.pdf

[48] The Guidelines on Application of Security Assessment of Cross-border Data Transfers require a person making a security assessment application to prepare:

- a certified copy of its unified social credit code certificate;
- a certified copy of its legal representative's ID card;
- a Power of Attorney appointing an agent handling the application related matters – a template of this is included in the Guidelines;
- a certified copy of the appointed agent's ID card;
- a completed Application Form for Security Assessment of Cross-border Data Transfers – a template of this is included in the Guidelines;
- a certified copy of the agreements or other legal documents with the overseas data recipients. (In practice, it may be preferable to fulfill this requirement by submitting a copy of a China-approved standard contract (if and when they are published. However, the viability of this approach remains to be seen);
- a Report of Self-assessment of Risks in Cross-border Data Transfers – a template of this is included in the Guidelines (including an explanation, and risk/compliance/mitigation analyses for each transfer); and
- other supporting documents and materials

For example, the Tianjin Pilot Free Trade Zone's negative list covers 46 different data subclasses, including data subclasses that are typically publicly available in other countries, including: (1) international trade data; (2) international agricultural cooperation data; (3) agricultural market data; (4) place names and addresses; (5) meteorological data; (6) scientific data; (7) production data; (8) financial transaction data; (9) macro-economic statistics; (10) data about the Chinese language, history, customs or national values; and so forth.

Similarly, on August 30, 2024, authorities in Beijing the Data Export Management List (Negative List) of China (Beijing) Pilot Free Trade Zone ("Negative List") and the Administrative Measures for the Negative List ("Administrative Measures"). The Administrative Measures propose rules referencing 13 categories and 41 subcategories of data and for uniform identification of important data. The Negative List specify five industries – automotive, pharmaceutical, retail, civil aviation and artificial intelligence – which are a particular focus of Beijing's efforts to restrict data exports, outlining 23 business scenarios and 198 data elements subject to restrictions.

Draft Rules for Large Personal Information Handlers (2026): On 7 August 2026 the CAC released for consultation draft rules applying to designated handlers that process the personal information of more than 10 million people and that also meet additional scale and impact criteria. The draft would require personal information collected or generated in China to be stored domestically and the covered data centres to be located in China, while retaining the existing security-assessment, standard-contract and certification pathways for outbound transfers. Because the regime is not confined to internet platforms, it would reach large organisations across data-intensive sectors generally, including manufacturing, automotive, financial services and health. The practical effect would be to add a broad localisation baseline underneath transfer pathways that remain formally available. Comments were due 7 September 2026.

Guidance for the Secure Cross-Border Transfer of Automotive Data (2026 Edition): On 3 February 2026 the Ministry of Industry and Information Technology, the CAC and other agencies published guidance requiring automotive data controllers to compile their own "important data" catalogues and file them with the authorities, with China standard contractual clauses or CAC approval required before transfer. The covered categories are extensive and reach the core of vehicle engineering: bills of materials, R&D design documentation and development source code generated in the integration of global R&D resources; product simulation, track and real-world road testing data; production control program source code; algorithms, training data and feature data for driver assistance and autonomous driving; source code for OTA safety and battery-management upgrades; vehicle identification codes, telematics identifiers, keys, digital certificates and control commands; vehicle-road perception data including external imagery, radar, location trajectories, inertial navigation and autonomous driving maps; and V2X platform operation data. For EU-headquartered vehicle manufacturers and their suppliers, this is among the most consequential single measures in this Annex: it prevents a European parent from consolidating the engineering, testing and safety data generated by its Chinese operations, which is precisely the inbound-transfer problem described at Section 1.1.

Sector-Specific Controls on Non-Personal Data Exports: China has extended export controls beyond personal information to industrial and scientific data. In May 2026 Hainan Province completed what state media described as China's first export security assessment for the overseas transfer of remote-sensing satellite data, with officials characterising such data as a strategic asset linked to national security. Separately, the Ministry of State Security warned against the unauthorised collection and outbound transfer of meteorological data, citing risks from weather-monitoring devices that upload meteorological and geographic information to servers abroad. In December 2025 the Fujian Free Trade Zone issued a sector-specific negative list setting thresholds and approval routes for pharmaceuticals, connected vehicles, aviation maintenance and advanced manufacturing. The direction of travel is toward sectoral, national-security-framed control of non-personal and industrial data exports, which is the category least addressed by existing transfer mechanisms.

C. India

Overview/Business Environment

The commercial environment for GDA members remains challenging in India, in part due to an increase in restrictive cross-border data policies.[49] Several government authorities, including the Ministry of Electronics and Information Technology (**MeitY)**, the India Computer Emergency Response Team (**CERT-In**), the Reserve Bank of India (**RBI**), the Insurance Regulatory Development Authority of India (**IRDAI**), the Securities and Exchange Board of India (**SEBI**), the Department for Promotion of Industry and Internal Trade (**DPIIT**), the Ministry of Health and Family Welfare (**MoHFW**), and the Department of Telecommunications (**DoT**) have advanced policies and proposals impacting cross-border data transfers.

The increase in data localisation requirements threatens the commercial and strategic interests of European companies while imposing a drag on India's own ambitions for growth and innovation. These requirements are included in various policies ranging from legacy regulations on government-owned weather data,[50] regulations on machine-to-machine (M2M) systems,[51] and payment processing regulations[52], to proposed rules for the Digital Personal Data Protection Act.[53]

Please see **here** for submissions on India's numerous cross-border data restrictions and digital sovereignty measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[54]

Digital Personal Data Protection Act and Rules: In August 2023, Parliament enacted India's Digital Personal Data Protection (DPDP) Act. Compared with the data transfer restrictions and localisation requirements in earlier versions, the provisions in the final Act are significantly improved. The final Digital Personal Data Protection Rules, 2025, notified on 13 November 2025 and published in the Gazette of India on 14 November 2025,[55] retain authorities to require data localisation and to restrict international data transfers. Rule 12(4) empowers the government to require data localisation for "significant data fiduciaries" and Rule 15 provides that a data fiduciary may transfer personal data outside India except where the Central Government restricts such transfer — a negative-list model that leaves the scope of future restrictions entirely open. Section 16 and the associated operational obligations commence eighteen months from 13 November 2025.

The National Data Sharing and Accessibility Policy 2012 (NDSAP 2012)*:* The Ministry of Science and Technology policy makes it challenging for software companies to leverage global computing facilities when it comes to government-owned data, such as weather data.[56]

Directive on Storage of Payment System Data: In April 2018, the RBI issued the Directive 2017-18/153 under the Payment and Settlement Systems Act 2007 (Directive),[57] requiring payments firms to store data solely in India and ensure that any data processed abroad be deleted within 24 hours. The Directive imposes data and infrastructure

[49] *See generally*, GDA Cloud Scorecard – 2018 India Country Report, https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

[50] *See Guidelines for Government Departments On Contractual Terms Related to Cloud Services,* (Section 2.1.d), http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms_0.pdf

[51] *National Telecom M2M Roadmap (2015),* at: http://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

[52] *Reserve Bank of India Storage of Payment System Data Directive (2018),* https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0

[53] Ministry Of Electronics And Information Technology Notification Draft Rules, Digital Personal Data Protection Act, mygov-999999999568142946.pdf

[54] Global Data Alliance, Submissions in India (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-india&sector=&language=&posts_filtered=1

[55] Ministry Of Electronics And Information Technology Notification Draft Rules, Digital Personal Data Protection Act, at https://static.mygov.in/innovateindia/2025/01/03/mygov-999999999568142946.pdf

[56] National Data Sharing and Accessibility Policy-2012 (NDSAP-2012), at https://dst.gov.in/sites/default/files/gazetteNotificationNDSAP.pdf

[57] Storage of Payment System Data Directive

localisation requirements that require payment system operators to "ensure that the entire data relating to payment systems operated by them (system providers) are stored in a system only in India."[58] "Data relating to payment systems" as specified in the Directive is an overbroad definition that applies to a wide range of data and the Directive affects both payment processors and their service providers.[59] The RBI directive imposed short deadlines and has required significant capital investments for companies to comply, and has resulted in a range of severe enforcement measures taken against certain financial service providers in 2021.

CERT-In Directions under IT Act: In April 2022, the Indian Computer Emergency Response Team (CERT-In) issued a notification titled "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000..." which requires logs of all IT systems to be stored in India.[60] While MeitY issued subsequent "Frequently Asked Questions (FAQs) on the Directions", it still did not address concerns around localised log storage.[61]

SEBI Cyber Security and Cyber Resilience Framework: In August 2024, SEBI issued its final Cybersecurity and Cyber Resilience Framework (CSCRF) which requires regulated entities (REs) to have their "Regulatory Data" to be stored and processed in India. SEBI strongly believes that "data localisation ensures data sovereignty and data residency together" and "lead to better governance and oversight." SEBI also shared concerns over the sharing of "Regulatory Data" with regulators outside of India which may negatively hamper the industry's need to fulfil reporting obligations. While the CSCRF came into effect on 1 January 2025, SEBI issued clarifications (December 2024) that the requirements around data localisation is put on hold until further notification. SEBI directed the industry to set up local working groups to formalize the approach to data localisation and the implementation timeline.

SEBI Cloud Framework: In March 2023, SEBI published its Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs). The Framework is effective immediately for new cloud deployments and REs are required to store and process their data in India, and this sweeping requirement is imposed across all types of REs' data. Moreover, REs must use a CSP that is empaneled (certified) by the Ministry of Electronics and Information Technology (MEITY). For PaaS and SaaS cloud services, REs may only work with providers that use underlying infrastructure from MEITY-empaneled CSPs. This requirement prevents firms from benefiting from cloud technology due to the costs and operational challenges that will be incurred, as well as the risks involved with a decentralized environment. This exposes FIs to greater cybersecurity risks by creating a more decentralized environment that needs to be safeguarded, which further inhibits central oversight and information sharing across borders. In addition, local processing will negatively impact FIs' global operation, their ability to undertake activities at a global level and cross-border service offering.

SEBI SaaS Circular: In November 2020, SEBI issued a SaaS Circular (Annexure A) which requires "critical data" – from credit risk data to liquidity risk data, audit data, system vulnerability information, and other types of data – that are stored on SaaS solutions, to be stored within India's legal boundaries. The SEBI Circular is based upon a CERT-IN advisory that highlighted the cybersecurity risk of FIs moving "critical data" cross border. SEBI and CERT-IN hold the view that there is heightened risk that critical data could fall into the hands of a malicious actor because of the cross-border use of SaaS applications.

RBI - Master Direction on KYC and Video based Customer Identification Process (V-CIP): In May 2021, RBI amended its Master Direction (MD) on KYC dated February 25, 2016 and added, amongst other requirements, a localisation requirement – "the entire data and recordings of V-CIP shall be stored in a system / systems located in India."

The IRDAI (Maintenance of Insurance Records) Regulation, 2015: Paragraph 3(9) of this measure requires organizations within the scope of the regulation in India to store insurance data within India.[62] Likewise, IRDAI's Reinsurance Regulations impose stringent data localisation requirements on foreign reinsurer branches. Customer data and business data must be stored on servers in India and obtain express consent from the data subject to

[58] Storage of Payment System Data Directive

[59] Storage of Payment System Data Directive

[60] No. 20(3)/2022-CERT-In, MeitY, at https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[61] BSA concerns on the CERT-In Directions on Information Security Practices at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

[62] IRDAI (Maintenance of Insurance Records) Regulations, 2015, https://irdai.gov.in/document-detail?documentId=604674

transfer data outside India. These regulations are redundant, applying on top of the Digital Personal Data Protection Act, and should be eliminated.

MeitY's "MeghRaj" initiative: This initiative seeks to promote the use of cloud services by the government, but also contains unnecessary requirements for the localisation of government data.[63] CSPs participating in the initiative must have "data center facility within India".[64]

***Geospatial and Weather Data Restrictions*:** The National Data Sharing and Accessibility Policy (NDSAP) notified by the Ministry of Science and Technology furthers data localisation making it challenging for software companies to leverage global computing facilities, especially when it comes to government-owned weather data.[65] Furthermore, guidelines relating to geospatial data and associated services introduced in 2021 were ostensibly aimed at opening up India's mapping policy and improving the ease of doing business through deregulation, however they also contain elements that are discriminatory to foreign service providers. These guidelines on geospatial data and services limit cross-border data transfers and are obstructing foreign firms, including EU companies, from forming partnerships and pursuing technology development in India.

National E-Commerce Policy: In February 2019, DPIIT released a Draft National E-Commerce Policy, which contains several proposals that restrict Indian customers' access to the most seamless and secure digital services. The draft policy included data localisation requirements and restrictions on data flows. The draft policy was later withdrawn given significant concerns from the industry, but it will be important to continue to monitor whether a replacement measure with similar challenges reappears.

Non-Personal Data Governance: On September 2019, MeitY constituted a Committee of Experts to develop a governance framework for non-personal data (NPD Framework). In August 2020, the Committee released its report.[66] In December, the Committee published the revised report.[67] In our written comments, GDA highlighted numerous concerns including mandatory sharing of proprietary non-personal data, restrictions on cross-border data transfers and local storage requirements.[68] This proposal no longer appears to be under active consideration, but it will be important to ensure that no similar measure reappears.

