Comments for National Trade Estimate Report

Office of the United States Trade Representative
Docket No. USTR–2026–0498

October 29, 2026

Mr. Mark A. DiPlacido
Chair of the Trade Policy Staff Committee
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508
ForeignTradeBarriersReport@ustr.eop.gov

Request for Comments on Significant Foreign Trade Barriers for the 2027 National Trade Estimate Report, 91 Fed. Reg. 58247 (Sept. 14, 2026): Docket Number USTR–2026–0498

Dear Mr. DiPlacido,

The Business Software Alliance ("BSA") and the Global Data Alliance ("GDA")[1] welcome the opportunity to respond to your request for written submissions[2] to the Trade Policy Staff Committee (TPSC) regarding significant trade barriers for inclusion in the 2027 National Trade Estimate Report on Foreign Trade Barriers ("NTE Report"). This submission focuses on cross-border data transfers, data localization, and digital sovereignty measures. It updates the Alliance's October 2025 NTE submission[3] with developments through October 2026.

The GDA is a cross-industry coalition of companies that support tens of millions of American jobs and that are active across all 50 states and in every sector of the US economy. BSA is the global trade association of the enterprise software industry, representing companies that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in over 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation.

We share the view of the Office of the US Trade Representative (USTR) that the United States should be a "production economy" — that is, one "oriented around the production of manufactured goods, agricultural products, services, and knowledge."[4] A strong production economy requires — first and foremost — access to knowledge, information, and data. Such access powers growth, innovation, jobs, and wage growth for companies of all sizes, from small and medium-sized enterprises (SMEs) to large corporations. It supports a strong cybersecurity posture by promoting threat visibility and the early detection of security risks. And it is essential to the functioning of manufacturing plants, modern farms, and service providers in every sector.

Efforts to renew the US production economy are increasingly undermined by barriers that restrict the ability of US companies to offer cross-border services, including restrictions on cross-border transfers of data. This challenge first emerged a decade ago with People's Republic of China (PRC) digital policies purportedly aimed at advancing "Internet sovereignty." Today, many governments — including some of the United States' closest allies and trading partners — are advancing policies of data mercantilism and digital protectionism.[5] Proponents of such policies cite broad concepts of "digital sovereignty," "AI sovereignty," and "data sovereignty" to justify blocking the cross-border transfer of information, mandating data localization, conditioning market access or procurement eligibility on a supplier's origin, ownership, or control, and undermining online economic opportunities to the detriment of domestic and foreign citizens and companies alike.

These trends underscore the importance of sustained efforts to reduce barriers to cross-border data transfers and digital trade. We welcome the renewed efforts of USTR to resolve unfair and non-reciprocal digital trade barriers in US trading partners that hurt US strategic interests, US companies, and American workers.

INTRODUCTION

We appreciate the focus in the NTE process on barriers to digital trade and e-commerce. We view digital trade barriers as corrosive to US national and economic security, as well as US relationships with allies, because:

- Cross-border access to knowledge, information, and technology is essential to America's economic and national security, and is a foundational input to the competitiveness, resilience, and technology leadership of American industry; and

- Foreign governments' unjustified data localization requirements, discriminatory origin- or ownership-related preferences, or other arbitrary, disguised, or unnecessary trade barriers can threaten US economic and national security, while also foreclosing export opportunities for American workers, farmers, manufacturers, service providers, and innovators.

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

BSA and GDA are 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 are headquartered across the globe, and include some of the largest US exporters and some of the most significant investors in, and employers of, American workers. Finally, our members occupy both sides of the question the NTE process asks – both as suppliers of data-driven products and services to customers abroad, and as users of data that must be accessed, consolidated, and analyzed across borders in order to serve those customers and to operate their US businesses.

This submission is organized as follows: An Executive Summary and Discussion section, followed by two Annexes: (1) an overview of the economic benefits of cross-border data transfers, the costs of data localization mandates and data transfer restrictions, and GDA's cross-border data policy principles; and (2) a country-by-country analysis of cross-border data policies of interest, covering Brazil, China, the European Union, India, Indonesia, the Republic of Korea, Saudi Arabia, Türkiye, the United Arab Emirates, Vietnam, and other markets.

EXECUTIVE SUMMARY

We welcome USTR's sustained attention to digital trade barriers and share the concerns that motivate the digital trade and e-commerce portions of the NTE federal register solicitation. Unjustified data localization mandates, discriminatory eligibility rules, and opaque government access regimes in foreign markets impose real and rising costs on American workers, farmers, manufacturers, and service providers. These are legitimate challenges that warrant a sustained US response – through the NTE Report, bilateral negotiations, trade agreements, and, where appropriate, enforcement – and they should also inform how US trading partners, including the European Union, design their own cross-border data policies.

The United States has a great deal to gain by working with its allies and trading partners to promote greater cross-border access to data, services, and technology. In 2024, US exports of digitally deliverable services reached $729.6 billion, against imports of $447.6 billion, for a digitally deliverable services trade surplus of approximately $282 billion. Of those exports, approximately $225 billion went to the EU alone, where digitally deliverable services account for roughly 76 percent of all US services exports.[6] Global exports of digitally delivered services reached approximately USD 5.3 trillion in 2025 and now account for roughly 55% of global services trade.[7] North America exports roughly 82% of its digitally deliverable services to economies outside the region.[8]

Our submission strikes several recurring themes:

1. **The barriers are real, documented, and systemic.** Annex II sets out specific foreign measures – in Brazil, China, Europe, India, Indonesia, the Republic of Korea, Saudi Arabia, Türkiye, the UAE, Vietnam and elsewhere – that restrict the ability of US companies and workers to access information or technology across global digital networks, or to sell data-enabled goods and services abroad.

2. **Digital sovereignty measures in allied markets are a rapidly emerging category of barrier.** These barriers are emerging most rapidly in some of the closest US allies. For example, the European Union's Cloud and AI Development Act proposal, Industrial Accelerator Act proposal, and Public Procurement Act proposals – and Member State schemes such as France's SecNumCloud – would condition market access, procurement eligibility, or cross-border data transfers on a supplier's origin, ownership, or control. These EU measures alone could broadly affect the nearly $2 trillion US-EU trading relationship.

3. **Obstacles to transferring data back to the United States deserve more attention than they receive.** Foreign restrictions on outbound data transfers prevent US-headquartered companies from consolidating operational, safety, quality, and regulatory compliance data at their US parent entities. This is not only a US economic and security challenge, but also a serious legal one – as it directly impedes those companies' ability to discharge obligations imposed on them by US law.

4. **Legitimate public policy tests should assess the character of the measure, not the nationality of the provider.** It is particularly challenging when a foreign measure conditions market access or regulatory status on origin, ownership, or corporate structure rather than on demonstrated security and performance.

NTE Statutory Criteria

Section 181 of the Trade Act of 1974 directs USTR to identify and analyze acts, policies, or practices that constitute significant barriers to, or distortions of, (1) US exports of goods and services, (2) foreign direct investment by US persons, and (3) US electronic commerce.[9] The measures described in this submission fall within each of those categories. Data localization mandates and cross-border transfer restrictions raise the cost of, or foreclose, the delivery of US digital and digitally enabled services. Origin-, ownership-, and nationality-based eligibility criteria condition investment and market access on the investor's nationality. And measures that restrict data flows impede US electronic commerce directly. Several of the measures described below – including mandatory in-country hosting of network and cloud infrastructure and local-SIM requirements for Internet of Things (IoT) devices – also bear on the telecommunications barriers that USTR reviews under Section 1377 of the Omnibus Trade and Competitiveness Act of 1988, 19 U.S.C. § 3106.

Estimated Effect on US Exports

The Federal Register notice asks commenters, to the extent possible, to estimate the increase in US exports of goods or services, US foreign direct investment, or US electronic commerce that would result from removing each significant barrier identified, using four ranges (less than $25 million; $25 million to $100 million; $100 million to $500 million; and over $500 million), together with a description of the methodology used.[10] BSA and GDA members operate across many sectors and markets, and publicly available data do not permit a precise, market-by-market forecast.

In 2024, US exports of digitally deliverable services totaled $729.6 billion. Approximately $361 billion (49.5 percent) went to Europe, and approximately $225 billion went to the European Union alone, where digitally deliverable services account for roughly 76 percent of all US services exports.[11] On those figures, 1 percent of US digitally deliverable services exports to the EU represents approximately $2.25 billion. A displacement effect of only 0.25 percent – approximately $560 million – would therefore exceed the highest of USTR's ranges. We estimate the potential annual effect of the EU's data transfer, cloud sovereignty, and origin-based procurement measures in the "over $500 million" range, on the assumption that, if adopted and applied as proposed, they would displace or deter at least 0.25 percent of those exports. We regard that assumption as conservative: the European Commission itself expects that roughly 30 percent of public-sector data contracts would require assurance Level 2 or higher under the Cloud and AI Development Act proposal, and the higher levels condition eligibility on EU-resident personnel and infrastructure, EU ownership, or EU control.[12]

The corresponding effect of the measures in the other markets covered by this submission is likely to be substantial, but it cannot responsibly be placed in a range without market-specific revenue and cost data. Independent modeling suggests that the stakes are significant: Oxford Economics, modeling five levels of AI-sovereignty restrictiveness in the Asia-Pacific region, found that costs rise non-linearly as origin-based restrictions replace performance-based criteria, with the most restrictive scenarios reducing firm-level AI adoption in Japan from a projected 20.3 percent to 3.4 percent by 2035 (an opportunity cost exceeding $58 billion, or 1.4 percent of 2035 GDP), and in Singapore from 43.8 percent to 9.6 percent (3.2 percent of 2035 GDP).[13]

DISCUSSION

Foreign Barriers to Accessing, Transferring, or Using Data

We group the measures that our members encounter into **six** categories. In each case, implementing governments seek to justify the restriction on sovereignty, security, privacy, or law-enforcement grounds. Regrettably, in many 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 localization mandates and data transfer restrictions

These types of measures may require that data be stored or processed within national territory. They may also impose restrictions on the ability to transfer data from a foreign market back to the United States 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.[14] We offer several illustrative examples below, and a more comprehensive listing in **Annex II** to this submission.

Example 1.1(a) — China: outbound transfer restrictions and "important data" catalogs	
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
Jurisdiction	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 authorize retaliatory measures against overseas entities. The practical result is that US-headquartered groups face material legal uncertainty if they attempt to consolidate and transfer data from Chinese operations.[15]
Isolated or systemic	Systemic. The framework is comprehensive, expanding through sub-national catalogs, 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
Jurisdiction	Kingdom of Saudi Arabia
Practical impact	The National Cybersecurity Authority's Essential Cybersecurity Controls require that an organization's information hosting and storage be inside the Kingdom (ECC-1:2018, 4-2-3-3) and that cybersecurity managed services centers 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 organizations

	localize by default[16]. 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 localization 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
Jurisdiction	India
Practical impact	Multiple sectoral regulators impose localization 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 center 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 US 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.[17]
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 localization	
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
Jurisdiction	Vietnam
Practical impact	Vietnam’s 2025 Cybersecurity Law, effective July 1, 2026, requires domestic and foreign enterprises providing telecommunications, Internet, and value-added services in Vietnam that collect, analyze, 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 August 19, 2026, specifies implementation. It requires domestic enterprises to store covered personal and user-generated data in Vietnam and establishes procedures under which foreign enterprises in a broad set of digital-service sectors can be ordered to localize 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 US 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[18].
Isolated or systemic	Systemic – impacts all sectors.

Example 1.1(e) — European Union: Data Act and Data Governance Act limits on international transfers of non-personal data

Sector	Cross-sectoral; providers of cloud, edge, and other data processing services; industrial, automotive, and health data
Data category	Non-personal data (including the non-personal component of mixed datasets) held in the Union by providers of data processing services; certain non-personal data designated "highly sensitive" under the Data Governance Act
Jurisdiction	European Union
Practical impact	Data Act Article 32 (applicable since September 12, 2025) requires providers of data processing services to take "all adequate technical, legal and organizational measures" to prevent international governmental access to, and transfer of, non-personal data held in the Union where that would conflict with Union or Member State law. A third-country judgment or decision requiring transfer or access is recognizable or enforceable only if based on an international agreement; absent one, transfer or access may occur only if cumulative conditions are met (a reasoned, proportionate, and specific decision; review of the addressee's reasoned objection by a competent third-country court; and due account of legally protected interests), and then only with the minimum data necessary.
Isolated or systemic	Systemic and potentially expanding. The provision applies across sectors and to mixed datasets, and several pending amendments would widen it.

Comparable measures apply in other markets of interest to US organizations, including:

- **European Union —** in addition to the Data Act and Data Governance Act provisions described in Example 1.1(e), the European Health Data Space Regulation (Articles 86–89: Union storage and processing options, adequacy conditions, and certain health data) and the Cloud and AI Development Act proposal (a Level 1 requirement that specified data remain in the Union) each go beyond the established GDPR transfer framework. Both are addressed in Section 1.5 and in Annex II (European Union).

- **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.

- **Kazakhstan** — Article 12 of the Law on Personal Data and Its Protection requires personal data to be stored domestically, and the Digital Code and related amendments adopted in January 2026 extend personal data requirements, including localization, to a wider set of digital objects and data products.

- **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 localization mandate with an explicit shareholding test.

- **Nigeria** — a June 15, 2026 Central Bank of Nigeria circular requires payments transaction data generated in Nigeria to be stored and managed in Nigeria, with full compliance required by January 1, 2027, and contains no express exception for cross-border processing.

- **Saudi Arabia** — draft amendments to the Implementing Regulations of the Personal Data Protection Law, published for public consultation on October 6, 2026, would introduce an express requirement under Article 23 that controllers store personal data in the Kingdom.

- **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 US citizens resident in or traveling to the Emirate.

- **Vietnam** — Article 28.1 of the draft Data Security Law would require Core and Important Data in named sectors, including finance and banking, to be stored in data centers in Vietnam, and would permit international cloud services only where a real-time backup is maintained in Vietnam under the control of state agencies.

These barriers impact US-based entities and US-invested foreign entities in several ways. First, where a foreign government restricts the export of data generated on its territory, the entity that loses visibility is the US parent or affiliate. A US-headquartered manufacturer or a US corporate affiliate with operations in a market that maintains an "important data" catalog or a sectoral residency mandate cannot reliably consolidate and scale that operation's cybersecurity, engineering, legal/regulatory, quality, safety, telemetry, or workforce data at its US headquarters. This could lead to circumstances in which the US corporate parent (or board of directors) is responsible for governing a foreign affiliate whose operational data it cannot see.

The compounding problem is that US law often requires American companies to do exactly what foreign measures prevent. A US entity must be able gather and analyze data from its non-US operations to be able to maintain product traceability, execute cross-border safety recalls, and run screening programs for anti-money laundering, counter-terrorist financing, foreign corrupt practices, sanctions, and export control purposes. A US entity with international operations must also have such cross-border data access to maintain accurate books, records, and internal controls; to trace supply chains for forced-labor and other import-compliance purposes; to manage ICT and cybersecurity risk; or to assess financial or actuarial risks.[19] Foreign localization mandates combined with data transfer restrictions therefore do not only harm American competitiveness; they directly impede compliance with US law.

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; other data types.
Jurisdiction	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 recognized standard for isolating sensitive workloads in multi-tenant environments); mandatory use of Korean-developed encryption algorithms (ARIA, SEED) in place of internationally recognized 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. 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.[20]
Isolated or systemic	Systemic and structural. Successive reforms have been piecemeal; the core eligibility architecture is unchanged.

We highlight Korea because it is a good illustration of a general point that bears directly on USTR's assessment of certification and procurement regimes: 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 program's operation is the measurable outcome.

The Korean framework is also being broadened and expanded 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 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 USTR to seek clarity on these points and to build on Korea's November 2025 commitment "to ensure that U.S. companies are not discriminated against and do not face unnecessary barriers in terms of laws and policies concerning digital services, including network usage fees and online platform regulations, and to facilitate cross-border transfer of data, including for location, reinsurance, and personal data."[21]

1.3 Foreign-government access to sensitive data

A recurring justification for the measures described above is the risk of foreign-government 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 the United States and the Member States of the European Union) 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.[22] 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 authorized 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 authorize 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.[23]

Finally, we underscore that mitigations that actually reduce exposure are technical and contractual rather than jurisdictional: encryption with customer-controlled key management, data minimization 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 domestic and foreign suppliers alike.[24]

1.4 Overly broad data classification

Several US 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 and Vietnam), "sovereign data" (Nigeria), "strategic interests of the state" (Kenya), and "Regulatory Data" (India, securities sector).[25] Because the categories are elastic, companies may encounter significant challenges in determining *ex ante* whether a given dataset may lawfully leave the jurisdiction.

Classification concepts of this kind are also emerging in the European Union: the Data Governance Act empowers the Commission to designate categories of non-personal data as "highly sensitive" for purposes of international transfer restrictions (Article 5(13)), and the European Health Data Space Regulation deems certain electronic health data "highly sensitive" (Article 88). Likewise, as discussed below, many jurisdictions automatically treat health- or finance-related data as "sensitive" or "highly sensitive," and impose broad data localization mandates or transfer restrictions to any such data. Such measures have a disproportionate impact on US-based financial service providers, biopharmaceutical companies, and medical technology firms.

1.5 Digital sovereignty frameworks that condition market access on origin, ownership, or control

A growing number of governments – including close allies and trading partners – are adopting "digital sovereignty" frameworks that condition market access, procurement eligibility, or certification on a supplier's national origin, ownership, headquarters, the nationality of its personnel, or its immunity from foreign law, rather than on demonstrated security and performance.

These frameworks differ in form from the localization mandates described in Section 1.1, but they frequently reproduce their effect: they restrict where data may be stored or processed, who may have access to it, and which suppliers may serve a customer, and they do so by reference to the supplier's origin rather than the security outcome of the measure.

BSA and GDA recognize that every government has legitimate security, resilience, and continuity-of-service interests and may invest in its own technological capability. Our concern is with criteria that exclude suppliers on the basis of nationality, origin, or ownership where less trade-restrictive means – encryption with customer-controlled keys, auditable resilience standards, and contractual accountability – would meet the same objective.

Example 1.5(a) — European Union: Cloud and AI Development Act (CADA) proposal	
Sector	Public sector and – through Article 31 and delegated acts – regulated private-sector entities (energy, transport, health, financial services, and digital infrastructure); cloud, AI, and related hardware
Data category	Public-sector and customer data processed in cloud services; non-personal data of the kind protected by Data Act Article 32; system and telemetry metadata
Jurisdiction	European Union
Practical impact	The European Commission's June 3, 2026 proposal (COM(2026) 502) would establish four assurance levels for cloud services procured by public bodies. Level 1 would require that certain data sets remain exclusively within the Union unless the public body requires otherwise, and Levels 2–4 would require evidence, including data-flow diagrams, that data does not leave the Union; higher levels carry additional EU-presence and certification requirements. Levels 3 and 4 would exclude providers subject to third-country control – at Level 4 with no recognition pathway at all – and Level 3 would be open to such providers only if their home country is designated an "associated third country" (Article 18). Article 30 would require public bodies to procure at least Level 1, and higher levels where public order is at stake; Article 31 would extend the same

	sovereignty risk assessment to NIS2-regulated private entities, with delegated acts able to make it mandatory; Article 16(2) would allow the Commission to amend the criteria by delegated act, with review every 18 months; and Article 32 would add "Union added value" award criteria, including whether critical hardware was designed or manufactured in the Union (Article 32(3)(d)). The Commission expects roughly 70 percent of public-sector data contracts to fall at Level 1, 20 percent at Level 2, fewer than 10 percent at Level 3, and about 1 percent at Level 4.[26]
Isolated or systemic	Systemic if adopted. The criteria are origin-based, may be amended by delegated act, and are expected to be mirrored by private-sector buyers (Recital 66). The proposal follows related origin-based instruments (below) and remains under negotiation, with adoption targeted for late 2027.

Example 1.5(b) — European Union: origin-based procurement, investment, and supply-chain instruments	
Sector	Public procurement across sectors; industrial, clean-technology, and ICT supply chains; telecommunications and other critical-infrastructure networks
Data category	Not data-specific; the instruments condition eligibility to supply data processing, cloud, networking, and related equipment and services on the supplier's origin, ownership, or control
Jurisdiction	European Union
Practical impact	The Industrial Accelerator Act proposal (March 4, 2026) would apply "Union origin" criteria in public procurement and support schemes, exclude operators owned or controlled by entities from jurisdictions without procurement access agreements (treating parties to the WTO Agreement on Government Procurement as equivalent), and attach commitments on technology transfer, EU research and development, and EU workforce and sourcing to certain foreign direct investment in specified sectors.[27] The Public Procurement Act proposal (September 9, 2026) would replace three procurement directives with a single regulation introducing a horizontal "European preference" and empowering the Commission to restrict coverage for third countries that do not give fair access or to avoid security-of-supply dependencies.[28] The proposed revision of the Cybersecurity Act (COM(2026) 11) would permit the designation of "high-risk" third countries and suppliers by reference to ownership and control, with phase-out obligations (36 months for mobile networks).[29]
Isolated or systemic	Cumulative. Each instrument is at a different stage of the legislative process; together they would establish a general presumption in favor of EU-origin and EU-controlled suppliers across procurement, investment, and security regimes.

Example 1.5(c) — France: SecNumCloud qualification	
Sector	Public sector, operators of vital importance, and other regulated entities handling sensitive data in cloud services
Data category	Sensitive and regulated data hosted in cloud services
Jurisdiction	France (European Union)
Practical impact	The ANSSI SecNumCloud qualification requires that the service be immune from non-EU laws and, in practice, limits non-EU ownership of the provider. Non-EU providers can therefore serve qualified-cloud customers only through joint ventures with EU partners.[30]
Isolated or systemic	Systemic within French public-sector and critical-operator procurement, and increasingly cited as a model for EU-level criteria, including the Level 3 and Level 4 criteria of the CADA proposal. The unadopted EU Cybersecurity Certification Scheme for Cloud Services (EUCS) remains a vehicle through which similar sovereignty requirements could be introduced at EU level.

Comparable origin-, ownership-, or personnel-based criteria appear outside Europe, including in Morocco (Decree No. 2-24-921: Moroccan incorporation and shareholding tests for qualified cloud providers), Saudi Arabia (regional-headquarters eligibility for government contracts), and the Republic of Korea (CSAP local-personnel and national-encryption requirements, Section 1.2). The GDA and BSA have urged the United States and the European Union to agree, under paragraph 17 of their August 2025 Joint Statement, that neither will condition market access, certification, or government procurement on requirements that service providers be owned or majority-controlled by nationals, that senior managers or operational personnel hold national citizenship, that suppliers be "insulated from foreign legal jurisdiction," or that products or services satisfy origin-based "dependency" tests.[31]

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.[32] A related group of measures requires that domestic payment transactions be switched, routed, or processed through domestic infrastructure or a state-designated operator – as in Vietnam (Circular 18/2024/TT-NHNN), Azerbaijan, and, in proposed or newly announced form, Nepal and Uzbekistan, as well as, for government payments and state-bank card issuance, Türkiye. These measures function as network-localization requirements even where they do not require data to be stored in-country (see Annex II).

Health data faces localization in the UAE and South Africa, among others. Public-sector and government data faces localization in Brazil, Bolivia, Kazakhstan, Nigeria, the Philippines, Saudi Arabia, South Africa, Türkiye, and Pakistan. For example, 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[33]. Measures that prohibit the cross-border consolidation of data generated at trial sites, in post-marketing pharmacovigilance, and in device servicing tend to degrade the demographic representativeness of clinical evidence; delay safety-signal detection; and impede the regulatory submissions that the Food and Drug Administration and other regulators require.[34]

Such cross-border data restrictions present challenges in the financial and health context, precisely because data localization 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.