Restrictions on IoT permanent roaming and mandating local SIMs: India's telecom regulator (TRAI) has recommended that all M2M devices using eSIMs be switched to local operators within six months. Although this remains at the proposal stage, it raises concerns because it could make global IoT deployments in India more complex and expensive, discouraging investment and innovation. Mandating local SIM migration could disrupt existing services and limit international roaming, which is essential for seamless global connectivity and data flows. Unlike other regions such as the EU, Australia and Singapore, which allow flexibility in eSIM implementation, India's approach risks isolating its market and increasing costs for both providers and consumers.

Sovereign Cloud Framework (under development): MeitY is developing a Sovereign Cloud framework for what it describes as high-risk government workloads. Requirements reported to be under consideration include operational control requirements and stringent data localisation. No draft has been published for public consultation; engagement to date has been conducted through one-on-one discussions with selected industry participants. This is a further instance of the transparency problem described at Section 1.4: a measure with potentially significant market-access consequences is being developed without a published text against which affected parties can comment.

---

[63] Adoption of Meghraj by User Departments, https://ambud.meity.gov.in/#GUIDELINES

[64] Process for Empanelment of Cloud Service offerings of Cloud Service Providers (CSPs), https://ambud.meity.gov.in/assets/web_assets/Includes/files/Stepwise%20guide%20on%20empanelment%20process.pdf

[65] National Data Sharing and Accessibility Policy-2012 (NDSAP-2012), gazetteNotificationNDSAP.pdf

[66] Report by the Committee of Experts on Non-Personal Data Governance Framework, August 2020, https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

[67] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dec 2020, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

[68] GDA Submission on Revised Non-Personal Data Governance Framework, January 2021, https://www.bsa.org/policy-filings/india-bsa-submission-on-revised-non-personal-data-governance-framework

D. Indonesia

The commercial environment in Indonesia is challenging for GDA member companies, as Indonesia maintains a number of policies that can make it more difficult to access the Indonesian market with digitally-enabled products and services. Please see here for submissions on Indonesia's cross-border data restrictions and digital sovereignty measures and here for its ranking in the GDA Cross-Border Data Policy Index.[69]

Customs Treatment of Digital Products: Indonesia continues to classify software and other digital products transmitted electronically as imported intangible goods under tariff heading 99.01. The current import-duty rate for the relevant tariff lines is 0 percent, but importers remain required to submit an import declaration (PIB) for intangible imports no later than 30 days after payment. Indonesia and the United States signed an Agreement on Reciprocal Trade on February 19, 2026 under which Indonesia committed to eliminate the existing tariff lines on "intangible products" and suspend the related import-declaration requirements. As of September 2026, however, that agreement is pending entry into force, and the existing Indonesian customs framework remains applicable. Accordingly, the present barrier is the customs classification and import-declaration requirement rather than a positive customs duty.[70]

GR71: Government Regulation 71/2019 and its implementing rules impose registration, government-access, and content-control obligations on electronic system operators. Ministerial Regulation No. 5 of 2020 on Private-Scope Electronic System Operators, as amended by Ministerial Regulation No. 10 of 2021, requires covered domestic and foreign private-scope electronic system operators to register. It also requires private-scope operators to provide access to electronic systems and/or electronic data for government supervision and law-enforcement purposes. Failure to register can result in access blocking, and failure to comply with applicable takedown obligations can also result in blocking. Komdigi has continued active enforcement of the registration requirement in 2026, including against foreign operators. The earlier reference to a possible GR71 amendment imposing new data localisation requirements has been omitted because no such draft has been published and the proposal cannot presently be characterized with sufficient reliability.[71]

Personal Data Protection and Cross-Border Transfers: Indonesia issued Government Regulation No. 33 of 2026 implementing the Personal Data Protection Law on July 16, 2026. The Regulation is scheduled to take effect six months after promulgation, on January 16, 2027. For transfers of personal data outside Indonesia, the Regulation requires controllers to assess the need for and risks of the transfer and provide specified information to data subjects before transfer. It establishes a hierarchy under which the recipient jurisdiction should provide an equivalent or higher level of protection; if that condition is not met, the controller must ensure adequate and binding safeguards; and only if neither condition is met may the controller rely on data-subject consent. Consent-based transfers are further limited, including to transfers that are non-recurring and involve a limited number of data subjects. The Regulation does not impose a general data localisation mandate, but it will add substantive transfer-assessment, notification, and documentation requirements when it enters into force.[72]

Data Localisation in the Financial Sector: Bank Indonesia Regulation No. 10 of 2025, which took effect on March 31, 2026, requires payment-system service providers to comply with domestic processing of payment transactions.

---

69 Global Data Alliance, Submissions in Indonesia (2020-2026), https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-indonesia&sector=&language=&posts_filtered=1; Global Data Alliance, Cross-Border Data Policy Index (2023), https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf.

70 Indonesia Ministry of Finance, Regulation No. 26/PMK.010/2022, Chapter 99 (software and other digital products transmitted electronically; import duty 0%), https://www.jdih.kemenkeu.go.id/api/download/04d90736-33d5-4b72-92a3-0d2b7c6bb8bd/26~PMK.010~2022Per.pdf; Directorate General of Customs and Excise, PER-2/BC/2023, art. 48 (PIB for intangible imports within 30 days of payment; heading 9901), https://jdih.kemenkeu.go.id/dok/per-2-bc-2023; USTR, 2026 Trade Policy Agenda and 2025 Annual Report, pp. 66-67 (U.S.-Indonesia ART signed Feb. 19, 2026 and pending entry into force; commitment to eliminate tariff lines on intangible products and suspend related import-declaration requirements), https://ustr.gov/sites/default/files/files/Press/Releases/2026/2026%20Trade%20Policy%20Agenda%202025%20Annual%20Report.pdf.

71 Indonesia, Government Regulation No. 71 of 2019 on Electronic Systems and Transactions; Ministry of Communication and Informatics Regulation No. 5 of 2020 on Private-Scope Electronic System Operators, especially arts. 7 and 21-22, https://jdih.komdigi.go.id/produk_hukum/view/id/759/t/peraturan%2Bmenteri%2Bkomunikasi%2Bdan%2Binformatika%2Bnomor%2B5%2Btahun%2B2020; Regulation No. 10 of 2021 amending Regulation No. 5 of 2020, https://jdih.komdigi.go.id/produk_hukum/view/id/774/t/peraturan%2Bmenteri%2Bkomunikasi%2Bdan%2Binformatika%2Bnomor%2B10%2Btahun%2B2021. See also Komdigi, "Perketat Pengawasan, Komdigi Minta 25 PSE Lingkup Privat Penuhi Kewajiban Pendaftaran" (17 Sept. 2026), https://portal.komdigi.go.id/kanal-publik/berita-kini/10548.

72 Indonesia, Government Regulation No. 33 of 2026 on Implementation of Law No. 27 of 2022 on Personal Data Protection, State Gazette 2026 No. 88, arts. 160-174 (promulgated 16 July 2026; effective six months after promulgation). Full-text navigator reproducing the official text: https://pppdp2026.karsa-siber.com/. See especially arts. 163-165, 168-173.

Payment transactions may be processed outside Indonesia only with Bank Indonesia approval, taking into account factors including integration with an overseas headquarters and the readiness of domestic industry and infrastructure. The current rule therefore continues to constrain the use of fully offshore processing architectures for Indonesian payment transactions, although it provides an approval pathway rather than a categorical prohibition.[73]

Local Content and Government Procurement Requirements: Indonesia continues to maintain domestic-content requirements and preferences that affect technology procurement. Ministry of Industry Regulation No. 22 of 2020 remains in force as the sector-specific framework for calculating domestic content (TKDN) for electronics and telematics, while Ministry of Industry Regulation No. 35 of 2025 establishes the current broader TKDN and Company Benefit Weight (BMP) certification framework. Presidential Regulation No. 46 of 2025 amended Indonesia's government-procurement rules in part to increase the use of domestic products. Presidential Instruction No. 2 of 2022 remains in force and directs public bodies, among other things, to allocate at least 40 percent of goods and services procurement spending to domestically produced products of micro and small enterprises and cooperatives and to apply TKDN-based domestic-product preferences. The prior statement that Indonesia had announced a specific extension of local-content requirements to software and cloud services has been omitted because a current, final rule establishing that proposition could not be verified.[74]

Cloud Services: For commercial banks, the current OJK framework is approval-based rather than an outright prohibition on public cloud or offshore cloud use. OJK Regulation No. 11/POJK.03/2022 remains the underlying framework for bank information-technology operations, and OJK Commissioner Board Member Regulation No. 1 of 2026, effective March 1, 2026, now sets the current procedures for permissions relating to placement of electronic systems and processing of IT-based transactions outside Indonesia. The framework therefore permits offshore arrangements, but subjects covered banking systems and transaction processing outside Indonesia to prior OJK authorization and specified application requirements. This remains a material regulatory constraint on the use of regional or global cloud architectures by banks operating in Indonesia.[75]

73 Bank Indonesia, Regulation No. 10 of 2025 on Payment System Industry Regulation, effective 31 March 2026. The regulation requires payment-system service providers to comply with domestic processing of payment transactions and permits processing outside Indonesia only with Bank Indonesia approval subject to specified considerations. https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI_102025.aspx.

74 Indonesia Ministry of Industry, Regulation No. 22 of 2020 on Calculation of Domestic Component Level (TKDN) for Electronics and Telematics (status: in force), https://peraturan.bpk.go.id/Details/166989/permenperin-no-22-tahun-2020; Ministry of Industry Regulation No. 35 of 2025 on TKDN and Company Benefit Weight (BMP) Certification (effective 11 Dec. 2025), https://peraturan.bpk.go.id/Details/333003/permenperin-no-35-tahun-2025; Presidential Regulation No. 46 of 2025 amending the government-procurement framework, https://peraturan.bpk.go.id/Details/318647/perpres-no-46-tahun-2025; Presidential Instruction No. 2 of 2022, including the instruction to allocate at least 40% of goods/services procurement spending to domestically produced products of micro and small enterprises and cooperatives and to apply TKDN-based domestic-product preferences, https://peraturan.bpk.go.id/Details/204320/inpres-no-2-tahun-2022.

75 OJK Regulation No. 11/POJK.03/2022 on Information Technology Operations by Commercial Banks, https://ojk.go.id/id/regulasi/Documents/Pages/Penyelenggaraan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%2011%20-%2003%20-%202022.pdf; OJK Commissioner Board Member Regulation No. 1 of 2026 on Information Technology Operations by Commercial Banks, effective 1 March 2026, including procedures for permissions concerning placement of electronic systems and processing of IT-based transactions outside Indonesia, https://ojk.go.id/id/regulasi/Pages/PADK-1-Tahun-2026-Penyelenggaraan-Teknologi-Informasi-oleh-Bank-Umum.aspx.

E. Republic of Korea

The overall commercial environment in the Republic of Korea (Korea) for GDA members is mixed on the subject of cross-border data transfers and data localisation.[76] Korea has a strong IT market and a mature legal system. On the other hand, digital protectionism – reflected in data residency mandates, physical network separation requirements, and other restrictive data-related requirements for industry sectors, such as government/public services, finance, healthcare, and education – severely hampers digital trade and the cross-border exchange of knowledge, information and data with Korea.

Please see **here** for submissions on South Korea's numerous cross-border data restrictions and digital sovereignty measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[77]

Cross-Border Data Transfers and Server Localisation: The Cloud Security Assurance Program ("CSAP") was created by the Korea Internet and Security Agency in 2016 and elevated from administrative guidance to a legal requirement through a March 2022 revision to the Cloud Computing Promotion Act. The CSAP, which applies to Korea's central, provincial, and local public sector with very limited exceptions, presents significant barriers to EU service providers seeking to enter Korea's public sector. EU service providers are required to fulfill technical and administrative requirements, many of which are not in line with global standards and business practices, and which do not lead to improved cloud security:

A) Physical Network Separation. Most public sector data systems are required to be hosted on infrastructure and networks that are physically separated from those used by other clients. This requirement diverges from international best practices, which recognise logical separation as a secure and effective method for isolating sensitive workloads in multi-tenant cloud environments. While a few countries retain physical network separation requirements for some highly sensitive areas (national security, defense), it is rarely applied throughout the public sector, including to institutions that handle non-sensitive or even public data, such as public universities.

B) Encryption. service providers are required to use Korean-developed encryption algorithms (e.g., ARIA, SEED). This is impractical for many leading service providers that already use state-of-the-art encryption algorithms that meet internationally recognised standards and are accepted for applications in the most sensitive circumstances in other markets. After substantial advocacy efforts, Korea's National Intelligence Service (NIS) indicated in September 2024 that it will relax encryption requirements up to the Medium tier. There remains significant ambiguity regarding how this will be implemented in practice. To date, no formal updates or amendments have been made to the CSAP to reflect this change, leaving foreign service providers in a state of legal and operational uncertainty.

C) Data Localisation. All data associated with public sector data systems must be physically located in Korea. This is an unnecessary barrier for many foreign service providers that store and process data in regional data centers outside of Korea. In some cases, the use of offshore data centers ensures redundancy and back-up. In cases of serious physical damage or cyberattack on one data center, data stored in physically remote data centers can be used to recover from the incident.