RECOMMENDATIONS

1. **Continue to use the NTE Report as an inventory of foreign data barriers, including those under development.** The NTE exercise, conducted annually under Section 181 of the Trade Act of 1974, already provides the evidentiary base for negotiation, allows prioritization by economic impact, and makes the problem visible to Congress, the interagency, and US stakeholders.[35] We encourage USTR to track pending instruments in the 2027 NTE Report.

2. **Prioritize cross-border data and open digital market provisions in trade negotiations and in the implementation of existing frameworks.** Ongoing and prospective negotiations are among 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 favorable treatment of cross-border transfers relative to domestic ones; prohibit sectoral carve-outs that disfavor transfers of financial or health data; 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.

3. **Secure reciprocal, written commitments under the US–EU Joint Statement on origin-neutral technology promotion.** Paragraph 17 of the August 21, 2025 US-EU Joint Statement commits the United States and the European Union to "address unjustified digital trade barriers." The GDA and BSA have urged that this commitment be implemented through four provisions: (i) a continuity-of-service commitment, under which neither Party adopts measures to interrupt lawful access to digital products or services supplied by or to the other; (ii) a prohibition on conditioning standards, certification, procurement eligibility, or the conduct of business on criteria that afford less favorable treatment to the other Party's suppliers – including the origin of a product or service, the nationality of the supplier or its personnel, the location of data or computing facilities, or a requirement that the supplier be immune from the other Party's law; (iii) express preservation of non-discriminatory measures as a means of promoting local technology development; and (iv) a notification and consultation mechanism for proposed measures affecting digital services.[36] Such commitments would give USTR a concrete, verifiable benchmark against which to assess the instruments noted above.

4. **Engage early on pending EU and Member State instruments, before they are finalized.** Several instruments described in this submission are still being developed. At a minimum, USTR should urge: (a) that assurance criteria under the Cloud and AI Development Act be grounded in demonstrated functional performance – including encryption and customer-held-key architectures – rather than corporate origin, nationality, or headquarters location; (b) deletion of Article 31 (extension to NIS2 and other private-sector entities) and of the hardware-origin criterion in Article 32(3)(d), and optional treatment of "Union added value" award criteria; (c) replacement of the "associated third country" model with predictable, reasoned, and reviewable designation rules and realistic transition periods; (d) clarification that Article 32 of the Data Act applies only where a law expressly precludes a transfer to a particular jurisdiction, and rejection of amendments that would extend it to "any" access or require prior national authorization; (e) narrow, risk-based, and non-discriminatory implementation of the high-risk-supplier provisions of the proposed Cybersecurity Act revision; and (f) confirmation that the "European preference" and "Union origin" provisions of the Public Procurement Act and Industrial Accelerator Act will be applied consistently with the EU's obligations under the WTO Agreement on Government Procurement and with the Joint Statement.

5. **Promote interoperable cloud security assurance and proportionate procurement requirements**. USTR should seek recognition of equivalent international certifications and audit evidence, reduce duplicative local assessments, and encourage technology-neutral approaches to workload separation. Governments should distinguish genuinely sensitive workloads from routine enterprise and public-sector applications and permit secure cross-border delivery wherever the risks can be addressed through auditable technical and contractual safeguards. These efforts should explicitly cover SaaS and cloud-delivered cybersecurity services, which may otherwise be excluded by requirements designed around locally hosted infrastructure.

6. **Commission or support a US-specific economic assessment.** We are not aware of any study that models the cost to US GDP, exports, productivity, and employment of: (a) foreign data localization mandates and transfer restrictions that impact US industries; and (b) the costs to US industries of origin-, ownership-, and control-based sovereignty requirements in major export markets. We urge USTR to consider requesting that the US International Trade Commission launch an investigation under section 332 of the Tariff Act of 1930 to this effect.

CONCLUSION

American workers and companies face real, documented, and systemic barriers to accessing data and technology across borders. Those barriers impose costs on US exports and investment and impede compliance with US law. 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.

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 USTR develops the 2027 NTE Report. We would welcome the opportunity to discuss this submission with USTR and/or the Trade Policy Staff Committee.

ANNEX I

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

A. Benefits of Cross-Border Data Transfers

The cross-border movement of data is essential to economic and national security. Companies rely on the ability to transfer data responsibly around the world to create jobs and to make local industries more competitive. Data transfers support US national policy objectives, including cybersecurity,[37] fraud prevention,[38] anti-money laundering, anti-corruption, and the protection of health, privacy, security, safety, consumers, and the environment, and they support shared economic prosperity.[39]

Data transfers support US industries across all sectors. An estimated 75 percent of the value of data transfers accrues to traditional sectors such as agriculture, logistics, and manufacturing.[40] Cross-border data transfers are critical to economic and supply chain resilience in agriculture, automotive, clean energy, finance, healthcare and medical technology, logistics, media, pharmaceuticals, and telecommunications, among many other sectors. Those benefits extend beyond access to foreign customers and suppliers to the core functional, R&D, and operational aspects of business in each sector.

Data transfers support US innovation. Scientific and technological progress require the exchange of information and ideas across borders. The G20 has underscored that the "[c]ross-border flow of data, information, ideas and knowledge generates … greater innovation."[41] Data localization mandates and unnecessary transfer restrictions impede the cross-border exchange of knowledge, technical know-how, laboratory analysis, and scientific research, and they hurt the innovation of the countries that impose them by limiting those countries' own industries' access to the technologies and data sources on which innovation depends.[42]

Data transfers support every stage of the value chain, small businesses, and American workers. The ability to move data across borders responsibly allows companies of all sizes to access key technologies in the cloud, to innovate, invest, and create jobs, and to improve productivity, workplace safety, and environmental efficiency at every stage of the production life cycle: R&D, market forecasting, safety and predictive maintenance, regulatory compliance, sales, inventory control, supply chain management, and post-sale service (including product traceability and recall). The following figures illustrate the stakes for small businesses and for the US workforce:[43]

- 32.5 million US small- and medium-sized businesses (SMEs) account for 99.9 percent of all US businesses, 48 percent of all US workers (61.2 million), and 90 percent of new business openings.
- SMEs account for 95 percent of all US exporting enterprises and roughly 25 percent of US exports; with greater foreign market access, SMEs estimate that they could increase sales by 15–40 percent and hire between 10 and 50 new employees each.
- 65 percent of SMEs move data across borders; 40–60 percent of SME survey respondents identified divergent data privacy rules, and 30–40 percent identified data localization rules, as key challenges.
- 67 percent of new US science, technology, engineering, and mathematics (STEM) jobs are in computing and software; nearly 16 million workers are employed in software jobs in the United States; and US workers in export-intensive sectors earn an average 15 percent more than workers in other sectors, with the highest premium (19 percent) in digitally skilled, export-intensive manufacturing.[44]

B. Costs of Data Transfer Restrictions and Data Localization Mandates

The unintended economic consequences of unreasonable data transfer restrictions and data localization mandates must not be underestimated. Such measures have consequences for jobs, exports, and investment. For both local enterprises and foreign-invested enterprises, they disrupt operations, raise the costs and challenges of providing services and manufacturing goods, and make it harder to invest and keep local workers employed. By some estimates, the number of data regulations worldwide grew by over 800 percent between 1995 and 2015 and now exceeds 250.[45] Four categories of cost deserve emphasis.

First, data localization mandates and unreasonable transfer restrictions are particularly damaging to the local industries – including agriculture, logistics, and manufacturing – that account for an estimated 75 percent of the value of data transfers.[46] Second, they raise the costs of international trade. One study estimates that digital tools helped micro, small, and medium-sized enterprises across Asia reduce export costs by 82 percent and transaction times by 29 percent,[47] and electronic commerce platforms, which operate on the basis of cross-border data transfers, are

estimated to reduce the cost to local firms of distance in trade by 60 percent.[48] Third, they hurt innovation and competitiveness by cutting local industries off from productivity-enhancing software, scientific and research publications, and manufacturing data and blueprints, and they undermine the attractiveness of the countries that impose them as destinations for investment and R&D. Fourth, they deprive local industries and economies of the tailored, data-enhanced analytics and AI-driven insights that come from consolidating local data sets within larger regional or global data sets.

The costs of origin-based sovereignty requirements are now being quantified. Oxford Economics, modeling five levels of AI-sovereignty restrictiveness across the Asia-Pacific region, found that costs and risks rise non-linearly when origin-based restrictions replace functional, performance-based criteria. At the most restrictive levels, firm-level AI adoption in Japan would fall from a projected 20.3 percent to 3.4 percent by 2035, with total opportunity costs exceeding $58 billion (1.4 percent of 2035 GDP); in Singapore, adoption would fall from 43.8 percent to 9.6 percent, at an opportunity cost of 3.2 percent of 2035 GDP.[49] The same dynamics – higher costs, slower diffusion, and lower productivity – should be expected wherever comparable restrictions are adopted, including in the European Union. The study does not cover the European Union or the United States, which is why Recommendation 9 urges a US-focused assessment.

C. Policy Arguments Relating to Data Transfer Restrictions and Data Localization Mandates

Several grounds are frequently cited as the basis for imposing data restrictions, but those grounds are often based on misconceptions, or are cited to justify trade barriers that are more restrictive than necessary to achieve the asserted objective. Correcting such misconceptions and identifying less restrictive means of achieving specific policy outcomes are important goals for both private and public sector representatives engaged in international dialogue on cross-border data policy. We address four common arguments.

- **Cybersecurity.** How data is protected is much more important to security than where it is stored. Companies may store data at geographically diverse locations to reduce the risk of physical attacks, to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. Cross-border transfers also allow cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. When governments mandate localization or restrict the ability to transfer and analyze data in real time, they create unintended vulnerabilities: silos that add complexity without security benefit; impaired real-time cyber awareness and responsiveness; weakened collaboration on detection and response; degraded third-party cybersecurity services; and concentrated risk and single points of failure.

- **Privacy.** Data localization mandates and data transfer restrictions do not increase personal data protection. Organizations that transfer data globally typically implement procedures to ensure that the data is protected even when transferred outside of the country. Different organization types and business models require different transfer mechanisms that are not interchangeable, so businesses need to be able to rely on a range of mechanisms – adequacy decisions, certifications, codes of conduct, binding corporate rules, and standard contractual clauses – that are integrated into national laws including those of the European Union,[50] Japan,[51] New Zealand,[52] and Singapore.[53] Those mechanisms are consistent with the "accountability principle" described in the OECD Privacy Framework,[54] the APEC Privacy Framework,[55] the APEC Privacy Recognition for Processors system,[56] the APEC Cross-Border Privacy Rules system,[57] the Global Cross-Border Privacy Rules Forum,[58] and the ASEAN Model Contractual Clauses.[59] Where differences exist among data protection regimes, governments should create tools to bridge those gaps in ways that protect privacy and facilitate global data transfers.

- **Law-enforcement and regulatory access.** The location of data is not the determining factor in whether authorities can obtain it. Responsible service providers work to respond to lawful requests for data consistent with their obligations to their customers and to protect consumer privacy. Where a provider faces a conflicting legal obligation not to disclose, authorities have established options: mutual legal assistance treaties and agreements, multilateral treaties, agreements under the US CLOUD Act, and letters rogatory.

- **Nationality, origin, or ownership as a proxy for security.** More recent "digital sovereignty"-based arguments hold that a supplier's nationality, ownership, headquarters location, or immunity from foreign law is a reliable proxy for the security or resilience of its service. It is not. In fact, origin-based criteria narrow the range of providers and architectures available to customers, concentrate rather than distribute operational risk, and

impede the cross-border flows and systematic redundancies on which resilience depends. Instead, technical and contractual controls – encryption with customer-held keys, access-management architectures, auditable resilience and continuity standards (such as ISO/IEC 27001, 27017, 27018, and ISO 22301), and published transparency reporting – address the risks in a meaningful, measurable way. Finally, there is an emerging trend toward "data mercantilism," a perspective premised on the view that cross-border restrictions and localization mandates offer protectionist economic benefits by fostering "local champions," jobs, and investment. Those assumptions are not supported by the economic evidence.[60]

D. Cross-Border Data Policies in International Agreements

The United States and its allies play an important role in ensuring that global cross-border data policies support economic and national security. Consistent with prevailing practice,[61] we urge the United States to continue to negotiate cross-border data commitments of the following kinds, subject to appropriate exceptions and limitations for national security and public policy purposes:

- Cross-border transfer of information by electronic means: across all sectors, Parties shall not prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of a business.
- Location of computing facilities: across all sectors, Parties shall not require the use or location of computing facilities in their territory as a condition for conducting business.
- Customs duties: Parties shall not impose customs duties on electronic transmissions.

These commitments address the cross-border impact of data regulations; they do not prevent the United States or its partners from enacting rules to promote legitimate public policy objectives such as privacy or cybersecurity. To address data regulations that involve incidental restrictions on transfers, we urge the United States to continue to clarify that such regulations should: be necessary to achieve a legitimate public policy objective;[62] not be applied to produce arbitrary or unjustifiable discrimination or disguised trade restrictions;[63] not impose restrictions on transfers greater than necessary;[64] not improperly discriminate among economic sectors;[65] not modify conditions of competition by according less favorable treatment to cross-border transfers relative to domestic ones;[66] be designed to be interoperable with other national legal frameworks;[67] and be developed in a transparent and accountable manner. These requirements reflect longstanding tenets of international law and practice: freedom to pursue necessary public policy objectives; renunciation of discrimination against non-national persons, products, services, or technologies; minimization of trade-restrictive effects; and due consideration for trading partner laws.[68]

Finally, the WTO Moratorium on customs duties on electronic transmissions and the Work Program on Electronic Commerce lapsed after the Fourteenth WTO Ministerial Conference (MC14) in Yaoundé in March 2026 failed to renew them, notwithstanding that 165 of 166 Members ultimately supported a more than four-year extension.[69] Without a renewed moratorium, WTO Members are no longer constrained by a multilateral commitment from imposing customs duties on electronic transmissions, which adds to the importance of securing that commitment in bilateral and plurilateral agreements.

E. The GDA Cross-Border Data Policy Principles

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.[70] The principles are **summarized** 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.[71]

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.[72] Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.[73] 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.[74]

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

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;[75]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[76]
- 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;[77] and
- Include other procedural safeguards and due process.[78]

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.[79]

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 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.[80]

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[81] 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, and little analysis of whether the proposed measure (and its most restrictive aspects) are necessary and proportionate to address any such risks.[82]

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.[83] 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 **localization** 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,[84] security,[85] and safety.[86] In the international context, this may include:

- **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 Localization:** Another trust-building mechanism involves negotiating agreements to prohibit unnecessary data transfer restrictions and data **localization** 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.[87]

ANNEX II

ANNEX II – COUNTRY-BY-COUNTRY ANALYSIS

We provide below a country-by-country summary of measures of concern in relation to cross-border data transfer restrictions and data localization mandates.

National policies on cross-border data transfers and data localization 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 localization 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 summarize measures of concern in several economies of priority interest: Brazil, China, the European Union, India, Indonesia, the Republic of Korea, Saudi Arabia, Türkiye, the UAE, and Vietnam. We also summarize measures of concern in other markets of interest: Azerbaijan, Bangladesh, Bolivia, Canada, Chile, Japan, Kazakhstan, Kenya, Malaysia, Mexico, Morocco, Nepal, Nigeria, Pakistan, the Philippines, South Africa, Taiwan, Thailand, and Uzbekistan.

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.[88]

***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 recognizes 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.[89]

Data and Server Localization 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.[90]

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, **US** IoT providers may be forced to migrate devices to a Brazilian operator, local SIM, or other arrangement.[91]

Sovereign Cloud Initiatives (2026): In August 2026 Brazil advanced two public-sector cloud initiatives framed around digital sovereignty. On August 11, 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 September 3, 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,[92] although the initiative is intended to increase national control over data and infrastructure.[93]

B. China

We outline below several concerns and recommendations regarding cross-border data policies and measures in China. Many BSA and 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.[94] 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.[95]

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 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 June 10, 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)[96] 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 localization 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 localization 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 localization and data transfer provisions noted above (PIPL Art. 38(1), 40);
(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 recognized 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).

32 global associations raised these concerns in a letter submitted to China during the drafting process, but the concerns were not addressed.[97]

***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.[98]

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 **catalogs** 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.

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 **August 7, 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 centers 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 organizations across data-intensive sectors generally, including manufacturing, automotive, financial services and health. The practical effect would be to add a broad localization baseline underneath transfer pathways that remain formally available.

Guidance for the Secure Cross-Border Transfer of Automotive Data (2026 Edition): On **February 3, 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" catalogs 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 US-headquartered vehicle manufacturers and their suppliers, this is among the most consequential single measures in this Annex: it prevents a US 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 characterizing such data as a strategic asset linked to national security. Separately, the Ministry of State Security warned against the unauthorized 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.

Cloud Service Classification and Local Deployment: In addition to restrictions on cross-border data transfers, the classification of cloud offerings under China's value-added telecommunications regime can constrain foreign suppliers' market access. Suppliers report that some SaaS offerings can operate outside that licensing regime, while others face licensing, local deployment, data-storage, and associated security requirements, or must be delivered through a local partner. The treatment therefore varies across services, and recent liberalization has not resolved all barriers. USTR should encourage China to publish clear and consistently applied classification criteria, avoid extending telecommunications licensing to ordinary enterprise software services, and remove unnecessary requirements for separate local infrastructure or partner-operated delivery.

C. European Union

Over the past several years, the European Union has built a dense body of digital regulation relevant to software and data service providers – in privacy, cybersecurity, data transfers, cloud, and artificial intelligence – and since 2025 it has placed "digital sovereignty" at the center of its industrial and trade agenda. The EU is also the destination for approximately $225 billion of US digitally deliverable services exports (2024), which account for roughly 76 percent of all US services exports to the EU.[99] BSA and GDA members fully respect and share the EU's interest in protecting the security and privacy of its citizens and in harnessing the value of data. Our concern is with the subset of measures that, by design or in practice, (i) condition market access, procurement eligibility, or certification on a supplier's origin, ownership, or control; (ii) restrict international transfers of non-personal data beyond the GDPR framework; or (iii) leave cross-border data policy dependent on unresolved legal challenges. Please see here for GDA submissions on the EU's cross-border data restrictions and digital sovereignty measures and here for its ranking in the GDA Cross-Border Data Policy Index.[100]

D. India

Overview/Business Environment

The commercial environment remains challenging in India, in part due to an increase in restrictive cross-border data policies.[101] 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 localization requirements threatens the commercial and strategic interests of US 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,[102] regulations on machine-to-machine (M2M) systems,[103] and payment processing regulations[104], to proposed rules for the Digital Personal Data Protection Act.[105]

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.[106]

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 localization requirements in earlier versions, the provisions in the final Act are significantly improved. The final Digital Personal Data Protection Rules, 2025, notified on November 13, 2025 and published in the Gazette of India on November 14, 2025,[107] retain authorities to require data localization and to restrict international data transfers. Rule 12(4) empowers the government to require data localization 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 November 13, 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.[108]

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),[109] 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 **localization** 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."[110] "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.[111] 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.[112] While MeitY issued subsequent "Frequently Asked Questions (FAQs) on the Directions", it still did not address concerns around localized log storage.[113]

CERT-In Guidelines regarding AI-Accelerated Vulnerability Protection and Response Requirements for Original Equipment Manufacturers (OEMs), and Technology Providers: As per the Guidelines, industry is expected to adopt secure development practices, maintain an updated Software Bill of Materials (SBOM), and immediately notify CERT-In and customers of any Critical or Zero-day vulnerabilities. Technology providers must report cyber incidents within 6 hours and permit Indian organizations or CERT-In to perform independent security audits and assessments

of their products and services. The challenging requirements include providing crypto BOMs, Quantum component inventory, vulnerability remediation Action Taken Report, et al. These Guidelines are further forwarded by the Telecom Department and Banking authorities to telecom service providers and banks, respectively, turning them into a compliance requirement from OEMs.

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 localization 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 fulfill reporting obligations. While the CSCRF came into effect on January 1, 2025, SEBI issued clarifications (December 2024) that the requirements around data localization is put on hold until further notification. SEBI directed the industry to set up local working groups to formalize the approach to data localization 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, **among** other requirements, a **localization** 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.[114] Likewise, IRDAI's Reinsurance Regulations impose stringent data localization 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 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 localization of government data.[115] CSPs participating in the initiative must have "data center facility within India".[116] These requirements also affect providers of software-as-a-service that depend on underlying cloud infrastructure. Suppliers report that serving government customers requires hosting their services in Indian data centers operated by MeitY-empaneled providers. Requirements for deployment within air-gapped government networks create additional barriers for globally delivered cloud services. The practical consequence can be exclusion from procurement opportunities where suppliers cannot replicate their services in a separate local or private-cloud environment. USTR should encourage India to calibrate these requirements to the sensitivity of the workload and permit secure cloud delivery models supported by internationally recognized certifications and auditable safeguards.

***Geospatial and Weather Data Restrictions*:** The National Data Sharing and Accessibility Policy (NDSAP) notified by the Ministry of Science and Technology furthers data localization making it challenging for software companies to leverage global computing facilities, especially when it comes to government-owned weather data.[117] 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 US 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 localization 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.[118] In December, the Committee published the revised report.[119] In our written comments, we highlighted numerous concerns including mandatory sharing of proprietary non-personal data, restrictions on cross-border data transfers and local storage requirements.[120] 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 localization. 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.

E. Indonesia

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.[121]

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 October 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.[122]

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 localization requirements has been omitted because no such draft has been published and the proposal cannot presently be characterized with sufficient reliability.[123]

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 localization mandate, but it will add substantive transfer-assessment, notification, and documentation requirements when it enters into force.[124]

Data Localization 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. 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.[125] Article 2.29 of the US–Indonesia Agreement on Reciprocal Trade addresses this issue.[126]

Cloud Services: 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 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.[127]

Local Certification Requirements for Public Cloud: Ministry of Communications and Digital Decree No. 519/2024 requires public cloud providers seeking to participate in the National Data Center Ecosystem to hold Indonesian certifications, including SNI ISO 9001, SNI ISO/IEC 27001, SNI ISO/IEC 27017, and SNI ISO/IEC 27018, without accepting the corresponding international certifications as equivalent. Industry also reports uncertainty over implementing guidance and the availability of local certification. These requirements duplicate existing assurance

processes and can delay or prevent access to public-sector customers. USTR should urge Indonesia to recognize equivalent international certifications, publish clear and workable implementation procedures, and avoid unnecessary local-presence or infrastructure requirements as conditions of qualification.

F. Republic of Korea

The overall commercial environment in the Republic of Korea (Korea) is mixed on the subject of cross-border data transfers and data localization.[128] Korea has a strong IT market and a mature legal system. However, 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.[129]

Cross-Border Data Transfers and Server Localization: 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 US service providers seeking to enter Korea's public sector. US 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 recognize 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 recognized 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 Localization. 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.

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 a US 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.

In April 2026, the Ministry of Science and ICT and the National Intelligence Service announced plans to consolidate CSAP certification and NIS verification into a single NIS-led framework aligned with the National Network Security Framework (N2SF). Industry understands that draft guidelines presented in September 2026 would recognize AES encryption and international Common Criteria certificates and permit operations and management systems to be located overseas. If adopted and implemented as described, these changes would address several longstanding concerns. However, the draft would retain physical separation of data systems for Sensitive workloads, preserving an important barrier to globally delivered cloud services. USTR should seek publication and clarification of the final requirements, recognition of logical separation below the Classified tier, and confirmation that certification provides a sufficient basis to compete for public-sector contracts without an additional approved-vendor requirement.

The continued lack of meaningful market access for US service providers underscores the need for sustained and elevated US Government advocacy. Korea's piecemeal and limited adjustments have failed to address the fundamental structural barriers that prevent US service providers from competing on fair and equal terms in the public sector market. The CSAP remains a significant non-tariff barrier for US service providers.
The transition to the new NIS-led framework provides an opportunity to remove the remaining barriers to public-sector cloud procurement. In implementing Korea's digital trade commitments, the United States should seek explicit commitments covering both the existing framework during the transition and its successor. 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 recognized 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 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 recognized 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.[130] Moreover, South Korea's network segregation rules, which require internal and external networks to be physically segregated,[131] effectively require the localization 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 localization mandates also effectively inhibit central oversight and information sharing across borders, reducing cyber threat awareness and visibility.