D) Local Personnel Requirements. Service providers must have operations and management personnel located within Korea to obtain CSAP certification. Local personnel requirements disadvantage foreign service providers, significantly raising their compliance costs, as they must duplicate personnel and infrastructure already managed efficiently at scale elsewhere.

These requirements do little to enhance security while undermining the main benefit of cloud computing services, which is the economy of scale and state-of-the-art security capabilities of a globally deployed cloud service. The CSAP continues to place foreign service providers at a competitive disadvantage to domestic competitors.

---

[76] *See generally*, GDA Cloud Scorecard – 2018 Korea Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Korea.pdf

[77] Global Data Alliance, Submissions in the Republic of Korea (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=korea&sector=&language=&posts_filtered=1

In 2023, Korea introduced a three-tiered scheme dividing all public sector data systems into three tiers: Low, Medium, and High. However, these reforms are insufficient and still present significant challenges for foreign service providers seeking to enter the public sector market in Korea:

- Most public-sector data systems continue to be classified as either Medium or High tier systems, for which foreign service providers are unable to get certified. The Low tier only covers data systems which are open, public, and do not contain any personal information, which is a very narrow subset of public sector data systems. Specifically, if a public institution's data system contains personal information, which is broadly defined in Korea's Personal Information Protection Act (**PIPA**), it would be classified as either Medium or High tier. As such, even if an EU CSP is CSAP-certified for Low tier data systems, it is still excluded from the majority of public sector opportunities in Korea, as it cannot serve institutions that handle even minimal amounts of personal information. Further, only service providers that are CSAP-certified for the Medium or High tiers are cleared to participate in the Korean Government's digital transformation initiatives.

- Even for the Low tier, most of the requirements highlighted above continue to apply. The requirement to use physical network separation no longer applies to Low tier systems, allowing service providers to use logical network separation to keep the public sector data systems distinct from those of their other customers. However, all three levels of CSAP classification, including Low tier, continue to require service providers to use only Korea-developed encryption algorithms, physically locate data in Korea, and maintain local personnel presence.

- To date, only three foreign service providers are CSAP-certified, and only for the Low tier. This outcome highlights the general ineffectiveness of Korea's limited reforms. Despite repeated claims of progress, the CSAP framework remains structurally protectionist and functionally inaccessible to foreign service providers.

On 20 April 2026 the Ministry of Science and ICT and the National Intelligence Service announced a plan to consolidate the MSIT-administered CSAP and the separate NIS security verification process into a single NIS-led public cloud security verification framework. Existing CSAP certifications are expected to remain valid for their current terms. Revisions to the National Cloud Computing Security Guidelines were expected in the first half of 2026, followed by a one-year grace period and full implementation in the second half of 2027. The technical criteria, the relationship between the new NIS-led framework and Korea's National Network Security Framework, and the extent to which the system will afford transparent, predictable and non-discriminatory treatment to foreign providers all remain unresolved. Korean authorities have also been reported to be considering extending CSAP from public-sector procurement into a private-sector certification mechanism described as "voluntary." If that occurred, the residency, encryption and local-personnel criteria described above would reach well beyond the public sector. The EU should seek commitments on the design of the consolidated framework now, while the criteria are still being written, rather than after implementation in 2027.

The continued lack of meaningful market access for EU service providers underscores the need for sustained and elevated European Commission advocacy. Korea's piecemeal and limited adjustments have failed to address the fundamental structural barriers that prevent EU service providers from competing on fair and equal terms in the public sector market. The CSAP remains a significant non-tariff barrier for EU service providers. In its negotiations with Korea, the EU should extract explicit and enforceable commitments from Korea to align the CSAP with global norms and enable market access for trusted foreign service providers. These commitments should include the following: (1) Classifying a larger share of public institution data systems as Low tier and remove references to personal information in the CSAP; and (2) Aligning certification requirements for Low and Medium tier data systems with international best practices by eliminating requirements for physical network separation, data residency, use of Korea-developed encryption algorithms, and local personnel presence. CSAP should also accept internationally recognised standards and certifications from internationally accredited bodies.

Personal Information Protection Regime: South Korea's personal information protection regime is one of the most stringent in the region and has significantly decreased the ability for GDA members to serve the South Korean market. Although the National Assembly has continued to amend the Personal Information Protection Act (PIPA) and the European Commission and South Korea have mutually recognised each other's personal data protection frameworks as "adequate" and equivalent, more work is required to reform South Korea's personal data protection regime. The PIPA should make a clearer distinction between data controllers and data processors to better delineate the roles and responsibilities of different entities. South Korea should also adopt measures that expand

the legal basis for processing personal information beyond consent. This would better support Korea's goal of promoting the development, adoption, and deployment of AI while ensuring that personal information is appropriately and adequately protected.

Cross-Border Data Restrictions in the Financial Services Sector: South Korea's Financial Services Commission (FSC) dictates that personal credit information cannot be processed overseas and, if processed in public cloud, the cloud computing systems must be maintained on servers located in South Korea.[78] Moreover, South Korea's network segregation rules, which require internal and external networks to be physically segregated,[79] effectively require the localisation of network infrastructure and data sets. These policies expose financial institutions to greater cybersecurity risks by creating a more diffuse and decentralized cybersecurity environment with a greater cyber-attack surface and potential points of failure. South Korea's localisation mandates also effectively inhibit central oversight and information sharing across borders, reducing cyber threat awareness and visibility.

Besides data localisation, the network segregation requirements prevent the Korea subsidiaries from leveraging on the global IT and cybersecurity service and expertise, and negatively impact financial institutions' adoption of cutting edge cybersecurity services delivered through SaaS and AI-enhanced tools. A recent interpretation provided by Financial Supervisory Service (FSS is the FSC's supervisory arm) deems global support as violation of network segregation rule, which poses non-compliance risk to all global FIs and cybersecurity risk.[80]

Cross-Border Data Restrictions in the Insurance Sector: Foreign reinsurance companies continue to face significant restrictions on transferring personal information outside of Korea in the ordinary course of business. These restrictions persist despite statements by Korea's FSC in 2022 and 2024 indicating a revised interpretation of the Personal Information Protection Act that would permit the cross-border transfer of primary insurance policyholder data for purposes such as data processing, risk management, and underwriting. In September 2024, Korean government officials verbally provided clarification related to the use of a revised consent form and possible changes to Korean law, no public written documentation has been issued to confirm these changes. In the absence of legal certainty, foreign reinsurers remain unable to transfer data outside of Korea.

Location Data: South Korea's restrictions on the transfer of location-based data have led to a competitive disadvantage for international suppliers seeking to incorporate such data into services offered from outside of South Korea. Among major markets, South Korea maintains a uniquely restrictive licensing framework for such data transfers. To date, Korea has never approved a license to transfer cartographic or other location-based data, despite numerous applications by foreign enterprises.

[78] Article 17 under the Credit Information Use and Protection Act. Under RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.

[79] RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.

[80] FSC. No Action Letter: Whether it violates Article 15, Paragraph 1, Item 5 of the Electronic Financial Supervision Regulations when an overseas trustee directly accesses the server in the domestic computer room to perform entrusted tasks (system operation), https://better.fsc.go.kr/fsc_new/replyCase/OpinionDetail.do?stNo=11&muNo=86&muGpNo=75&opinionIdx=2261

F. Saudi Arabia

Saudi Arabia has pursued assertive data localisation as part of its "Vision 2030" and digital sovereignty policies. The government views local data retention as enhancing national security and support for local tech sectors. Accordingly, Saudi Arabia maintains localisation requirements particularly for Saudi government data and certain regulated financial-sector workloads, and since 1 January 2024 generally restricts government agencies from contracting with certain foreign companies that have a regional headquarters elsewhere in the Middle East and North Africa but not in Saudi Arabia, subject to specified exceptions.[81]

Please see here for submissions on Saudi Arabia's cross-border data restrictions and here for its ranking in the GDA Cross-Border Data Policy Index.[82]

Cloud and Cybersecurity Localisation Requirements: The National Cybersecurity Authority's current Essential Cybersecurity Controls (ECC-2:2024) and Cloud Cybersecurity Controls (CCC-2:2024) supersede the 2018 and 2020 versions previously cited in this section. The NCA expressly deleted the former ECC control requiring in-Kingdom hosting and storage and the former CCC subcontrols requiring cloud storage, processing, disaster recovery, monitoring, and support to be provided from within the Kingdom; the NCA states that data-localisation controls were transferred to the National Data Management Office (NDMO) at SDAIA. Separately, the Communications, Space and Technology Commission's Cloud Computing Services Provisioning Regulations (Version 4), effective 10 October 2023, remain a concrete localisation measure for Saudi government data. The regulations provide that[83] registered cloud service providers and cloud subscribers must not transfer Saudi government-agency data outside the Kingdom, permanently or temporarily, unless such transfer is expressly permitted under other Saudi laws or regulations, and require Saudi government-agency data placed in public, community, or hybrid cloud environments to be handled by a cloud service provider properly registered with CST.[84]

Personal Data Protection Law (2023): Saudi Arabia's PDPL (first enacted in 2021 and amended in 2023) regulates transfers of personal data outside the Kingdom, but it does not impose a general requirement that most personal data be stored in-country or a general requirement to obtain a transfer permit from SDAIA. Article 29 of the PDPL permits transfers for specified purposes subject to conditions including that the transfer not prejudice national security or the Kingdom's vital interests and that an adequate level of protection be available. Where an adequate level of protection is not available, the Regulation on Personal Data Transfer Outside the Kingdom permits specified appropriate safeguards, including standard contractual clauses, binding common rules, and accreditation certificates. A transfer-risk assessment is required in specified circumstances, including transfers relying on those safeguards and continuous or large-scale transfers of sensitive data.[85]

Financial Sector Localisation: Saudi financial-sector rules continue to impose localisation and approval requirements. SAMA's Cyber Security Framework provides that, in principle, only cloud services located in Saudi Arabia should be used, and that a SAMA-regulated member organization must obtain explicit SAMA approval before

---

[81] See Saudi Press Agency, "Saudi Arabia Will Stop Contracting with Any Company or Firm That Has Regional Headquarters Outside Saudi Arabia, Starting From 2024" (15 Feb. 2021), https://www.spa.gov.sa/en/b1924d1ebb; and Umm Al-Qura, Controls for Government Agencies Contracting with Companies that Do Not Have a Regional Headquarters in the Kingdom and Related Parties, https://www.uqn.gov.sa/details?p=21199.

[82] Global Data Alliance, Submissions to the Kingdom of Saudi Arabia (2020–2025), https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-saudiarabia&sector=&language=&posts_filtered=1; Global Data Alliance, Cross-Border Data Policy Index (2023), https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf.

[83] Communications, Space and Technology Commission, Approval on the Update of the Cloud Computing Service Provisioning Regulations and its Guides, Decision No. 506/1445 (8 Oct. 2023; effective 10 Oct. 2023), https://www.cst.gov.sa/en/regulations-and-licenses/decisions/Regulation-1482; Cloud Computing Services Provisioning Regulations (Version 4), paras. 3-3-5 to 3-3-7.

[84] National Cybersecurity Authority, Essential Cybersecurity Controls (ECC-2:2024), Appendix C (deleting former control 4-2-3-3 and transferring data-localisation controls to NDMO/SDAIA), https://cdn.nca.gov.sa/api/files/public/upload/86e09090-44e4-481f-bc28-355673607654_ECC--2024-EN.pdf; National Cybersecurity Authority, Cloud Cybersecurity Controls (CCC-2:2024), Annex D (deleting former subcontrols 2-3-P-1-10 and 2-3-P-1-11 and transferring data-localisation controls to NDMO/SDAIA), https://cdn.nca.gov.sa/api/files/public/upload/6d5408a3-d8e6-4e96-963b-2c7198e5b7c2_CCC-2-2024-EN-.pdf.

[85] Saudi Data & AI Authority, Personal Data Protection Law, art. 29, https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL/; SDAIA, Regulation on Personal Data Transfer Outside the Kingdom, arts. 2, 4 and 7, https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL2/; see also SDAIA, Standard Contractual Clauses for Personal Data Transfers and Guidelines for Binding Common Rules, available at https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx.

using cloud services outside Saudi Arabia. SAMA's payment-card rules also require contracting-entity personal data, including data collected from payment-device transactional activity, to be stored in secure facilities within the Kingdom. Separately, Saudi Arabia's regional headquarters rules, effective from 1 January 2024,[86] generally restrict government agencies from contracting with covered foreign companies that lack a regional headquarters in the Kingdom, subject to monetary thresholds, specified exceptions, and an exception process.[87]

Internet of Things: Saudi Arabia's current IoT Regulations, issued by CST in July 2024, require all physical SIM cards and eSIMs used in IoT devices intended for use in the Kingdom to be issued by a provider holding the relevant CST service license. The current regulations do not use the term "permanent roaming," but the SIM/eSIM requirement means that a foreign SIM not issued by a CST-licensed provider cannot be relied upon for an IoT deployment in Saudi Arabia, including connected devices such as vehicles.[88]

[86] Umm Al-Qura, Controls for Government Agencies Contracting with Companies that Do Not Have a Regional Headquarters in the Kingdom and Related Parties, arts. 3-8 and 21, https://www.uqn.gov.sa/details?p=21199 (effective 1 Jan. 2024).
[87] Saudi Central Bank, Cyber Security Framework, § 3.4.3 (Cloud Computing), https://rulebook.sama.gov.sa/en/343-cloud-computing-0 (providing that, in principle, cloud services should be located in Saudi Arabia and explicit SAMA approval is required for cloud services outside Saudi Arabia); Saudi Central Bank, Payment Card Issuing and Acquiring Guidelines, § 2.6.2, https://rulebook.sama.gov.sa/en/26-data-protection.
[88] Communications, Space and Technology Commission, Internet of Things (IoT) Regulations, Decision No. 556/1446 (31 July 2024), para. 5-4, https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1602.