Besides data localization, 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.[132]

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. Korea long declined applications by foreign enterprises to export cartographic and other location-based data, including in 2007 and 2016. On February 27, 2026, Korea conditionally approved the export of 1:5,000-scale map data to a US technology provider, subject to conditions that include: (a) processing on domestic servers operated by a local partner; (b) transfer limited to government-reviewed base-map and transportation-network data; (c) removal or restriction of coordinate data; obscuring of sensitive imagery; (d) exclusion of contour data; and (e) a "red button" suspension mechanism and a designated map affairs officer.[133] While the approval is a step in the right direction relative to the US-Korea November 2025 Joint Fact Sheet, the onerous conditions attached to it confirm that the regime still turns on case-by-case governmental discretion and that no broad, transparent licensing standard exists.

G. Saudi Arabia

Saudi Arabia has pursued assertive data localization 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 localization requirements particularly for Saudi government data and certain regulated financial-sector workloads, and since January 1, 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.[134] 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.[135]

Cloud and Cybersecurity Localization 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-localization controls were transferred to the National Data Management Office (NDMO) at the Saudi Data and AI Authority (SDAIA). Separately, the Communications, Space and Technology Commission's Cloud Computing Services Provisioning Regulations (Version 4), effective October 10, 2023, remain a concrete localization measure for Saudi government data. The regulations provide that[136] 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.[137]

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. Subject to the problematic 2026 regulatory amendments discussed below, 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 in the destination jurisdiction. 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.[138]

Draft Amendments to the PDPL Implementing Regulations (October 2026): On October 6, 2026, SDAIA opened a public consultation, running through November 5, 2026, on draft amendments to the PDPL's Implementing Regulations. The amendments would introduce an express localization requirement under Article 23, according to which controllers would be required to store personal data in the Kingdom, while continuing to permit transfers and disclosures outside the Kingdom in accordance with the PDPL and its regulations. Under a proposed Article 34, the amendments would make registration with the National Register of Controllers mandatory where a controller transfers or discloses personal data outside the Kingdom.[139] If the storage requirement operates as a default to which cross-border transfers are exceptions, the amendments would convert the PDPL's current transfer framework – built on adequacy, appropriate safeguards, and transfer-risk assessments – into a localization regime, and would require companies that today serve Saudi customers from regional or global infrastructure to localize storage or restructure their architectures. We urge USTR to encourage SDAIA to preserve the PDPL's risk-based transfer framework; to confine any storage requirement to narrowly defined categories of data presenting a clearly articulated national-security risk; and to recognize the United States as providing an adequate level of protection for purposes of Article 29 of the PDPL and the Regulation on Personal Data Transfer Outside the Kingdom.

Financial Sector Localization: Saudi financial sector rules continue to impose localization and approval requirements. The Cyber Security Framework of the Saudi Central Bank (formerly known as the Saudi Arabian Monetary Authority) (SAMA) 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 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 January 1, 2024,[140] 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.[141]

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.[142]

H. Türkiye

Türkiye has imposed data localization mandates 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.

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 organizations 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. [143] This approach is mirrored in the Information and Communication Security Guide.[144]

Banking & Cloud Localization 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.[145]

- **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.[146]

- **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.[147]

- **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.[148]

- **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.[149]

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, March 12, 2024) replaced Article 9 with effect from June 1, 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 September 1, 2024, and (2) the Authority published standard contract texts and binding corporate rules forms in July 2024, it is unfortunate that, as of October 2026 the Board had issued no adequacy decision for any country.[150] 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 US parent) legally perilous. Many multinationals have had to localize HR, customer, and other databases in Türkiye to avoid violating the law.[151]

IoT and Telecom Data: Türkiye also requires localization 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 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.[152]

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.[153]

Domestic Communications Traffic: Presidential Circular No. 2019/12 also requires authorized 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.[154]

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.[155]

Cybersecurity Law No. 7545 (2025): Law No. 7545 on Cybersecurity, published in the Official Gazette on March 19, 2025, empowers the Cybersecurity Presidency to authorize and certify cybersecurity products, systems, and services. Under Article 7, cybersecurity products, systems, and services used by public institutions or within critical infrastructure must be supplied by providers authorized and certified by the Presidency, and the Law provides that domestic and national products are to be primarily preferred in cybersecurity-related activities. On May 5, 2026, the Cybersecurity Board determined 15 critical infrastructure sectors, including finance, digital infrastructure, digital services, electronic communications, energy, healthcare, and transportation. The detailed obligations that will apply to those sectors – technical compliance requirements, supply-chain and third-party technology requirements, and potentially localization of critical systems – await secondary legislation and further determinations by the Presidency. Article 16 provides for administrative fines of TRY 1 million to TRY 10 million for non-compliance with certain obligations.[156] How the certification process and the statutory preference for domestic

products are implemented will determine whether foreign technology providers can compete for public-sector and critical infrastructure business on the basis of security performance rather than origin.

Domestic Card Scheme Preference: **Presidential Decree No. 2025/1 on the Use of Cards Issued by Local Card Schemes (2025):** This provision, published in the Official Gazette on January 16, 2025, requires listed public bodies to make specified payments – including personnel pay, pensions, and social aid – principally with cards issued under domestic, licensed card schemes, and directs that, for cards issued or renewed by state-owned banks, priority be given to the infrastructures of card system institutions resident and licensed in Türkiye.[157] The only operating domestic card scheme is TROY (Türkiye'nin Ödeme Yöntemi), a Turkish payment card network established in 2016 and operated by the Interbank Card Center (BKM), which is majority-owned by Türkiye's central bank.[158] Read together with the requirement in Article 21(2) of the CBRT Communiqué described above that every information system used to execute payment transactions reside in Türkiye, the Decree channels government payment flows and state-bank card issuance to domestic infrastructure and limits the scope for US-based networks to compete on the merits.

I. United Arab Emirates

While the UAE advertises itself as a data hub, certain regulations – especially for health and public sector data – act as localization mandates. Furthermore, the UAE has mandated strict data localization 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 January 2, 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-localization 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 October 2026, so some operational details remain unsettled.[159]

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.[160] 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.[161]

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 **US** healthcare, insurance, pharmaceutical, medical-device, and cloud-service providers to use globally distributed infrastructure and cross-border support models.[162]

Abu Dhabi Mandatory Multi-Cloud and On-Site Backup Requirements (2026): Abu Dhabi Department of Health Circular No. 191/2026, effective January 1, 2027, requires covered healthcare providers, payers, and service providers to adopt multi-cloud strategies and maintain on-site physical backups. It also prohibits exclusive reliance on a single cloud provider for critical healthcare systems. These prescriptive requirements may impose substantial compliance costs, restrict architectural flexibility, and disadvantage US cloud and healthcare technology providers, even where alternative configurations offer equivalent or superior security and resilience. The Circular also creates uncertainty regarding the continued use of geographically distributed disaster recovery and cross-border support services. The UAE should permit equivalent, risk-based architectures, clarify permissible cross-border operations, and provide adequate implementation time.[163]

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.[164]

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 localization requirements, although they do not amount to a blanket prohibition on foreign cloud services or all cross-border processing.[165]

Internet of Things: The UAE's current IoT framework imposes local licensing and registration requirements, but it should not be characterized as a general IoT data-localization 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 authorized 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.[166]

J. Vietnam

As of October 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 localization 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 United States – making it more difficult for US enterprises and US workers to export digitally-enabled services and goods to Vietnam.

Over the past several years, Vietnam has enacted, implemented, and proposed various measures that raise serious 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 US businesses and workers, Vietnam has:

1. Made no public effort to remove these cross-border data restrictions or data localization mandates;
2. Introduced wholly new restrictions and mandates that hurt US interests – e.g., Decree 102 and the Data Security Law – that did not exist in January 2025.

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.[167]

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 July 1, 2026, and Decree No. 333/2026/ND-CP of August 19, 2026, described at Example 1.1(d) above; the discussion below should be read together with that description.[168]

The Cybersecurity Law and its subsequent implement decrees raise concerns and will likely significantly impact the ability of many companies 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.

Decree 53: 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 72: 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.

Decree 147: Under Decree 147/2024/ND-CP (Decree 147), effective December 2024, these localization 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, localize personal data, verify user IDs via local credentials, and respond to takedown and data requests from Vietnamese authorities. These data localization 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 were initially set out in its PDP Decree (i.e., Decree 13/2023/ND-CP), which took effect in 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 January 1, 2026.

Decree 356: Decree No. 356/2025/ND-CP, issued on December 31, 2025 and effective January 1, 2026, provides detailed guidance for implementation of the PDP Law and has replaced the PDP Decree.[169] The Decree imposes restrictive data transfer requirements on the industries and businesses subject to it, and in several respects it tightens them. The Decree also review of cross-border transfer impact assessment (CTIA) dossiers from an *ex post* to an *ex ante* mechanism, under which the MPS Department of Cybersecurity and High-Tech Crime Prevention (A05): (a) reviews and approves each dossier; (b) gives A05 15 days to evaluate the dossier and the enterprise 30 days to supplement a deficient dossier, failing which administrative sanctions may be imposed; (c) expands the required contents to include internal personal data protection policies, procedures, and templates; (d) requires separate descriptions of controller and processor roles and a data-flow diagram for each; and (e) requires dossiers to be updated every six months in specified circumstances and within 10 days of specified organizational changes.

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 meeting; (c) Publishing personal data in cyberspace that is received by persons outside Vietnam; (d) 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 July 1, 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.

- 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.

- Incorporates certain provisions of the Data Law by reference, such as those relating to cross-border data transfers and risk assessments. 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.

Draft Data Security Law (2026): MPS published a draft Data Security Law in August 2026, following a policy dossier circulated earlier in the year. As drafted, the law would: (1) establish a four-level data classification mechanism built on broad definitions of "Core Data" and "Important Data"; (2) apply an automatic classification uplift based on aggregation alone; (3) impose classification, risk-assessment and transfer obligations on processors as well as controllers, including in respect of matters outside a processor's actual control; (4) retain private-sector localization requirements; and (5) require annual transfer impact filings rather than a single durable assessment.[170]

Decree 330/2026 — Penalties: On August 19, 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 percent of the preceding year's revenue, together with remedies that can include suspension of transfer activity. It also penalizes 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 US organizations will rationally answer by localizing.

We recommend: (1) deleting the sectoral lists in Articles 6.4, 16.2, 24.1, and 28.1; (2) replacing the "supreme control" requirement with clearly defined access, audit, and cooperation arrangements; (3) permitting regulator access to data through less trade-restrictive means; and (4) recognizing internationally accepted standards and certifications – such as ISO/IEC 27001 and SOC 2 and, for payment data, PCI DSS – together with the EU standard contractual clauses, the ASEAN Model Contractual Clauses, and the Global CBPR System, as valid bases for security and for transfer without further approvals.

AI in Banking – Decision 33/2026 and Circular 53/2026: Two 2026 instruments impose requirements on AI systems used in banking in ways that could limit Vietnamese financial institutions' access to US technologies. Decision No. 33/2026/QD-TTg of the Prime Minister (June 30, 2026; effective August 15, 2026), issued under the Law on Artificial Intelligence, includes in its sectoral list of high-risk AI systems those that autonomously conduct electronic banking transactions or make credit approval decisions. Law firm analysis reports that high-risk systems are subject to mandatory conformity assessment before deployment, local presence requirements for foreign providers, and strict liability for damages even where the provider is fully compliant, with compliance deadlines of March 1, 2027 for most systems and September 1, 2027 for finance systems already in operation before August 15, 2026.[171] The State Bank of Vietnam's Circular No. 53/2026/TT-NHNN (September 30, 2026) separately prescribes safety, risk-management, and deployment conditions for AI in the banking sector, including a requirement that the total value of transactions an AI system automatically executes for a customer not exceed VND 100 million per day for individual customers or VND 500 million per day for institutional customers (or the institution's lower internal limit, if any), together with a signed customer authorization, human-intervention capability, and model testing and monitoring requirements.[172]

Domestic Card Switching (Circular 18/2024/TT-NHNN): Article 22(2) of State Bank of Vietnam Circular 18/2024/TT-NHNN, effective July 1, 2024, provides that switching of domestic card transactions on cards bearing international-brand bank identification numbers must be conducted through a gateway operated by a card switching organization licensed by the State Bank.[173] This is a network-localization requirement: it mandates domestic routing of domestic transactions irrespective of the network the issuer and acquirer would otherwise select, and it limits the ability of US-based networks to provide authorization, fraud-detection, and tokenization services on those transactions. We recommend that Vietnam eliminate the requirement or, at a minimum, permit issuers and acquirers to route domestic transactions through any network that satisfies objective security and performance standards.