G. Türkiye

Türkiye has ramped up data localisation through both new laws and strict enforcement of existing regulations. Please see here for Türkiye's ranking in the GDA Cross-Border Data Policy Index.

While Türkiye's general data protection law is similar in some respects to the EU, the government has gone much further in the data restrictions that it imposes, mandating that banking and many other types of data stay within Türkiye's borders and failing to declare any partner economies "adequate" for data transfers. We provide below a summary of Türkiye's many barriers that impact EU-based enterprises. Given the relatively larger scale of European investment in Türkiye, EU investors and commercial entities are disproportionately burdened by these Turkish digital trade restrictions – as compared with their counterparts based in APAC or the Americas.

Presidential Circular No. 2019/12 and the Information and Communication Security Guide: Under this Circular, many categories of information and data – including population, health, and communication records, as well as genetic and biometric data – must be securely stored within Türkiye. The Circular also prohibits public institutions and organisations from storing their data on cloud services, except where those services are operated on the institution's own private infrastructure or by local service providers under its control. Consequently, private-sector vendors that process or store data on behalf of public entities are effectively required to host such data on servers located in Türkiye. [89] This approach is mirrored in the Information and Communication Security Guide.[90]

Banking & Cloud Localisation Regulations: Turkish banking regulators require financial institutions to keep data on Turkish soil. The Banking Regulation and Supervision Agency (BDDK) mandates that banks' primary and secondary IT systems (including backup servers) be hosted in Türkiye. Likewise, the Central Bank of Türkiye restricts outsourcing of certain operations to foreign cloud services and outright prohibits use of public cloud for critical workloads, pushing banks toward local IT solutions. This not only impacts foreign firms' market access, but also means higher costs and less flexibility for Türkiye's financial sector. We outline five major financial sector restrictions below.

- **Regulation on Banks' Information Systems and Electronic Banking Services (Official Gazette No. 31069, 15 Mar 2020; in force 1 Jul 2020).** Article 25(1) of this measure requires banks to keep in Türkiye their primary information systems, comprising infrastructure, hardware, software, and data essential to carrying out banking obligations and meeting legal obligations) as well as secondary systems (comprising backups. If those systems or their backups are run by an external/cloud provider, they are still deemed primary/secondary and must also be in Türkiye. Community cloud is only allowed with BRSA permission and tight logical separation. BRSA can also restrict transfers abroad of certain customer/bank data.[91]

- **CBRT Communiqué on Information Systems of Payment and Electronic Money Institutions and Data-Sharing Services (Official Gazette No. 31676, 1 Dec 2021; amended 7 Oct 2023).** Article 21(1) of this measure requires that all primary and secondary systems, along with data backup centers, be located inside Türkiye. Furthermore, Article 21(2) stipulates that every information system used for executing payment transactions—whether between the institution and its own clients or with the clients of other institutions—must also reside in Türkiye, including all backups. If such systems are outsourced, the service provider's systems and backups must likewise be domestically hosted.[92]

---

[89] Presidential Circular No. 2019/12, para. 3 (providing that public institutions' data are not to be stored in cloud services except on the institution's own private systems or with domestic service providers under the institution's control); Information and Communication Security Guide, current framework under the Cyber Security Presidency.

[90] Presidential Circular No. 2019/12 on Information and Communication Security Measures, para. 1 (providing that critical information and data, including population, health and communication records and genetic and biometric data, are to be securely stored in Türkiye). See also Mehmet Bedii Kaya, "Kişisel Verileri Türkiye'de Barındırma Zorunluluğu – Türk Hukukunda Veri Lokalizasyon Hükümleri" (2026), https://mbkaya.com/veri-lokalizasyon-turkiye-kvkk/.

[91] Regulation on Banks' Information Systems and Electronic Banking Services, Official Gazette No. 31069 (15 March 2020), art. 25(1)-(2), requiring banks' primary and secondary systems, including backups, to be located in Türkiye. Current consolidated text available at https://mevzuat.wiki/bankalarin-bilgi-sistemleri-ve-elektronik-bankacilik-hizmetleri-hakkinda-yonetmelik/25.

[92] Central Bank of the Republic of Türkiye, Communiqué on the Information Systems of Payment and Electronic Money Institutions and Data-Sharing Services of Payment Service Providers in the Field of Payment Services, Official Gazette No. 31676 (1 December 2021), as amended, art. 21; current legislation index at https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB%2BTR/Main%2BMenu/Banka%2BHakkinda/Mevzuat/Odeme%2BSistemleri/Teblig.

- **Communiqué on Management and Supervision of Information Systems of Financial Lease, Factoring and Finance Companies.** Article 15(2) of this measure requires subject companies to retain both their primary and secondary information systems within Türkiye. In situations where the management of these systems is outsourced, the service provider's operational systems and backup facilities must also be kept domestically.[93]

- **Regulation on Internal Systems in the Insurance and Private Pension Sectors (25 Nov 2021)** requires insurers, reinsurers and pension companies to keep primary and secondary systems in Türkiye, but explicitly exempts email, tele- and video-conferencing services from the residency obligation.[94]

- **Communiqué on Information Systems Management VII-128.10 (Official Gazette No. 32840, 13 Mar 2025; effective 30 Jun 2025).** VII-128.10 repealed and replaced VII-128.9. Article 27(1) requires entities subject to Capital Markets Board oversight—including, among others, publicly listed companies and pension investment funds—to store their primary systems (the full infrastructure, software, and data enabling secure and continuous electronic access to required information) and secondary backup systems within Türkiye, subject to specified exemptions. Public companies retain some exemptions from the in-country requirement. For crypto-asset trading platforms, VII-128.10 allows certain matching-engine workloads to run abroad on cloud if the provider has a representative office in Türkiye and all records created abroad are transferred back to Türkiye by end-of-day—still keeping the core data-residency model.[95]

Personal Data Protection Law – Cross-Border Transfer Rules (2016): Türkiye's Law on the Protection of Personal Data (No. 6698) contains stricter cross-border transfer conditions than the EU GDPR. Law No. 7499 (Official Gazette, 12 March 2024) replaced Article 9 with effect from 1 June 2024, moving away from the previous explicit-consent model to a three-tier structure: adequacy decisions; appropriate safeguards, including international agreements between public authorities approved by the Board, Board-approved binding corporate rules, standard contracts, and Board-approved written undertakings; and narrow derogations for incidental transfers. While it is positive that: (1) explicit consent ceased to be a basis for regular or repeated transfers on 1 September 2024, and (2) the Authority published standard contract texts and binding corporate rules forms in July 2024, it is unfortunate that, as of September 2026 the Board had issued no adequacy decision for any country.[96] In the absence of an adequacy decision, routine transfers must therefore rely on one of the appropriate safeguards provided by Article 9; standard contracts must be notified to the Authority within five business days of signature. This regime makes routine data flows (e.g. a Turkish subsidiary sharing HR data with its EU parent) legally perilous. Many multinationals have had to localise HR, customer, and other databases in Türkiye to avoid violating the law.[97]

IoT and Telecom Data: Türkiye also requires localisation of certain telecommunications data. In 2019 the ICT regulator (BTK) adopted rules for remotely programmable SIM technologies (eSIMs) requiring, for devices intended for use in Türkiye, that eSIM modules be capable of loading only profiles of Turkish mobile operators while in Türkiye. The subscription-management infrastructure and related storage for those eSIM technologies must be established in Türkiye, and all data within that eSIM system must be kept in Türkiye. The same decision limits international-roaming data service for devices manufactured, imported or marketed for use in Türkiye to the 120-day IMEI registration period. Separately, BTK's permanent-data-roaming regime treats the use of roaming service

---

[93] Communiqué on Management and Supervision of Information Systems of Financial Lease, Factoring and Finance Companies, art. 15(2). See CMS Law, "Data localisation requirements in Türkiye" (24 January 2023), https://cms-lawnow.com/en/ealerts/2023/01/data-localisation-requirements-in-turkiye.

[94] Regulation on Internal Systems in the Insurance and Private Pension Sectors (25 November 2021). See Moroğlu Arseven, "Turkey Announces the Regulation on Internal Systems in Insurance and Private Pension Sectors" (1 February 2022), https://www.morogluarseven.com/news-and-publications/turkey-announces-the-regulation-on-internal-systems-in-insurance-and-private-pension-sectors/.

[95] Capital Markets Board, Communiqué on Procedures and Principles Regarding Information Systems Management (VII-128.10), Official Gazette No. 32840 (13 March 2025), arts. 27(1), 30(3)-(4), 32 and 33. Article 32 repealed VII-128.9; Article 27(1) contains the in-country primary/secondary system requirement; Article 30 contains relevant exemptions. Text available at https://www.lexpera.com.tr/resmi-gazete/metin/bilgi-sistemleri-yonetimine-iliskin-usul-ve-esaslar-tebligi-vii-128-10-32840.

[96] https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim.

[97] Personal Data Protection Law No. 6698, art. 9, as amended by Law No. 7499 (effective 1 June 2024); Personal Data Protection Authority (KVKK), "Yurt Dışına Aktarım," https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim; KVKK, "Standart Sözleşme Bildirim Modülü Hakkında Kamuoyu Duyurusu," https://www.kvkk.gov.tr/Icerik/8043/Standart-Sozlesme-Bildirim-Modulu-Hakkinda-Kamuoyu-Duyurusu. The standard-contract notification deadline is five business days.

by the same IMEI for 91 accumulated days or more in a 120-day period as permanent data roaming. These rules have consequences far beyond mobile telephony, including for connected vehicles and other IoT deployments that rely on centrally managed foreign connectivity.[98]

Regulation on Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector: Article 5(2) of this measure states that, for national-security reasons, traffic and location data should as a principle not be transferred abroad. That principle is not an absolute prohibition: Article 51(6) of the Electronic Communications Law provides that, subject to the generally applicable rules on cross-border personal-data transfers, traffic and location data may be transferred abroad with the explicit consent of the data subject; the sectoral regulation also prescribes specific consent and information requirements where the recipient is abroad.[99]

Domestic Communications Traffic: Presidential Circular No. 2019/12 also requires authorised electronic-communications operators to establish an Internet exchange point in Türkiye and to take measures to prevent domestic communications traffic that should be exchanged domestically from being routed abroad. This is distinct from a categorical prohibition on all transfers of subscriber or traffic data abroad.[100]

Social Media Law No. 7253 (2020): Türkiye amended its Internet Law in 2020 to require foreign social network providers with more than one million daily accesses from Türkiye to appoint a representative in Türkiye and to take necessary measures to host in Türkiye the data of users in Türkiye. The statutory language therefore creates a localization obligation for covered providers, but is not phrased as an absolute requirement that every item of Turkish-user data be stored only in Türkiye.[101]

[98] Information and Communication Technologies Authority (BTK), Decision No. 2019/DK-TED/053, 12 February 2019, https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf. The decision requires Turkish-operator profiles for eSIMs used in Türkiye, in-country eSIM subscription-management infrastructure and storage, and limits international-roaming data service for covered devices to the 120-day IMEI registration period. BTK's separate permanent-data-roaming rules treat 91 accumulated days or more in a 120-day period as permanent roaming.

[99] Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector, art. 5(2) (providing that, for national-security reasons, traffic and location data should as a principle not be transferred abroad); Electronic Communications Law No. 5809, art. 51(6) (permitting transfer abroad with explicit consent, subject to generally applicable personal-data transfer law). See current consolidated regulation at https://www.lexpera.com.tr/mevzuat/yonetmelikler/elektronik-haberlesme-sektorunde-kisisel-verilerin-islenmesi-ve-gizliligin-korunmasina-iliskin.

[100] Presidential Circular No. 2019/12 on Information and Communication Security Measures, para. 20 (requiring authorised communications operators to establish an Internet exchange point in Türkiye and measures to prevent domestic communications traffic that should be exchanged domestically from being routed abroad).

[101] Law No. 5651, Additional Article 4 (as currently in force), requiring covered social network providers to appoint a representative in Türkiye and to take necessary measures to host in Türkiye the data of users in Türkiye. See also Republic of Türkiye, Investment Environment Improvement Coordination Board materials quoting the localization provision, https://www.baib.gov.tr/files/downloads/PageFiles/10777b4b-2d23-ef11-a939-000c29511bae/Files/ek-1.pdf.

H. United Arab Emirates

While the UAE advertises itself as a data hub, certain regulations – especially for health and public sector data – act as localisation mandates. Furthermore, the UAE has mandated strict data localisation for certain types of health and other data. Together, these measures disadvantage foreign companies that lack a local footprint. Please see here for the UAE's ranking in the GDA Cross-Border Data Policy Index.

Federal Personal Data Protection Law (2021): The UAE's PDPL (Federal Decree-Law No. 45 of 2021) came into force on 2 January 2022 and establishes rules for cross-border personal data transfers. Articles 22 and 23 permit transfers to jurisdictions approved as providing an adequate level of protection and also permit transfers, where an adequate level is not available, in specified circumstances including under a contract or agreement requiring the recipient to apply protections equivalent to the PDPL, with the data subject's express consent where consistent with the UAE's public and security interests, or where the transfer is necessary for specified contractual, judicial-cooperation, legal-claims, or public-interest purposes. The PDPL therefore does not impose a blanket data-localisation requirement or a general requirement to obtain prior UAE Data Office approval for every transfer to a non-adequate jurisdiction. The Executive Regulations contemplated by the PDPL had not been issued as of September 2026, so some operational details remain unsettled.[102]

Health Data Law (2019): Federal Law No. 2 of 2019 establishes a general restriction on storing, processing, generating, or transferring outside the UAE health data relating to health services provided in the UAE.[103] However, Ministerial Decision No. 51 of 2021 subsequently established a number of exceptions permitting cross-border storage and transfers for specified purposes, including pharmacovigilance, insurance claims, scientific research and clinical trials, diagnostic testing, telemedicine, and patient-requested transfers.[104]

Abu Dhabi Healthcare Information and Cyber Security Standard: The Abu Dhabi Department of Health's current Healthcare Information and Cyber Security Standard (ADHICS V2) requires cloud environments used by covered healthcare entities to be physically hosted within the UAE, including backup and disaster-recovery environments, and restricts offshore analytics and remote support involving health information. ADHICS V2 further provides that health information may not be stored, shared, processed, disseminated, or transferred outside the UAE unless a valid and specific DoH exemption has been issued. These requirements continue to restrict the ability of EU healthcare, insurance, pharmaceutical, medical-device, and cloud-service providers to use globally distributed infrastructure and cross-border support models.[105]

National Cloud Security Policy (2023; current V2.0): The UAE's National Cloud Security Policy was developed in 2023 and the current V2.0 framework establishes requirements concerning data location, sovereignty, cloud operations, and security for cloud consumers and cloud service providers. The current framework does not categorically exclude foreign technology. In 2026, UAE Cyber Security Council-endorsed sovereign cloud platforms using global hyperscale technology were approved for government and regulated-sector workloads other than data classified as Secret or Top Secret, while maintaining in-country data residency and local operational controls. The practical effect is that access to sensitive public-sector and regulated workloads may depend on use of UAE-based, sovereign-compliant infrastructure, with stricter arrangements applying to Secret and Top Secret workloads.[106]

---

[102] *See* Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data, arts. 22-23, https://www.uaelegislation.gov.ae/en/legislations/1972/download; U.S. Department of Commerce, United Arab Emirates Allows Cross Border Data Flows of Personal Data, https://www.trade.gov/market-intelligence/united-arab-emirates-allows-cross-border-data-flows-personal-data; Chambers and Partners, TMT 2026 - UAE, https://practiceguides.chambers.com/practice-guides/tmt-2026/uae.

[103] *See* UAE Ministry of Health and Prevention, Ministerial Decree No. 51 of 2021 Regarding Cases in Which Health Data and Information May Be Stored or Transferred Outside the Country, https://mohap.gov.ae/en/w/ministerial-decree-no.-51-of-the-year-2021-regarding-cases-in-which-health-data-and-information-may-be-stored-or-transferred-outside-the-country.

[104] *See* Federal Law No. 2 of 2019 Concerning the Use of Information and Communications Technology in Health Fields, arts. 12-13, https://uaelegislation.gov.ae/en/legislations/1209/download; Cabinet Resolution No. 32 of 2020 Concerning the Executive Regulation of Federal Law No. 2 of 2019, https://uaelegislation.gov.ae/en/legislations/1444.

[105] *See* Abu Dhabi Department of Health, Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS V2), effective August 2024, controls CO 9.2 and CS 1.2, https://www.doh.gov.ae/-/media/Feature/Resources/Standards/ADHICS-v2-standard.ashx; Department of Health, AAMEN, https://www.doh.gov.ae/en/programs-initiatives/Aamen.

[106] UAE Government, The National Cloud Security Policy (issued 6 February 2023), https://uaelegislation.gov.ae/en/policy/details/lsy-s-lotny-llamn-lsh-by; UAE Government, National Cloud Security Policy, https://u.ae/en/about-the-uae/digital-uae/digital-transformation/strategies-policies-and-initiatives/National-Cloud-Security-Policy; Emirates News Agency, du Tech's National Hypercloud receives UAE Cyber Security Council certification (5 May 2026), https://www.wam.ae/en/article/177h4m4-tech%E2%80%99s-national-hypercloud-receives-uae-cyber; e& enterprise, UAE Sovereign Launchpad by e& and AWS Now Live

Financial Data & Banking Regulations: The UAE Central Bank's current Outsourcing Regulation for Banks imposes an express local-record requirement. When outsourcing outside the UAE, banks must continuously maintain and store in the UAE the Master System of Record, which includes all Confidential Data; sharing customer Confidential Data outside the UAE requires Central Bank approval and prior written customer consent. In the payments sector, the Central Bank launched the Jaywan domestic card scheme in 2024, and nationwide card issuance began in July 2026. The Central Bank states that Jaywan enables local routing of domestic debit-card transactions and ensures that payment-related data is processed and stored within the UAE. These rules impose concrete financial-sector localisation requirements, although they do not amount to a blanket prohibition on foreign cloud services or all cross-border processing.[107]

Internet of Things: The UAE's current IoT framework imposes local licensing and registration requirements, but it should not be characterised as a general IoT data-localisation rule. TDRA requires IoT service providers to register, and its current service conditions require the applicant to be locally licensed or to have a legal representative in the UAE. The IoT Regulatory Policy permits the use of physical SIMs and eSIMs, while Soft SIMs require prior TDRA approval. Separately, the sale or provision of domestic or foreign SIM cards in the UAE is a regulated activity that may be conducted only by a UAE licensee or an authorised agent. These rules can impose local-presence and connectivity constraints on IoT deployments, but current TDRA materials do not support describing them as a general requirement that IoT data remain in the UAE.[108]

Across UAE, https://www.eandenterprise.com/en/press-release/uae-sovereign-launchpad-by-e-and-powered-by-aws-now-live-and-commercially-available-across-uae.html.

[107] Central Bank of the UAE, Outsourcing Regulation for Banks, art. 6, https://rulebook.centralbank.ae/en/rulebook/article-6-outsourcing-outside-uae; Central Bank of the UAE, Annual Report 2024, https://centralbank.ae/media/ymgnwy3x/2024-en-annualreport.pdf; Al Etihad Payments, Mansour bin Zayed inaugurates 'Jaywan', UAE's first national card scheme (20 July 2026), https://aep.ae/en/news-media/press-releasesarticles/mansour-bin-zayed-inaugurates-jaywan-uae-s-first-national-card-scheme/.

[108] Telecommunications and Digital Government Regulatory Authority (TDRA), IoT Regulatory Policy, Version 1, https://tdra.gov.ae/userfiles/assets/gRSpS8WHHaS.pdf; TDRA, Internet of Things Services Registration, https://tdra.gov.ae/en/Services/internet-of-things-services-registration; TDRA, Licensing FAQ (sale or provision of domestic or foreign SIM cards is a regulated activity), https://tdra.gov.ae/en/About/tdra-sectors/telecommunication/departments/regulatory-affairs-department/licensing.

I. Vietnam

As of September 2026, Vietnam continues to advance severe trade restrictions on foreign digital exports and services market access. Not only has Vietnam failed to remove any of its onerous data localisation mandates or cross-border data restrictions, it is moving quickly to bring into effect new restrictions. The collective effect of these measures is to undermine economic opportunity for the EU – making it more difficult for EU enterprises to export digitally-enabled services and goods to Vietnam

Over the past several years, Vietnam has enacted, implemented, and proposed various measures that raise concerns from a cross-border data policy perspective. Remarkably, despite the strong and unified concerns raised by foreign industry groups, and despite the costs that they impose on EU businesses and workers, Vietnam has:

1. Made no public effort to remove these cross-border data restrictions or data localisation mandates;
2. Introduced wholly new restrictions and mandates that hurt EU interests – e.g., Decree 102 and the Data Security Law – that did not exist eighteen months ago.

Please see **here** for dozens of submissions on Vietnam's numerous cross-border data restrictions and digital sovereignty measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[109]

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the Cybersecurity Law. The Cybersecurity Law went into effect in January 2019. This framework has since been superseded in material part by Vietnam's 2025 Cybersecurity Law, effective 1 July 2026, and Decree No. 333/2026/ND-CP of 19 August 2026, described at Section 4.1(d) above; the discussion below should be read together with that description.[110]

The **Cybersecurity Law** raises serious concerns and will likely significantly impact the ability of many GDA members to provide software products and services in Vietnam. Its breadth far exceeds cybersecurity protection and extends to a broad regulation of the Internet generally. It also grants vast powers to authorities and imposes stringent requirements on software product and service providers to comply with local cybersecurity standards and regulations and to apply for certification by local agencies. In sum, the Cybersecurity Law is a significantly negative development in Vietnam's market access environment for the software sector.

In August 2022, the Ministry of Public Security (MPS) published the final Decree No. 53/2022/ND-CP (**Decree 53**) that took effect from October 2022. Decree 53 is concerning because it requires domestic enterprises (potentially including domestic customers of foreign service providers) to store data within Vietnam and it is not clear whether domestic enterprises include foreign-invested enterprises or subsidiaries of foreign or multinational corporations with head offices in Vietnam. While Decree 53 is silent on the transfer of data overseas, it requires affected enterprises to store data in Vietnam. This leads to market access issues if domestic enterprises are unable to use cloud-based services that do not or cannot store data in Vietnam as part of their services.

Decree 147: Vietnam's Decree No. 72/2013/ND-CP (**Decree 72**) enacted in July 2013, originally mandated that all aggregated information websites, social media platforms, and online content and game providers maintain at least one server in Vietnam "serving inspection, storage, and provision of information at the request of competent state management agencies". This requirement, initially vague and infrequently enforced, became increasingly burdensome and prescriptive after the 2018 Cybersecurity Law, which formally obligated both domestic and foreign service providers of personal and user-generated data to store such data in Vietnam and establish a local legal presence requirement. Under Decree 147/2024/ND-CP (**Decree 147**), effective December 2024, these localisation rules were tightened: offshore platforms hosting Vietnamese users (e.g. social networks, app stores) that lease local data center space or receive at least 100,000 monthly visits must now notify regulators, localise personal data, verify user IDs via local credentials, and respond to takedown and data requests from Vietnamese authorities. These

[109] Global Data Alliance, Submissions in Vietnam (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=&location=loc-vietnam&sector=&language=&posts_filtered=1

[110] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/

data localisation mandates and cross-border controls impose disproportionate compliance burdens, stifle competition, increase infrastructure costs, and heighten risks from centralized data storage.

Personal Data Protection Law: Vietnam's personal data protection regulations are currently set out in its PDP Decree (i.e., Decree 13/2023/ND-CP), which took effect on July 2023. However, Vietnam's National Assembly recently passed the Personal Data Protection Law (**PDP Law**) on June 26, 2025. The PDP Law entered into force on 1 January 2026. The relationship between the PDP Decree and the PDP Law has not been clearly addressed, and it is likely that the PDP Decree will remain in effect until it is explicitly replaced by a new Decree issued under the PDP Law. The PDP Decree imposes restrictive data transfer and data localisation requirements on industries and businesses subject to it. In particular, there are burdensome requirements for personal data processors to register with the Personal Data Protection Commission (**PDPC**) for cross-border transfers of personal data with very detailed requirements for registration, and for the PDPC to carry out annual assessments or audit-like exercises on cross-border data transfers by data transferring entities. These obligations are impractical and may create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

Vietnam's recently passed PDP Law introduces a large number of new restrictions on the ability to transfer data across borders in comparison to the PDP Decree. The PDP Law imposes obligations to conduct transfer impact assessments (although, helpfully, in the enacted PDP Law, this requirement no longer applies to entities using cloud computing services), make impact assessments available to government authorities, and face severe penalties (including cancellation of the authority to transfer data) for any violations.

The above obligations are further exacerbated by the broad definitional scope of "data transfers":

- Article 2(24) defines "overseas transfer" to include not only the act of transferring data, but also the act of accessing data from outside of Vietnam: (i.e., the "use of cyberspace, equipment, electronic means or other forms of transfer of personal data of Vietnamese citizens to a location outside the territory of the Socialist Republic of Vietnam or the use of a location outside the territory of the Socialist Republic of Vietnam for the processing of personal data.")