Cloud Services under the Telecommunications Framework: Vietnam's revised Telecommunications Law and implementing Decree No. 163/2024/ND-CP removed foreign ownership limits for data center and cloud services and established a notification or registration approach. However, the framework requires data center and cloud services supplied to state agencies to store data in Vietnam. This creates a distinct localization barrier alongside the requirements imposed under cybersecurity and data legislation. For foreign SaaS providers, the cumulative effect can be a requirement to replicate infrastructure locally or forgo government customers. USTR should encourage Vietnam to narrow localization requirements to clearly defined sensitive workloads, clarify the treatment of Internet-based enterprise services, and ensure that overlapping telecommunications, cybersecurity, and data rules do not impose duplicative obligations.

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.

Other Economies of Interest

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

A. Azerbaijan

Azerbaijan's central bank regulates how payment system operators located outside the country may exchange information about transactions conducted within Azerbaijan. Article 3.18 of the Central Bank of the Republic of Azerbaijan's Regulation on Maintaining Payment Operations and on Payment Instruments (Decision No. 12/3, approved March 13, 2024, as amended) provides that providers and payment system operators operating outside the country may directly exchange data about transactions conducted within the country only where such transactions cannot be conducted without such an exchange, and it excludes from that permission domestic transactions in which payment for goods, works, or services is made through electronic commerce.[174] Read together with the Regulation's provisions on the domestic transmission, processing, and clearing of payment data, the provision channels domestic e-commerce transactions through domestic infrastructure. Members report that, because the domestic switch does not support globally interoperable tokenization standards, the practical effect is that domestic e-commerce transactions cannot be tokenized and authorized through global payment networks, which limits the availability of secure tokenized credentials, digital wallets, and checkout services for Azerbaijani cardholders and merchants.

B. Bangladesh

Bangladesh Bank's draft Payment System Operator (PSO) Regulation, published in November 2025, would require international card schemes to incorporate locally and to obtain a Bangladesh Bank licence. Mandatory local incorporation and licensing of a cross-border network that supplies services into Bangladesh, coupled with any requirement to process or store cardholder and transaction data in-country, would raise costs, fragment fraud-prevention and security architectures that depend on global data flows, and limit the availability of cross-border payment services to Bangladeshi consumers and businesses. We recommend that USTR encourage Bangladesh Bank to exempt international card schemes from local incorporation and licensing requirements; to permit cross-border processing and data flows without localization; to keep any regulatory data requests targeted and proportionate; and to avoid notification requirements that could delay security and fraud-prevention services.

C. Bolivia

Bolivia has moved toward strict data localization 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.[175] 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 **localization** 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[176] — 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.

D. Canada

Canada has historically applied an accountability-based approach, under which an organization 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 organization to conduct an impact assessment before transferring or disclosing personal information outside Canada.[177] 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, recognize 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.[178]

E. Chile

Chilean financial regulations impose several local data-related obligations.[179] 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 processing and cloud services performed outside Chile.[180] 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.[181]

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.[182] 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.[183] Please see here for Chile's ranking in the GDA Cross-Border Data Policy Index.

F. Kazakhstan

Kazakhstan maintains a broad requirement that personal data be stored domestically. Article 12 of the Law on Personal Data and Its Protection (Law No. 94-V of May 21, 2013) requires personal data to be stored in the country – in the words of the American Chamber of Commerce in Kazakhstan, "data storage shall take place on the territory of the Republic" – and the rule has survived several revisions; Order No. 395 of October 21, 2020 on the rules for collecting and processing personal data has at times strengthened it.[184] The requirement complicates the use of global cloud services, because cloud and AI providers generally rely on regional clusters of infrastructure rather than data centers in each national market. Recent legislation has widened the reach of localization. The Digital Code (Law No. 255-VIII of January 9, 2026) requires owners of "digital resources" to comply with the personal data rules, including the Law on Personal Data, and Articles 30 and 31 add restrictions on the cross-border transfer of "digital data products," including data-processing outcomes. Amendment Law No. 256-VIII of the same date repealed Article 36 of the Law on Informatization but extended personal data requirements, including localization, to a wider set of "digital objects," and the Law on Informatization separately requires localization for state, quasi-state, and critically important information and communications infrastructure. The Law on Artificial Intelligence (Law No. 230-VIII of November 17, 2025) likewise requires adherence to personal data protection rules.

Kazakhstan is also considering a draft decree on comprehensive measures for the development of data processing and storage infrastructure and ecosystem, which, according to the American Chamber of Commerce in Kazakhstan, would lift mandatory domestic storage of digital databases and allow the cross-border transfer of most categories

of personal data subject to conditions such as adequacy, binding corporate rules, standard contractual clauses, or recognized certification, with special categories permitted in the cloud if a Kazakhstan-based entity retains control of the encryption keys. The draft decree would also adopt a "Cloud First" principle for government data and ease security, compliance, and operating requirements for foreign-owned participants in the Data Center Valley, but only where they do not serve users in Kazakhstan. A separate draft Online Platforms Bill would require foreign companies to open local representative offices. We urge USTR to press Kazakhstan to remove the domestic-storage requirement in Article 12 and, at a minimum, to adopt the draft decree's transfer-based approach on terms that apply to all companies serving users in Kazakhstan rather than only to Data Center Valley participants; to separate the limited categories of sensitive data that must remain in Kazakhstan from data that may be stored and processed abroad; to recognize globally recognized security standards and certifications; and to ensure that implementation of the Digital Code and the Law on Artificial Intelligence does not extend localization to additional datasets and processing outcomes.

Finally, in June 2025, Kazakhstan's government published a consultative regulatory policy document, proposing to require foreign online platforms to formally register a local representative office in the country. The Draft Law on Online Platforms and Mass Media was submitted to Parliament in June 2026. The draft law would require foreign online platforms to register a legal entity, branch, or representative office in Kazakhstan.[185]

G. Japan

Japan's Information System Security Management and Assessment Program (ISMAP) creates significant compliance costs for foreign cloud and software-as-a-service providers seeking to supply government customers. Limited recognition of existing international certifications and audit evidence requires providers to repeat assurance activities already undertaken for other markets. Although Japan has pursued reforms to reduce the burden, recognition of equivalent evidence remains an important unresolved issue. USTR should encourage Japan to accept relevant evidence from internationally recognized assurance frameworks, including ISO/IEC 27001 and SOC 2, streamline assessment and renewal procedures, and implement proportionate requirements for lower-risk SaaS offerings.

Industry has also identified discussions concerning domestic ownership, Japanese-citizen operations, and Japan-based infrastructure for sovereign cloud services. These possible requirements warrant monitoring as policy design develops.[186] USTR should encourage transparent consultation and seek assurances that eligibility will be based on demonstrable security and resilience rather than supplier nationality or ownership, and that any localization requirements will be narrowly tailored to clearly identified risks.

H. Kenya

Kenya has introduced several measures that require data localization. Under the Computer Misuse and Cybercrimes Act[187] 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).[188] 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."[189]

Separately, the Data Protection Act (2019)[190] 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[191] 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 April 7, 2025 and took effect on gazettement on May 2, 2025, as the Kenya Cloud Policy, 2025.[192] 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.[193]

In April 2026 the Office of the Data Protection Commissioner published for consultation a Draft Guidance Note on Cross-Border Data Transfers, recognizing multiple transfer bases including adequacy, safeguards, binding corporate rules, contractual safeguards, derogations and consent.[194] 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 recognize accountability tools including ISO/IEC 27701 and the Global CBPR System.[195]

On September 8, 2026, the ODPC published the final Guidance Notes for Cross-border Data Transfers.[196] The final text addresses several of these points but leaves the core concerns intact. On the positive side, the Guidance expressly recognizes that a compelling legitimate interest may support a transfer where an organization "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 organizations 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 **localization** 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 recognized 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.[197]

I. Malaysia

Malaysia's developing sovereign AI approach raises questions about future conditions for supplying government cloud and AI services. Industry has identified proposals involving government-owned compute infrastructure for the most sensitive workloads and additional sovereignty certification requirements. Depending on their final design, these measures could require separate domestic infrastructure and create additional barriers for foreign suppliers. USTR should encourage transparent consultation, proportionate data classification, recognition of internationally accepted security assurance, and procurement criteria that permit domestic and foreign providers to compete on the basis of security and performance.

J. Mexico

Mexico historically allowed free data flows, but a recent fintech regulation creates a de facto **localization** 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 **localization** based on purported disaster recovery concerns.[198] 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.[199] 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 international cloud solutions face extra hurdles in Mexico. In practice, a fintech using a foreign service provider must nevertheless **localize** 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.[200] 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.[201] 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.[202]

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.[203]

K. 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 August 25, 2025, urging removal of the local shareholding and ownership requirements and of the associated data localization and residency requirements. This measure warrants particular attention 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 US provider can qualify at Level 2 by improving either.

L. Nepal

Nepal Rastra Bank (NRB) has proposed a National Payment Switch (NPS) through which payment transactions would be centrally routed. NRB's master reference document on the NPS and the national payment ecosystem (October 2025) provides that all card-related transactions acquired by Nepali merchants shall be routed through the NPS National Card Switch (NPS-NCS), which would also include a centralized system for back-office, fraud, and risk management.[204] In the first phase, transactions on international card networks would continue to be routed under the existing arrangements between the card schemes and Nepali banks and financial institutions; in the second phase, "international routing of all card-related transactions shall be handled through NPS-NCS." The document is not entirely clear on how the second-phase routing would apply to cards issued abroad and used at Nepali merchants, does not address data localization or residency expressly, and leaves detailed procedures to separate specifications and operating rules to be issued by NRB. A requirement that all card transactions – domestic and, in the second phase, international – be routed through a single state-designated switch is a network-localization measure: it would displace cross-border routing and the fraud and risk analytics that depend on it, reduce competition among networks, and concentrate operational risk. We urge USTR to encourage NRB to preserve

issuers' and acquirers' choice of routing; to ensure that international networks may continue to authorize, route, and settle cross-border transactions; and to develop the operating rules through public consultation.

M. Nigeria

Nigeria has embraced data localization 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 localization.[205]

Nigeria's draft National Cloud Policy 2025[206] 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.[207]

That draft has since been superseded. On August 17, 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 localization 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 **localization** 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.

Central Bank of Nigeria Circular on Payments Data (June 2026): Although the National Digital Cloud Policy declines to impose general localization requirements on commercial data, a sectoral measure points in the opposite direction. On June 15, 2026, the Central Bank of Nigeria (CBN) issued Circular PSS/DIR/PUB/CIR/001/004 on market structure, data localization, ultimate beneficial ownership disclosure, and systemic oversight in the payments sector. Clause 2 requires all financial institutions and participants facilitating payments within Nigeria to ensure that "payments transaction data generated within Nigeria are stored and managed in Nigeria," in accordance with applicable Nigerian data protection laws, and requires full compliance effective January 1, 2027.[208] The Circular is addressed to deposit money banks, microfinance banks, mobile money operators, switching and processing companies, payment terminal service providers, payment solution service providers, super agents, and other licensed operators, and on its face contains no exception for cross-border processing. The terms "stored" and "managed," and the scope of "payments transaction data," are not defined. Read broadly, the requirement could oblige payment networks, processors, and the cloud and technology providers that support them to maintain duplicative in-country systems and to restructure the data flows on which fraud monitoring, cybersecurity, anti-money-laundering and sanctions screening, authorization, dispute resolution, analytics, and operational resilience depend, and it could favor domestic providers. We urge USTR to encourage the CBN to clarify the scope of the requirement before the January 1, 2027 compliance date and to adopt a targeted approach that preserves the CBN's supervisory access to payment data while permitting secure, risk-based cross-border processing.

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.[209]

N. 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.[210] 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.[211] 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 **localization** requirements for covered government workloads, while the policy separately contemplates consultation with the Cloud Office for legitimate cross-border data-flow use cases.[212]

Third, in the financial sector, the State Bank of Pakistan (SBP) regulates offshore cloud outsourcing by covered financial institutions.[213] 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.

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.[214]

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.[215]

O. Philippines

Local industry stakeholders and some government agencies have advocated vigorously for **localization** mandates in recent years.[216] We **summarize** 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 **localization** 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 **Localization** 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 **localization** 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.

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. A final Executive Order on the same subject, Executive Order No. 119, was issued in July 2026 and is described below. The difficulty that remains is that the October 2025 Policy and Executive Order No. 119 point in different directions, and we are not aware of any instrument that definitively supersedes the October 2025 Policy.

Executive Order No. 119 (2026): Executive Order No. 119, "Updating the Government Data Classification, Establishing a Data Residency Framework, and for Other Purposes," was issued on July 13, 2026 and took effect on July 15, 2026.[217] The Order divides government data into Restricted Access Data (Top Secret, Secret, Confidential, and Restricted) and Open Access Data (Unclassified or Open). Under Section 7, Top Secret data must be stored within Philippine territory or other territory under Philippine sovereignty or jurisdiction, such as embassies and consulates; Confidential data must as a general rule be stored and maintained within Philippine territory, and may be stored or processed abroad only with the express prior approval of the Joint Oversight Committee for Data Classification (JOC-DC) and safeguards that maintain governmental control; Restricted data may be stored on a secured cloud computing platform subject to encryption, risk-mitigation, and cybersecurity requirements; and all other government data, including open access data, may be stored on secure cloud computing platforms regardless of physical location or ownership. The Order does not apply to the private sector or to commercial data owned by private entities, but it does apply to government data processed or stored by private entities for an agency, including entities in public-private partnerships, public utilities, and critical infrastructure and other strategic or sensitive projects, as the implementing guidelines will define. The JOC-DC must issue implementing guidelines within 120 days of effectivity, and covered agencies must achieve full compliance in phases over three years. EO 119 is considerably narrower than the October 2025 DICT Policy, because it ties residency to classification tier rather than to all government data and it permits cloud storage regardless of location for lower tiers. We nevertheless recommend that USTR monitor the implementing guidelines, which will determine how broadly agencies classify data at the Confidential level and above; whether the offshore-approval pathway for Confidential data is administered transparently and promptly; how far the Order reaches private service providers; and whether the Order displaces the October 2025 Policy, including its "sovereign cloud" accreditation process limited to local cloud service providers. We encourage risk-based, narrowly tailored implementation that permits cross-border processing of lower-risk government data.

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.

P. Singapore

Suppliers report that serving certain air-gapped public-sector environments requires cloud applications to be deployed within government data centers. These deployment conditions can prevent access to globally delivered SaaS and cloud-based security services where a separate local instance is unavailable. Singapore's Multi-Tier Cloud Security standard, SS 584, also introduces requirements beyond ISO/IEC 27001, creating additional certification work for providers already assessed against international standards.

Q. 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.[218] 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 **USTR** to monitor and oppose any expansion of these data sovereignty provisions.[219] 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 March 6, 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 organizations, pension funds, employers, administrative bodies and institutions acting on their behalf. For US 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.[220]

R. Taiwan

Taiwan maintains a surprisingly large number of data **localization mandates. We summarize** these below.

Financial Sector Data Residency Rules: Taiwan's financial regulators impose explicit data **localization** 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 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.[221]

Healthcare Data Localization: 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.[222]

Data for Localization 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 localized within Taiwan.[223] 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 localization 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.

S. 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 August 14, 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 recognize 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 localization requirement inside an AI statute rather than a data protection or cybersecurity statute, and because localization of this kind would cut critical infrastructure operators off from precisely the cross-border threat intelligence and telemetry on which their security depends.

T. Uzbekistan

Uzbekistan is establishing a state-controlled national payment switch through which payment transactions in the national currency would have to be routed. A presidential decree signed on November 27, 2025, as part of a broader fintech development package, provides for a national payment switch operated by the Central Bank under its "full control" and described in press reports as "the mandatory gateway for all transactions in national currency," through which local and international payment system operators must route every soum-denominated transaction; regulatory acts requiring all payment operators, including e-money companies, to connect exclusively to the switch were scheduled for March 2026.[224] Press reports in July 2026 indicate that the launch of the switch is now planned for 2027.[225] The published reports do not state what principles will govern the fees the switch operator may charge. A requirement that every domestic-currency transaction pass through a single state-controlled switch is a network-localization measure that would confine international networks to cross-border volume, remove competition in the routing and pricing of domestic transactions, and create a single point of operational failure.

---

[1] The Global Data Alliance (globaldataalliance.org) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others. The Business Software Alliance administers the Global Data Alliance.

[2] USTR, Request for Comments on Significant Foreign Trade Barriers for the 2027 National Trade Estimate Report, 91 Fed. Reg. 58247 (Sept. 14, 2026), Docket No. USTR-2026-0498, https://www.federalregister.gov/d/2026-18775.

[3] Global Data Alliance, Submission of Global Data Alliance for National Trade Estimate on Foreign Trade Barriers (Oct. 30, 2025) (Docket No. USTR-2025-0016), https://globaldataalliance.org/wp-content/uploads/2025/10/10302025gdante.pdf.

[4] USTR, 2025 Trade Policy Agenda (Mar. 2025), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2025/march/us-trade-representative-announces-2025-trade-policy-agenda; see also USTR, 2026 Trade Policy Agenda and 2025 Annual Report (Mar. 2, 2026), https://ustr.gov/sites/default/files/files/Press/Releases/2026/2026%20Trade%20Policy%20Agenda%202025%20Annual%20Report.pdf.

[5] Global Data Alliance, GDA Cross-Border Data Policy Index (2023), https://globaldataalliance.org/resource/cross-border-data-policy-index/

[6] AmCham EU, The Transatlantic Economy 2026, ch. 2 (Digital Commerce and Connectivity), at 47–48 (Mar. 2026) (citing US Bureau of Economic Analysis data), https://transatlantic.amchameu.eu/wp-content/uploads/2026/03/Transatlantic_Economy_2026_Chapter_2_Digital-Commerce-and-Connectivity.pdf. US digitally deliverable services exports totaled $729.6 billion in 2024, against imports of $447.6 billion (a surplus of approximately $282 billion). Exports to Europe totaled $361 billion (49.5 percent of the total). Exports to the EU totaled approximately $225 billion – 76 percent of the approximately $295 billion in total US services exports to the EU – and produced a digitally deliverable services surplus with the EU of approximately $124 billion.

[7] 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.

[8]WTO, "WTO and OECD release expanded dataset on trade in services covering over 200 economies" (February 17, 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.

[9] Trade Act of 1974 § 181, 19 U.S.C. § 2241(a)(1); see also 91 Fed. Reg. 58247 (Sept. 14, 2026), https://www.federalregister.gov/d/2026-18775.

[10] 91 Fed. Reg. 58247, 58248–49 (Sept. 14, 2026) (Part III, Estimate of Increase in Exports), https://www.federalregister.gov/d/2026-18775.

[11] AmCham EU, The Transatlantic Economy 2026, ch. 2 (Digital Commerce and Connectivity), at 47–48 (Mar. 2026) (citing US Bureau of Economic Analysis data), https://transatlantic.amchameu.eu/wp-content/uploads/2026/03/Transatlantic_Economy_2026_Chapter_2_Digital-Commerce-and-Connectivity.pdf. In 2024, US digitally deliverable services exports to Europe totaled $361 billion (49.5 percent of the US total), and exports to the EU totaled approximately $225 billion.

[12] Kenneth Propp, The EU Cloud and AI Development Act, Lawfare (June 24, 2026), https://www.lawfaremedia.org/article/the-eu-cloud-and-ai-development-act (reporting the Commission's estimate that approximately 70 percent of public-sector data contracts would fall at Level 1, 20 percent at Level 2, fewer than 10 percent at Level 3, and about 1 percent at Level 4); see also Jones Day, European Commission's Proposed Cloud Sovereignty Framework Creates New Compliance Tiers for Software Providers (June 2026), https://www.jonesday.com/en/insights/2026/06/european-commissions-proposed-cloud-sovereignty-framework-creates-new-compliance-tiers-for-software-providers (reporting the Commission's estimate that only 1 percent of public services require Level 4). See European Commission, Proposal for a Regulation on the Cloud and AI Development Act, COM(2026) 502 (June 3, 2026), procedure 2026/0138(COD), https://www.eerstekamer.nl/nonav/bijlage/20260609/com_2026_502_proposal_for_a/document3/f=/vmy8optarooc.pdf.

[13] Oxford Economics for the AI Adoption Initiative, The Economics of Sovereign AI: Balancing Autonomy, Innovation, and Growth in the Asia-Pacific (May 2026), Figures 3, 24 and 25.

[14]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.

[15] PRC Cybersecurity Law (effective June 1, 2017); Data Security Law (adopted June 10, 2021, effective September 1, 2021); Personal Information Protection Law (effective November 1, 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 September 1, 2022); CAC, Regulations on Promoting and Standardising Cross-Border Data Transfers (March 22, 2024). On the sub-national "negative lists", see Annex II (China), describing the Tianjin Free Trade Zone list of 46 data subclasses (May 17, 2024) and the Beijing Pilot Free Trade Zone list of 23 business scenarios and 198 data elements across five industries (August 30, 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

[16] 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

[17] 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 November 13, 2025). See Annex II (India) for the full inventory.

[18] Vietnam, Law on Cybersecurity (2025), effective July 1, 2026; Decree No. 333/2026/ND-CP (August 19, 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.

[19]See, e.g., Bank Secrecy Act, 31 U.S.C. §§ 5311–5336, and 31 C.F.R. ch. X (anti-money laundering programs and suspicious activity reporting); International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1707, and 31 C.F.R. ch. V (sanctions compliance); Export Administration Regulations, 15 C.F.R. pts. 730–774; Securities Exchange Act of 1934 § 13(b)(2), 15 U.S.C. § 78m(b)(2) (books, records, and internal controls, extending to consolidated foreign subsidiaries), and Sarbanes-Oxley Act § 404, 15 U.S.C. § 7262 (internal control over financial reporting); Consumer Product Safety Act § 15(b), 15 U.S.C. § 2064(b), and 49 U.S.C. §§ 30118–30120 and 49 C.F.R. pt. 579 (defect, early-warning, and recall reporting); and Tariff Act of 1930 § 307, 19 U.S.C. § 1307, and the Uyghur Forced Labor Prevention Act, Pub. L. No. 117-78 (supply-chain tracing for import compliance). Each of these obligations is imposed on the US parent, issuer, or importer, and each presupposes that it can obtain data from operations located outside the United States. The European Union imposes comparable group-level duties, for example under Directive (EU) 2024/1760 (Corporate Sustainability Due Diligence Directive) and Regulation (EU) 2022/2554 (DORA).

[20] 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.

[21] The White House, Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae-myung (Nov. 13, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/.

[22] OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD/LEGAL/0487 (adopted December 14, 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 to which the United States, the European Union, and other major trading partners have all subscribed.

[23] We recognize that some commentators 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 individualized targeting decisions, subject to annual certification and to judicial approval of targeting and minimization procedures, and is overseen by the Foreign Intelligence Surveillance Court, the Privacy and Civil Liberties Oversight Board, and the Congress. The United States is also an adherent to the OECD Declaration, as are the European Union and its Member States.

[24] These controls are already expressed in internationally recognized, 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: compliance can be verified by an accredited third party, and the same requirement can be applied to domestic and foreign providers on identical terms.