- Article 45 further defines transfers to include: (a) Sharing personal data with recipients outside [Vietnam]; (b) Sharing personal data at an overseas [or meeting]; (d) Publishing personal data in cyberspace that is received by persons outside [Vietnam]; (dd) Providing personal data to other organizations, enterprises and individuals for the purpose of carrying out business activities; and (e) Providing personal data on the fulfillment of legal obligations abroad or according to the laws of the host country.

The foregoing provisions imply that sharing personal information within Vietnam will be treated as a transfer if it is accessed by those outside of Vietnam, even if that was not the intention and even if that outcome was not foreseeable. Additionally, subparagraphs (c) and (dd) raise questions as to whether provision to a Vietnam-based subsidiary of a foreign enterprise or to a non-national in Vietnam would be deemed to constitute a "transfer" and thus restricted.

Data Law and Draft Implementing Decree: Vietnam's Law on Protection of Consumer Data in the Digital Environment (**the Data Law**) was promulgated in 2023 and took effect in July 2025. It establishes a comprehensive legal framework governing the collection, processing, storage, and transfer of data in Vietnam, including special provisions for what it terms "important data" and "core data." The Draft Implementing Decree for the Data Law (**Draft Implementing Decree**) imposes sweeping obligations on all businesses, both domestic and foreign. Notably, it requires companies that handle important or core data to conduct internal risk assessments, prepare cross-border data transfer impact assessment reports, and submit these reports to the Ministry of Public Security (**MPS**) or other designated authorities for approval. Further, businesses must include specific contractual terms with foreign data recipients and conduct self-assessments of their data transfer operations annually (for important data) or bi-annually (for core data), submitting those results to the government.

Decree 102: In May 2025, the Government of Vietnam issued a new data-related regulation (Decree No. 102/2025/ND-CP regulating Medical Data Management ("**Decree 102**")). Decree 102 entered into full force on 1 July 2025. The Decree incorporates several restrictions on cross-border data transfers and international data access.

- Decree 102 has an **extra-territorial governing scope**, which can broadly apply to any entities directly involved in or related to digital medical data activities in Vietnam. Onshore and offshore companies collecting and processing medical data of their employees or customers in Vietnam could theoretically fall under Decree 102's purview.

- Decree 102 imposes a **strict consent requirement** on the processing, exploitation, and use of personal medical data, with a narrow exemption granted to State authorities when acting in the public interest or for community health purposes. It is arguable that the broader consent exemptions under the Personal Data Protection Decree (e.g., contract performance) may not apply in this context, based on the rule of law application where regulations diverge.

- Decree 102 incorporates certain provisions of the **Data Law by reference**, such as those relating to **cross-border data transfers and risk assessment**s. It remains uncertain whether these referenced provisions will apply directly to companies, or if their applicability depends on whether the entities first meet the threshold conditions outlined in the Data Law.

Moratorium on Customs Duties on Electronic Transmissions: Vietnam has committed in some of its regional trade agreements not to impose customs duties on electronic transmissions, yet its degree of support for the multilateral Moratorium on such customs duties remains uncertain.

Draft Data Security Law (2026): The Ministry of Public Security published a draft Data Security Law in August 2026, following a policy dossier circulated earlier in the year. As drafted, the law would establish a four-level data classification mechanism built on broad definitions of “Core Data” and “Important Data”; apply an automatic classification uplift based on aggregation alone; impose classification, risk-assessment and transfer obligations on processors as well as controllers, including in respect of matters outside a processor’s actual control; retain private-sector localisation requirements; and require annual transfer-impact filings rather than a single durable assessment. The GDA has recommended narrowing the Core and Important Data definitions, removing the private-sector localisation requirements, recognising standard contractual clauses and certifications, and calculating any revenue-based penalty on Vietnam-derived revenue rather than worldwide turnover. The GDA also requested at least 60 additional days of consultation and a consolidated review of Vietnam’s overlapping data, privacy and cybersecurity instruments before further obligations are added.

Decree 330/2026 — Penalties: On 19 August 2026 the government issued Decree 330/2026, establishing administrative penalties for cybersecurity and personal data protection violations, in force immediately and without a transition period. For serious cross-border personal data transfer violations the Decree permits fines of up to 5 per cent of the preceding year’s revenue, together with remedies that can include suspension of transfer activity. It also penalises deficient transfer-impact assessment dossiers. The combination of expansive transfer definitions described above, turnover-based penalties, and no transition period produces a compliance risk that many European organisations will rationally answer by localising.

Other Economies of Interest

We provide brief summaries of cross-border data measures in other markets below.

A. Bolivia

Bolivia has moved toward strict data localisation for government data. Under the new Plan de Implementación de Software Libre y Estándares Abiertos (PISLEA), approved by Supreme Decree No. 5322 of January 23, 2025 (with implementation running through January 12, 2030), Bolivian public agencies are required to keep all "non-public" state data on servers located within Bolivia.[111] The PISLEA is mandatory for the Executive Branch – ministries, entities and institutions under their dependency or oversight, and public enterprises – while the Legislative, Judicial and Electoral Branches, autonomous territorial entities, and public universities "may" apply it. The policy explicitly forbids storing any non-public government data on servers outside national territory (e.g. on foreign cloud platforms). Instead, such data must reside on infrastructure of the state – either on the agencies' own systems or on a cloud service operated by the Bolivian government within the country. (Public data are treated more permissively but are not fully exempt: agencies may use open platforms only so long as they maintain local backups on State technological infrastructure sufficient to guarantee accessibility and preservation — so no category of government data may be held exclusively offshore.)

The PISLEA does not define "public" or "non-public" data, and Bolivia has no general access-to-information statute that supplies a definition, essentially treating most government-held information as non-public unless explicitly open. This localisation mandate, coupled with the requirement that government entities migrate to open-source systems — completion of migration by December 31, 2028 under the plan, followed by a consolidation and optimization phase running from January 1, 2029 to the January 12, 2030 deadline fixed by Supreme Decree No. 5309[112] — poses a barrier to foreign cloud providers: Bolivian agencies cannot host sensitive data with overseas vendors, which effectively blocks international cloud services from much of the Bolivian public-sector market. Please see **here** for Bolivia's ranking in the GDA Cross-Border Data Policy Index.

B. Canada

Canada has historically applied an accountability-based approach, under which an organisation remains responsible for personal information regardless of where it is processed. Bill C-36 would potentially depart from that approach. Section 57 of the Bill would require an organisation to conduct an impact assessment before transferring or disclosing personal information outside Canada. The trigger is geographic rather than risk-based: the assessment is required because the recipient is abroad, not because the transfer presents any assessed risk. The GDA filed comments with the House of Commons Standing Committee on Industry and Technology in August 2026 recommending that the accountability approach be preserved and that, if Section 57 is retained, it be confined to high-risk transfers, permit assessments covering recurring or related transfers, recognise equivalent Canadian assessments, and treat established mechanisms such as the Global CBPR System, EU standard contractual clauses, the UK IDTA and binding corporate rules as satisfying or presumptively satisfying the requirement. We record this measure because the diagnostic test set out at Section 2 of this submission must be applied consistently, including to partners whose alignment the EU seeks.

C. Chile

Chilean financial regulations impose several local data-related obligations.[113] Chapter 20-7 of the Recopilación Actualizada de Normas (RAN) for banks — issued in 2000 by the former Superintendencia de Bancos e Instituciones Financieras (SBIF) and administered by the Chilean Financial Market Commission (CMF) since it absorbed the SBIF in 2019 — sets the conditions banks must meet to outsource services, with heightened requirements for data

---

[111] Decreto Supremo No. 5322, de 23 de enero de 2025 (Bol.), Anexo, Plan de Implementación de Software Libre y Estándares Abiertos, ch. IV, § 4.4 ("Servicios en la nube"), https://agetic.gob.bo/sites/default/files/2025-02/ANEXO-DS-5322.pdf; decree text at https://www.lexivox.org/norms/BO-DS-N5322.xhtml

[112] Decreto Supremo No. 5309, de 8 de enero de 2025 (Bol.), https://www.lexivox.org/norms/BO-DS-N5309.xhtml; Anexo to D.S. 5322, *supra* note 1, ch. V, § 5.3

[113] AWS, Guide to Financial Services Regulations in Chile (2023), at https://d1.awsstatic.com/whitepapers/compliance/Guide_to_Financial_Regulations_in_Chile_SMBR-LEGAL-OK-Dec-2023.pdf

processing and cloud services performed outside Chile.[114] In fact, if a bank outsources "significant or strategic" processing abroad, it must also keep a contingency data processing center in Chile to ensure continuity. This essentially means critical banking processing capacity must be duplicated inside Chile. The obligation dates to 2008, when it reached banks designated systemically relevant, and was extended in 2014 to any supervised entity outsourcing significant or strategic activities abroad; it applies to banks and extends to bank subsidiaries, sociedades de apoyo al giro, and non-bank payment card issuers and operators.[115]

The Chilean regulator relaxed this rule in December 2019 (Circular No. 2,244), allowing the board of directors to waive the Chilean site requirement where an annual report by an independent firm of recognized standing confirms that the entity meets four conditions: a recovery time objective (RTO) approved by the board on the basis of business-impact and risk analyses and tested at least annually; processing sites meeting an operational availability level at or above the RAN Chapter 20-9 standard of 99.98%; sites located so as to mitigate geographic and political risk; and information-security conditions consistent with the entity's own policies and standards. For banks, the waiver additionally requires an adequate operational-risk-management rating in the CMF's most recent evaluation under RAN Chapter 1-13; the rating condition does not apply to non-bank entities or to banks that carry no such rating.[116] The effect of RAN 20-7 is make in-country contingency infrastructure the regulatory default: offshore-only processing of critical workloads is available solely through a conditional, board-approved and externally certified exception, and the CMF retains standing authority to require that particular services be performed in Chile or brought back in-house.[117] Please see here for Chile's ranking in the GDA Cross-Border Data Policy Index.

D. Kenya

Kenya has introduced several measures that require data localisation. Under the Computer Misuse and Cybercrimes Act[118] and its 2024 regulations, Kenya has mandated that any designated critical system or data deemed essential for national security/public order must be hosted in Kenya, unless a special exemption is obtained from the NC4 (National Computer and Cybercrimes Co-ordination Committee).[119] Regulation 28 requires the owner of a designated critical information infrastructure to ensure that the infrastructure on which critical information is domiciled is located in Kenya; an owner seeking to locate critical information abroad must apply to the Committee on Form CMCA 3, and the Committee decides within thirty days after consulting the National Security Council and the relevant security agencies, weighing national security, public interest and whether offshore storage is "necessary."[120]

---

[114] Comisión para el Mercado Financiero, Recopilación Actualizada de Normas para Bancos, cap. 20-7 (Externalización de servicios), https://www.cmfchile.cl/portal/normativa/624/articles-28982_doc_pdf.pdf (chapter index at https://www.cmfchile.cl/portal/normativa/624/w4-propertyvalue-49163.html).

[115] Comisión para el Mercado Financiero, Informe Normativo: Modificación Capítulo 20-7, Externalización de Servicios 3–4 (Dec. 2019).

[116] *Id.* at 11–13 (final text of the amendment to Title IV, No. 1(b)(i)); Circular No. 2,244 (Dec. 23, 2019); CMF, Preguntas Frecuentes: Modificación Norma sobre Externalización de Servicios (RAN 20-7) (Dec. 2019), https://www.cmfchile.cl/portal/principal/613/articles-28050_doc_pdf.pdf

[117] Comisión para el Mercado Financiero, Informe Normativo: Actualización del Capítulo 20-7 de la RAN sobre Externalización de Servicios y nuevo archivo normativo para servicios externalizados 7 n.4 (Apr. 2026), https://www.cmfchile.cl/institucional/legislacion_normativa/normativa_tramite_ver_archivo.php?id=20260407633&seq=1

[118] Computer Misuse and Cybercrimes Act, No. 5 of 2018 (Cap. 79C) (Kenya), https://new.kenyalaw.org/akn/ke/act/2018/5/eng@2022-12-31; see also Government of Kenya, Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations (2024), https://nc4.go.ke/the-computer-misuse-and-cybercrime-criticalinformation-infrastructure-and-cybercrimemanagement-regulations-2024/

[119] Digital Policy Alert, 2025 Digital Digest — Kenya (2025), https://digitalpolicyalert.org/digest/dpa-digital-digest-kenya.

[120] Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024, Legal Notice No. 44 of 2024, reg. 28 ("Localisation of critical information"), Kenya Gazette Vol. CXXVI—No. 18 (16 Feb. 2024), https://new.kenyalaw.org/akn/ke/act/ln/2024/44/eng@2024-02-16.

Separately, the Data Protection Act (2019)[121] empowers the government to require certain data processing to occur only within Kenya for strategic or national interest reasons. The subordinate Data Protection (General) Regulations 2021[122] mandate that personal data involving the "strategic interests of the state" be processed and stored on servers located in Kenya (or at least that a local copy of such data is stored within Kenya). "Strategic" data is defined to include areas like national civil registries, elections data, public finance data, health and education records, and any system designated a protected computer system under section 20 of the Computer Misuse and Cybercrimes Act, which means a broad swath of public data cannot be solely hosted abroad.

Kenya's cloud framework has since hardened from guidance into requirement. The Kenya Cloud Policy, first issued by the Ministry of Information, Communications and the Digital Economy in December 2024, was signed by the Cabinet Secretary on 7 April 2025 and took effect on gazettement on 2 May 2025 as the Kenya Cloud Policy, 2025.[123] The gazetted policy conditions hosting on a data classification framework that all entities — national and county government, state organs, public enterprises, private enterprises, and data controllers and processors — are required to implement. Public entities must procure cloud services by classification: "Top Secret" and "Secret" data must be hosted on dedicated Government Cloud infrastructure located in Kenya; "Restricted" data must be hosted in public cloud infrastructure located in Kenya; and "Open" data must be hosted by a Government cloud service provider. Public entities may turn to third-party providers only where Government providers do not meet the required standards, and then only subject to approval by the Cloud Adoption Committee. Providers serving government must register and obtain accreditation from that Committee, document data hosting locations, and maintain real-time tracking of data movement across jurisdictions. Public entities were given twelve months from publication to comply and to implement a phased migration plan; private-sector compliance remains advisory. In June 2026 the Ministry issued Implementation Guidelines elaborating the data classification scheme and provider registration process.[124] The practical effect is that the most sensitive tranches of Kenyan government data are reserved to state-operated domestic infrastructure, with foreign providers reachable only through a committee approval that must first find the domestic option deficient.

In April 2026 the Office of the Data Protection Commissioner published for consultation a Draft Guidance Note on Cross-Border Data Transfers, recognising multiple transfer bases including adequacy, safeguards, binding corporate rules, contractual safeguards, derogations and consent.[125] The GDA filed comments recommending that the ODPC distinguish routine commercial processing from sensitive military or national security functions, calibrate onward-transfer duties to actual risk, and recognise accountability tools including ISO/IEC 27701 and the Global CBPR System.[126]

---

[121] Government of Kenya, Data Protection Act No. 24 of 2019, § 50, https://www.odpc.go.ke/wp-content/uploads/2024/02/TheDataProtectionAct__No24of2019.pdf.

[122] Data Protection (General) Regulations, 2021, reg. 26, https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf.

[123] Ministry of Information, Communications and the Digital Economy, Kenya Cloud Policy (2024), https://www.ict.go.ke/sites/default/files/2024-12/Kenya%20Cloud%20Policy%20-%202024.pdf; Digital Policy Alert, Kenya Cloud Policy Including Data Localisation Requirements Entered into Force (2 May 2025), https://digitalpolicyalert.org/event/29666-kenya-cloud-policy-2025-entered-into-force-including-authorisation-of-cloud-computing-services; Bowmans, Kenya: Establishing the Regional Digital Hub — Key Highlights of the Cloud Policy 2025 (16 May 2025), https://bowmanslaw.com/insights/kenya-establishing-the-regional-digital-hub-key-highlights-of-the-cloud-policy-2025/

[124] Ministry of Information, Communications and the Digital Economy, Kenya Cloud Policy (2025) Implementation Guidelines (June 2026), https://www.ict.go.ke/sites/default/files/2026-07/Final%20%20Kenya%20Cloud%20Policy%202025%20Implementation%20Guidelines.pdf

[125] Office of the Data Protection Commissioner, Draft Guidance Note on Cross-border Data Transfers (Apr. 2026), https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf; ODPC, Draft Guidance Notes (consultation notice, comments due 15 May 2026), https://www.odpc.go.ke/draft-guidance-notes/.

[126] GDA, Submission on Kenya's Draft Guidance Note on Cross-Border Data Transfers (June 2026), at https://globaldataalliance.org/wp-content/uploads/2026/06/06232026gdakenyadatatransfer.pdf

On 8 September 2026 the ODPC published the final Guidance Notes for Cross-border Data Transfers.[127] The final text addresses several of these points but leaves the core concerns intact. On the positive side, the Guidance expressly recognises that a compelling legitimate interest may support a transfer where an organisation "opts to host personal data on cloud servers located outside the country to enhance operational efficiency, improve service effectiveness, and ensure greater convenience," and it annexes controller-to-controller and controller-to-processor standard clauses that organisations are encouraged to adapt to the circumstances of the transfer rather than adopt verbatim.

On the other side, the Guidance confirms that remote access from abroad and any cloud processing on servers outside Kenya constitute regulated transfers; it reiterates the localisation obligation for the six "strategic interests of the State" categories and directs controllers to assess their infrastructure against gazetted critical information infrastructure designations; it requires explicit consent plus confirmation of safeguards for every cross-border transfer of sensitive personal data, defined to include health status, property details, marital status and family details; and it imposes an eight-condition onward transfer regime under which transfers "for the Data Recipient's own purposes including analytics, commercial exploitation, profiling, product improvement, or marketing — are strictly prohibited," a provision that cuts directly against ordinary sub-processor and service improvement arrangements in enterprise software and AI contracts. Neither ISO/IEC 27701 nor the Global CBPR System appears among the recognised accountability mechanisms, which remain confined to Malabo Convention ratification, reciprocal data protection agreements, binding corporate rules and the ODPC's own standard clauses.

Please see **here** for submissions on Kenya's cross-border data measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[128]

E. Mexico

Mexico historically allowed free data flows, but a recent fintech regulation creates a de facto localisation mandate for certain financial services. A 2021 regulation by National Banking and Securities Commission ("CNBV"), Mexico's bank regulator, requires that e-payment firms have a robust disaster recovery within Mexico – either by using two distinct foreign clouds in different countries or maintaining a secondary on-premises data center in Mexico. In practice, many e-wallet and fintech companies have had to set up local backup infrastructure because using two global clouds is complex. Moreover, Mexican authorities subject foreign cloud usage to a burdensome approval process, while local in-country hosting needs only a simple notification. More specifically, Mexican rules make using foreign cloud providers an approval-intensive process. Financial institutions must notify and in some cases obtain prior authorization from the CNBV (and even Banco de México) if outsourcing core processing or sensitive customer data storage to an overseas cloud service. This asymmetry "de facto" favors local data hosting. Foreign cloud providers and fintech firms face delayed deployments and higher costs in Mexico due to this rule, as it biases banks toward domestic cloud or hybrid setups.

Additionally, Mexico's financial regulations address mandate data localisation based on purported disaster recovery concerns.[129] In 2021, the CNBV updated rules under the Fintech Law that effectively mandate in-country disaster recovery capabilities for regulated fintechs. For example, licensed e-money institutions (IFPEs) and crowdfunding platforms (IFCs) must have robust continuity and backup plans, often interpreted as needing a local data center or secondary site within Mexico for critical operations.[130] These requirements were driven by "prudential" concerns that reliance on foreign cloud infrastructure could be disrupted by external factors, so regulators expect fintech data and systems (especially those of strategic importance) to have an onshore fail-safe. For instance, any cloud service for a bank that is performed abroad requires explicit CNBV approval, and fintech entities need approval from both regulators if the foreign vendor will handle personal or sensitive user data. These conditions mean that

[127] Office of the Data Protection Commissioner, Guidance Notes for Cross-border Data Transfers (2026) at 20–22, https://www.odpc.go.ke/wp-content/uploads/2026/09/ODPC-%E2%80%93-Guidance-Notes-for-Cross-border-Data-Transfers.pdf; see Covington & Burling, Kenya Issues New Cross-Border Data Transfer Guidance (16 Sept. 2026), https://www.insideprivacy.com/cross-border-transfers/kenya-issues-new-cross-border-data-transfer-guidance-familiar-concepts-but-important-local-differences/

[128] Global Data Alliance, Submissions in Kenya (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-kenya&sector=&language=&posts_filtered=1

[129] Baker McKenzie, Mexico – Cloud Compliance Center (2025) at https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/na/mexico

[130] *See* https://www.cofece.mx/wp-content/uploads/2024/10/Estudio-Fintech.pdf

international cloud solutions face extra hurdles in Mexico. In practice, a fintech using a foreign service provider must nevertheless localise its data and go through regulatory scrutiny for the cross-border arrangement.

Finally, in Mexico's 2026 Economic Package, the government proposed to add *Article 30-B* to the tax code, which could create new mechanisms for "blocking" data transfers and digital access to Mexico for certain foreign companies.[131] This provision would require various technology service providers to give Mexico's tax authority (SAT) continuous, real-time access to their internal data systems – enforced through agreements with the National Agency for Digital Transformation and Telecommunications – for those service providers' operations in Mexico.[132] If a service provider fails to comply, the SAT may order a temporary blockage of that digital service in Mexico. More specifically, SAT would instruct internet service providers to restrict access to the non-compliant service for users within Mexican territory.[133]

Please see **here** for submissions on Mexico's cross-border data measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[134]

F. Morocco

Morocco's Decree No. 2-24-921 conditions eligibility to supply qualified cloud services on the nationality of the supplier and the nationality of its shareholders. For certain purposes the Order limits qualified providers to companies incorporated in Morocco with their entire operational and business systems located within the country (Level 1 providers), or to companies with a majority of Moroccan shareholders, with Moroccan persons holding the majority of shares and all data processing and storage taking place in Morocco (Level 2 providers). The GDA submitted comments to the Direction Générale de la Sécurité des Systèmes d'Information and the Moroccan Computer Emergency Response Team on 25 August 2025 urging removal of the local shareholding and ownership requirements and of the associated data localisation and residency requirements. This measure warrants particular attention in this consultation because it is the clearest available illustration of the distinction drawn throughout this submission: nothing in the Decree turns on the security or performance of the service, and no European provider can qualify at Level 2 by improving either.

G. Nigeria

Nigeria has embraced data localisation as a national policy stance. The National Information Technology Development Agency's 2019 "Nigeria Data Sovereignty" guidelines direct that all "sovereign data" be stored on local servers in Nigeria. While "sovereign data" isn't clearly defined, it is interpreted to include government data and potentially any data about Nigerian citizens, essentially pushing for broad localisation.[135]

Nigeria's draft National Cloud Policy 2025[136] would require foreign cloud providers to invest in local infrastructure or partner with local firms to bid on government contracts. These measures haven't all been codified in enforceable law yet, but they signal Nigeria's intent to keep as much data as possible within its borders. The immediate impact is that foreign cloud companies have to establish local data centers (or significant partnerships) to remain competitive in Nigeria, and Nigerian businesses may face government pressure to use domestic clouds even if global services are more advanced.[137]

---

[131] *See* https://www.elfinanciero.com.mx/nacional/2025/10/18/el-sat-te-espiara-desde-tu-cuenta-de-netflix-de-esto-trata-la-reforma-al-codigo-fiscal-2025/; https://www.xataka.com.mx/legislacion-y-derechos/diputados-aprueban-que-sat-revise-datos-tiempo-real-apps-como-netflix-amazon-tinder-asi-nuevo-articulo-al-codigo-fiscal

[132] https://www.ey.com/es_mx/technical/tax/boletines-fiscales/paquete-economico-2026-cambios-codigo-fiscal-federacion

[133] WIRED, El SAT quiere saber cuánto facturan los servicios digitales en tiempo real. Expertos temen por tus datos, at: https://es.wired.com/articulos/el-sat-quiere-saber-cuanto-facturan-los-servicios-digitales-en-tiempo-real-expertos-temen-por-tus-datos

[134] Global Data Alliance, Submissions in Mexico (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-mexico&sector=&language=&posts_filtered=1

[135] Practical Law, Data Localisation Laws in Nigeria (2025) at: https://uubo.org/wp-content/uploads/2019/12/data-localisation-laws-nigeria-w-022-1015.pdf

[136] *See* https://nitda.gov.ng/wp-content/uploads/2025/10/National-Cloud-Policy-2025-Oct2-2025.pdf

[137] Techpoint, NITDA's new rule mandates cloud providers to host key data within Nigeria (2025), at https://techpoint.africa/news/nitda-cloud-providers-host-data/

That draft has since been superseded. On 17 August 2026 Nigeria published its National Digital Cloud Policy, which expressly maintains an open, competitive, multi-provider market and states that it does not impose general data localisation requirements on commercial data. Residency and control requirements are limited to defined categories of government and regulated data. The policy also supports cross-border data flows, regional interconnection, alignment with international standards and mutual-recognition arrangements. This is a materially better outcome than the 2025 draft and is worth recording as such: it demonstrates that a state pursuing regional cloud-hub ambitions can do so without a general localisation mandate. The residual concerns are the 2019 "sovereign data" guidelines, which remain in place and undefined, and the scope of the "regulated data" category under the new policy.

Please see **here** for GDA submissions on Nigeria's cross-border data measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[138]

H. Pakistan

Pakistan has proposed or adopted several cross-border data policies of concern.

First, Pakistan still has not enacted a comprehensive personal data protection law. MoITT's public legislation page continues to list the May 2023 Personal Data Protection Bill as a draft.[139] The published 2023 draft would require "critical personal data" to be processed on servers or digital infrastructure located in Pakistan, and would condition other cross-border transfers on adequacy and specified safeguards. A June 2026 government response to the National Assembly stated that MoITT had finalized a newer data-protection bill, but MoITT has not published that text as enacted legislation and continues to list the 2023 text as a draft. Accordingly, this submission does not rely on the substance of any unpublished revision.

Second, the MoITT also launched a "Cloud First Policy" in 2022.[140] The policy remains approved and applies to federal public-sector cloud adoption and procurement. It classifies government data as open, public, restricted, sensitive/confidential, or secret. Its cloud-selection matrix directs restricted and sensitive/confidential government data to a Government Cloud and secret data to a Private or Government Cloud; the policy defines Government Cloud and Private Cloud deployments as located in Pakistan. These rules create localisation requirements for covered government workloads, while the policy separately contemplates consultation with the Cloud Office for legitimate cross-border data-flow use cases.[141]

Third, in the financial sector, the State Bank of Pakistan (SBP) regulates offshore cloud outsourcing by covered financial institutions.[142] Under SBP's 2023 framework, banks, microfinance banks, digital banks, development finance institutions, and designated payment-system operators and providers may use offshore cloud service providers for non-material workloads. Outsourcing material workloads to offshore providers requires SBP approval on a case-by-case basis. The current framework is therefore an approval-based restriction on offshore cloud use for material workloads, rather than a categorical prohibition on all offshore cloud processing.

---

[138] Global Data Alliance, Submissions in Nigeria (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-mexico&sector=&language=&posts_filtered=1

[139] See Ministry of Information Technology and Telecommunication, *Legislations* (listing "Personal Data Protection Bill May 2023 - Draft"), https://www.moitt.gov.pk/Legislations; see also *Personal Data Protection Bill* (May 2023), §§ 30–32, https://www.moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf; National Assembly of Pakistan, *Questions for Oral Answers and Their Replies* (June 2026), at 34, https://na.gov.pk/uploads/documents/6a1d62bdce349_708.pdf.

[140] See Ministry of Information Technology and Telecommunication, *Policies* (listing "Pakistan Cloud First Policy" as Approved), https://www.moitt.gov.pk/Policies; MOITT, *Pakistan Cloud First Policy* (2022), https://moitt.gov.pk/SiteImage/Misc/files/Pakistan%20Cloud%20First%20Policy-Final-25-02-2022.pdf.

[141] See *Pakistan Cloud First Policy* §§ 7.2–7.3 and Annex E. Section 7.2 provides that Government Cloud infrastructure "can only be located in Pakistan," and Section 7.3 applies the same location rule to Private Cloud infrastructure. Annex E assigns restricted and sensitive/confidential public-sector data to Government Cloud and secret data to Private or Government Cloud. The policy also states that, where legitimate use cases require cross-border data flows, relevant stakeholders may consult the Cloud Office regarding appropriate security standards and controls.

[142] State Bank of Pakistan, *Framework on Outsourcing to Cloud Service Providers* (2023), § E(2), https://www.sbp.org.pk/bprd/2023/C1-Annix-A.pdf; State Bank of Pakistan, *Banking Regulation and Supervision* (current page), https://www.sbp.org.pk/our-operations/banking-regulation-and-supervision.

Fourth, the Securities and Exchange Commission of Pakistan (SECP) imposes a direct data-residency requirement on NBFCs engaged in digital lending. SECP Circular No. 12 of 2024 requires that data not be stored on cloud infrastructure outside Pakistan, and SECP's related self-assessment framework repeats this requirement as a specific data-residency compliance item.[143]

Please see **here** for GDA submissions on Pakistan's cross-border data measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[144]

I. Philippines

Local industry stakeholders and some government agencies have advocated vigorously for localisation mandates in recent years.[145] We summarise a few relevant proposals below.

Draft Executive Order on Government Cloud (2023): In September 2023, a draft Administrative Order (Executive Order) was unveiled to establish a "Cloud First" Government Cloud policy with sweeping localisation requirements. The draft order would mandate local data storage for cloud service providers handling Philippine government data, and even for private entities processing confidential or sensitive personal information on behalf of the government. This measure was not signed into effect.

Draft Department Circular on Localisation of Government Data (2024): In 2024, the Department of Information and Communications Technology (DICT) circulated a draft department circular that sought to require all government agencies to host their data and systems domestically. This draft policy broadly mandated localisation of government data, aiming to bar agencies from using overseas servers for official data.

On October 27, 2025, the DICT issued yet another Policy that required all service providers to store substantially all government-related data within the Philippines, and that established a new "sovereign cloud" accreditation process that was open only to "local cloud service providers."

These requirements apply broadly outside of any discernible national security context to the data of Philippine "departments and agencies under the Executive Branch, State Universities and Colleges (SUCs), Government-Owned or -Controlled Corporations (GOCCs) and their subsidiaries, Government Financial Institutions (GFIs), Local Government Units (LGUs), and other government instrumentalities [and] cloud service providers, intermediaries, and other private entities with transactions, contracts, or data related to … cloud computing services for all covered government agencies."

The Policy requires DICT clearance for storage offshore, for the offshore provider to be subject to Philippines legal jurisdiction, and a complete copy of the data to be maintained within the Philippines territory. Such requirements are onerous and would be a barrier to foreign service providers providing services to the Philippines government.

---

[143] See Securities and Exchange Commission of Pakistan, Circular No. 12 of 2024, *Updated Requirements of NBFCs engaged in Digital Lending*, https://www.secp.gov.pk/document/circular-12-of-2024-updated-requirements-of-nbfcs-engaged-in-digital-lending/; SECP, Circular No. 14 of 2024, *Requirement for Self-Assessment Declaration to be submitted by NBFC engaged in Digital Lending*, https://www.secp.gov.pk/document/circular-no-14-requirement-for-self-assessment-declaration-to-be-submitted-by-nbfc-engaged-in-digital-lending-along-with-application-for-whitelisting-of-digital-lending-app-2/.

[144] Global Data Alliance, Submissions in Pakistan (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-pakistan&sector=&language=&posts_filtered=1

[145] Recent regulatory developments, from the passage of the Open Access Act to the publication of its subsequent Implementing Rules and Regulations (IRR), have suggested that there is significant momentum building for formal data localisation requirements in the Philippines. Any changes mandating that foreign companies store data physically within the Philippines, which we understand is under discussion, pose a significant threat to the country's economic competitiveness, risks derailing the Philippines government digital transformation agenda, and could significantly diminish the country's position as a regional leader in the digital landscape. In addition to the EO's discussed above, concerns exist with respect to the Konektadong Pinoy Act (Open Access Act): lapsed into law on August 23rd 2025, officially taking effect on September 8th 2025. The published Act gives the Department of Information and Communications Technology (DICT) the authority to "formulate policies to safeguard local data, when necessary to advance national security and public interest, with primacy given to cross-border data flows as a key enabler of the global economy" (Rule II, Section 3). On September 24th 2025, DICT conducted a public consultation on the Implementing Rules and Regulations (IRR), with no clarification on whether or how data localisation might be operationalized following the language in the published Act.

A subsequent draft Executive Order on Data Classification and Data Residency, circulated in November and December 2025, took a narrower approach, requiring residency only for data classified "top secret" and "secret," applying heightened encryption and key-management controls to "confidential" data stored offshore, and expressly defining "unclassified / open" data to include routine commercial and financial activity, cybersecurity, fraud prevention, anti-money-laundering, back-up and resilience functions, global customer support, internal reporting and compliance, and AI- and cloud-enabled workloads dependent on globally distributed infrastructure. That approach is a workable model and is close to what this submission recommends generally. The difficulty is that the October 2025 Policy and the draft Executive Order point in different directions and neither has been definitively superseded.

The GDA has engaged extensively with the Philippine government on these matters via GDA submissions made in October 2025, September 2025, March 2025, September 2024, April 2024, December 2023, September 2023, and September 2022.

J. South Africa

In 2024, South Africa implemented a National Policy on Data and Cloud that reinforces data sovereignty for government and sensitive information. Notably, the policy requires that any government data which concerns "the protection and preservation of national security and sovereignty" be stored only on digital infrastructure located in South Africa.[146] In practice, this means highly sensitive government datasets (defense, intelligence, etc.) cannot be hosted with overseas cloud providers – they must reside in local data centers or a state-controlled cloud. More broadly, the policy prioritizes capturing all government data in digital form and migrating state IT systems to the cloud (under South African oversight). It also emphasizes the need for local cloud capacity and data centers, in line with the country's data sovereignty goals. We urge the EU to monitor and oppose any expansion of these data sovereignty provisions.[147] The policy's local-first approach suggests that future regulations could increase local storage requirements in other sectors as well – a trend to watch.

Separately, South Africa brought into force on 6 March 2026 new regulations under the Protection of Personal Information Act governing the processing of health information. Article 6.1 provides that the responsible party is prohibited from transferring a data subject's health information to a third party in a foreign country unless one or more of the requirements in section 72(1) of the Act are met. The regulations apply to insurers, medical schemes and administrators, managed healthcare organisations, pension funds, employers, administrative bodies and institutions acting on their behalf. For European insurers and reinsurers with South African operations, and for clinical research conducted in South Africa, this is a sector-specific transfer restriction of direct commercial consequence.

Please see **here** for GDA submissions on South Africa's cross-border data measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[148]

K. Taiwan

Taiwan maintains a surprisingly large number of data localisation mandates. We summarise these below.

Financial Sector Data Residency Rules: Taiwan's financial regulators impose explicit data localisation and residency requirements on banks and other financial institutions. The Financial Supervisory Commission (FSC) restricts banks from outsourcing or transferring customers' critical financial data to overseas cloud or IT service providers without

[146] Ellipsis, Overview of South Africa's National Policy on Data and Cloud (2024), at https://www.ellipsis.co.za/wp-content/uploads/2024/05/Ellipsis-Overview-of-the-National-Policy-on-Data-and-Cloud-2024-Final.pdf

[147] South Africa Instrumentation & Control, How South Africa's cloud policy fuels digital leadership (2025) at https://www.instrumentation.co.za/25278r

[148] Global Data Alliance, Submissions in South Africa (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=south-africa&sector=&language=&posts_filtered=1

prior approval. This policy effectively requires that core banking data and other sensitive financial information be stored and processed on servers located in Taiwan, unless a special case exemption is granted by the FSC.[149]

Healthcare Data Localisation: Taiwan's health authorities also maintain data residency requirements. Hospitals and healthcare providers traditionally have been expected to store medical records and sensitive patient data on servers located in Taiwan (on-premises or in locally based clouds). The Ministry of Health and Welfare has only cautiously begun to allow use of cloud services in healthcare – for instance, in 2021 it proposed rules to enable certified cloud solutions for electronic medical records, while ensuring compliance with security standards. Moreover, regulators have shown concern about cross-border transfers of health data. For example, in late 2024 the Taiwan Food and Drug Administration (TFDA) drafted a rule prohibiting pharmaceutical companies from exporting any personal data from Taiwan's clinical trials or pharmacy customers to certain overseas jurisdictions (China, Hong Kong, Macau) unless specific exceptions apply. This draft regulation underscores Taiwan's cautious approach: certain health-related personal data cannot leave Taiwan at all, or only under strict conditions.[150]

Data for Localisation for Public Sector Use of Generative AI: Taiwan's National Science and Technology Council (NSTC) has issued an administrative ruling restricting government agencies from using public cloud-based generative AI services unless all data processing is localised within Taiwan.[151] While intended to protect sensitive information, the ruling creates significant market access barriers for global cloud service providers and their AI offerings. The ruling's core requirement mandates on-premises deployment for the use of generative AI by government agencies, explicitly prohibiting public cloud-based AI services for government data processing. This creates a *de facto* data localisation requirement and restricts the use of public cloud through technical specifications. The measure appears to mandate on-premises deployment, physical system isolation, and local data control. These features will result in increased infrastructure costs, reduced access to advanced AI technologies, and limited scalability.

L. **Thailand**

Thailand's IoT regulations require service providers to obtain local telecom licenses and follow rules for SIM registration, numbering and data access. While permanent roaming is not explicitly banned nationwide, local hosting of IoT data is encouraged, and international connectivity is only allowed through licensed partners. In the southern provinces of Pattani, Yala, and Narathiwat, stricter rules apply: IoT devices must be registered with authorities, and only Thai-issued SIMs are permitted – foreign SIMs and cross-border roaming are not allowed.

Of greater consequence is Thailand's draft Artificial Intelligence Act. Section 50 of the draft would impose an in-country processing requirement on AI systems used by government agencies and critical information infrastructure entities. Sections 48 and 49 would impose mandatory contractual controls over international data transfers. The GDA filed comments on 14 August 2026 recommending removal of the Section 50 requirement or, if it is retained, confining it to clearly defined national-security use cases and permitting trusted cross-border processing arrangements; and recommending that, if Sections 48 and 49 remain, they recognise established transfer mechanisms including binding corporate rules, standard contractual clauses, the Global CBPR System and the ASEAN Model Contractual Clauses. The measure is significant beyond Thailand because it locates a localisation requirement inside an AI statute rather than a data protection or cybersecurity statute, and because localisation of this kind would cut critical infrastructure operators off from precisely the cross-border threat intelligence and telemetry on which their security depends.

---

[149] Chambers & Partners, Taiwan Data Protection & Privacy Guide (2025), at https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/taiwan

[150] Chambers & Partners, Taiwan Data Protection & Privacy Guide (2025), at https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/taiwan

[151] *See* https://www.nstc.gov.tw/folksonomy/detail/f9242c02-6c3b-4289-8e38-b8daa7ab8a75?l=ch