[25]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 (October 30, 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.

[26] European Commission, Proposal for a Regulation on the Cloud and AI Development Act, COM(2026) 502 (June 3, 2026), procedure 2026/0138(COD), https://www.eerstekamer.nl/nonav/bijlage/20260609/com_2026_502_proposal_for_a/document3/f=/vmy8optarooc.pdf. Articles 16, 18, 30–32 and Annexes II–III; Global Data Alliance, Position Paper: Cloud & AI Development Act – Preserving Cross-Border Digital Access Across All EU Sectors (Sept. 9, 2026), https://globaldataalliance.org/wp-content/uploads/2026/09/09092026gdacadacmts.pdf. The Commission's distribution estimate is reported in Kenneth Propp, The EU Cloud and AI Development Act, Lawfare (June 24, 2026), https://www.lawfaremedia.org/article/the-eu-cloud-and-ai-development-act.

[27] European Commission, Proposal for an Industrial Accelerator Act (Mar. 4, 2026); see Clifford Chance, The EU Industrial Accelerator Act: Made in Europe? (Mar. 6, 2026), https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2026/03/eu-industrial-accelerator-act-briefing.pdf; Sarah Beard et al., The European Union's "Made in Europe" Push, Holland & Knight Alert (May 22, 2026), https://www.hklaw.com/en/insights/publications/2026/05/the-european-unions-made-in-europe-push; European Parliamentary Research Service, EPRS_BRI(2026)791495 (Sept. 2026), https://eprs.europarl.europa.eu/contents/publications/EPRS/2026/09/EPRS_BRI(2026)791495.html.

[28] European Commission, Commission proposes simpler and more strategic Public Procurement rules, Press Release IP/26/1817 (Sept. 9, 2026), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_1817/IP_26_1817_EN.pdf.

[29] European Commission, Proposal for a Regulation revising the Cybersecurity Act, COM(2026) 11 final (Jan. 20, 2026); see Jens Neitzel, Piotr Rataj & Michael Biendl, The CSA2 – Digital Sovereignty or Protectionism?, CMS (Apr. 1, 2026), https://cms.law/en/deu/legal-updates/the-csa2-digital-sovereignty-or-protectionism.

[30] Orrick, Data Localization and the Sovereign Cloud: EU Cloud Regulations Explained (Jan. 20, 2026), https://www.orrick.com/en/Insights/2026/01/Data-Localization-and-the-Sovereign-Cloud-EU-Cloud-Regulations-Explained (describing SecNumCloud's requirements, including immunity from third-country public authority requests and EU-based registered office and administration, and noting that non-European providers may serve clients through joint ventures with local companies); the reported 61 percent EU-ownership threshold is described, in its summary of the France entry of the 2026 NTE Report, in Michael

Geist, The Global Battle for Data Control: How the 2026 U.S. Report on Trade Barriers Targets Data Sovereignty Worldwide (Apr. 14, 2026), https://www.michaelgeist.ca/2026/04/the-global-battle-for-data-control-how-the-2026-u-s-report-on-trade-barriers-targets-data-sovereignty-worldwide/.

[31] Business Software Alliance & Global Data Alliance, Recommendations for Implementation of the Digital Trade Commitments in the Joint Statement on a US-EU Joint Framework on Trade (Mar. 18, 2026), https://globaldataalliance.org/wp-content/uploads/2026/03/03182026bsagdauseujointfrmwktrade.pdf.

[32]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 (October 30, 2025). The principal instruments are: India - RBI, Storage of Payment System Data, DPSS.CO.OD No. 2785/06.08.005/2017-2018 (April 6, 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, March 15, 2020), and the CBRT Communiqué on Information Systems of Payment and Electronic Money Institutions, art. 21 (Official Gazette No. 31676, December 1, 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.

[33] 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 July 1, 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.

[34] Three further measures should be recorded in this category. South Africa's Health Information Regulations under the Protection of Personal Information Act, in force since March 6, 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 organizations, 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. In the European Union, the European Health Data Space Regulation (Regulation (EU) 2025/327) allows Member States to require that primary-use electronic health data be stored in the Union (Article 86), requires secondary-use processing operations to be carried out in the Union absent an adequacy decision (Article 87), deems certain non-personal electronic health data "highly sensitive" for purposes of transfer to third countries (Article 88), and obliges data users and access bodies to take measures to prevent governmental access to, and transfer of, non-personal electronic health data held in the Union (Article 89). Regulation (EU) 2025/327 (European Health Data Space Regulation), arts. 86–89, https://eur-lex.europa.eu/eli/reg/2025/327/oj; see Global Data Alliance, White Paper on Data Transfer Provisions of the EU Proposal for a European Health Data Space (2022), https://globaldataalliance.org/wp-content/uploads/2022/08/07282022gdaeuhealthdataspace.pdf.

[35] The US exercise is conducted under Section 181 of the Trade Act of 1974, 19 U.S.C. § 2241, and proceeds by annual public solicitation of stakeholder evidence. See USTR, Request for Comments on Significant Foreign Trade Barriers for the 2027 National Trade Estimate Report, 91 Fed. Reg. 58247 (Sept. 14, 2026), https://www.federalregister.gov/d/2026-18775. For an illustration of the resulting evidentiary record on cross-border data measures specifically, see Global Data Alliance, Submission of Global Data Alliance for National Trade Estimate on Foreign Trade Barriers (Oct. 30, 2025) (Docket No. USTR-2025-0016), https://globaldataalliance.org/wp-content/uploads/2025/10/10302025gdante.pdf.

[36] Business Software Alliance & Global Data Alliance, Recommendations for Implementation of the Digital Trade Commitments in the Joint Statement on a US-EU Joint Framework on Trade (Mar. 18, 2026), https://globaldataalliance.org/wp-content/uploads/2026/03/03182026bsagdauseujointfrmwktrade.pdf (proposing continuity of service, impermissible and permissible technology promotion, and notification and consultation provisions).

[37] Global Data Alliance, Cross-Border Data Transfers & Data Localization Measures (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/02112020GDAcrossborderdata.pdf

[38] Global Data Alliance, GDA Website – Finance (2022), https://globaldataalliance.org/sectors/finance/

[39] Global Data Alliance, Cross-Border Data Transfers & Economic Development: Access to Global Markets, Innovation, Finance, Food, and Healthcare (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/05062021econdevelopments1.pdf

[40] Global Data Alliance, Cross-Border Data Transfer Facts and Figures (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf

[41] G20, Ministerial Statement on Trade and Digital Economy (2019), http://www.g20.utoronto.ca/2019/2019-g20-trade.html

[42] Global Data Alliance, Cross-Border Data Transfers & Innovation (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf

[43] Underlying sources for the data in Box 1 follow: OECD, SME Digitalisation to "Build Back Better", Digital for SMEs (D4SME) Policy Paper (2021), at: https://www.oecd-ilibrary.org/economics/sme-digitalisation-to-build-back-better_50193089-en; OECD, Enhancing SMEs' Resilience through Digitalisation (2021), at: https://www.oecd-ilibrary.org/economics/enhancing-smes-resilience-through-digitalisation_23bd7a26-en; US Census Bureau, Preliminary Profile of US Exporting Companies, 2022 (Nov. 4, 2021), at: https://www.census.gov/foreign-trade/Press-Release/edb/2019/2019prelimprofile.pdf; US Chamber of Commerce, Growing Small Business Exports (2021) at https://www.uschamber.com/assets/archived/images/ctec_googlereport_v7-digital-opt.pdf Other reports also bear out this critical opportunity for small businesses. See e.g., CSIS, Filling in the Indo-Pacific Economic Framework (2022) at: https://csis-website-prod.s3.amazonaws.com/s3fs-

public/publication/220126_Goodman_Indo_Pacific_Framework.pdf?eeGvHW0ue_Kn118U5mhopSjLs7DfJMaN ; ("In the Indo-Pacific region, SMEs account for 60–70 percent of employment but only 35 percent or less of direct exports, meaning there is ample room for growth.") citing: https://development.asia/explainer/how-can-asia-reignite-its-sme-growth-engine-through-trade ; https://www.apec.org/groups/som-steering-committee-on-economic-and-technical-cooperation/working-groups/small-and-medium-enterprises ; AlphaBeta, MicroRevolution: The New Stakeholders of Trade in APAC (2019), at: https://alphabeta.com/our-research/micro-revolution-the-new-stakeholders-of-trade-in-apac/; Federal Reserve Banks, Small Business Credit Survey: 2021 report on employer firms (2021), at: https://www.fedsmallbusiness.org/medialibrary/FedSmallBusiness/files/2021/2021-sbcs-employer-firms-report ; IDC, Small Business Digital Transformation: A Snapshot of Eight of the World's Leading Markets (2020) https://www.cisco.com/c/dam/en_us/solutions/small-business/resource-center/small-business-digital-transformation.pdf ; US International Trade Commission, Digital Trade in the US and Global Economies (Part II) (2014), at: https://www.usitc.gov/publications/332/pub4485.pdf A 2019 survey of US-based SMEs shows that 96% of eBay-enabled SMEs exported to an average of 16 different markets, whereas 0.9% (less than one percent) of other businesses exported to an average of 4 markets. Furthermore, eBay-enable SMEs across the United States averaged 16 different export markets. eBay, United States Small Online Business Report (May 2021), at: https://www.ebaymainstreet.com/sites/default/files/policy-papers/2021%20Small%20Online%20Business%20Report.pdf ; Center for Strategic and International Studies, What Do CPTPP Member Country Businesses Think about the CPTPP (2021), at: https://www.csis.org/analysis/what-do-cptpp-member-country-businesses-think-about-cptpp For SMEs engaged in online sales, the most important digital economy provisions were those that: (1) ensured that companies can move customer data across borders; (2) permitted companies to choose where to store their data; (3) prohibited digital customs duties; and (4) protected consumers from harmful practices, such as spam.

[44] Underlying sources for the data in Box 2 follow: Congressional Research Service, Digital Trade and US Trade Policy (2021) at: https://sgp.fas.org/crs/misc/R44565.pdf; GDA | The Software Alliance, Advancing a Jobs-Centric Digital Trade Policy (2021), at: https://www.bsa.org/files/policy-filings/11132021jobscentricdigitrade.pdf ; Software.org, Supporting US Through COVID (2021), at: https://software.org/wp-content/uploads/2021SoftwareJobs.pdf ; GDA | The Software Alliance, GDA Workforce Agenda (2019), at: https://www.bsa.org/policy-filings/innovation-competitiveness-opportunity-a-policy-agenda-to-build-tomorrows-workforce ; Software.org, Every Sector is a Software Sector – Manufacturing (2019), at https://software.org/wp-content/uploads/Every_Sector_Software_Manufacturing.pdf ; ransform Your Trade Website (2022) at: https://transformyourtrade.org/; International Trade Administration, COVID-19 Economic Recovery: An Important Moment Arrives for U.S. Exporters (May 2021), at: https://blog.trade.gov/2021/05/19/covid-19-economic-recovery-an-important-moment-arrives-for-u-s-exporters/

[45] As connectivity and data have become integrated into every aspect of our lives, data-related regulation has become common in many areas: data privacy, cybersecurity, intellectual property, online health services – to name a few. Globally, the number of data regulations grew by over 800% between 1995 and 2015, and exceeds 250 today. See OECD, Trade and Cross-Border Data Flows, OECD Trade Policy Papers (2019), at: https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1636811939&id=id&accname=guest&checksum=4D81CCF1C6E59168A9C5AE0E43F3F9FB

[46] See Global Data Alliance, Cross-Border Data Transfer – Facts and Figures (May 2020), at : https://globaldataalliance.org/downloads/gdafactsandfigures.pdf

[47] Micro-Revolution: The New Stakeholders of Trade in APAC, Alphabeta, 2019.

[48] See Global Data Alliance, Submission to The World Bank on Concept Note for the World Development Report 2021 – Data for Better Lives (June 16, 2020) at: https://www.globaldataalliance.org/downloads/061220GDAWorldDevReport2021Notes.pdf

[49] Oxford Economics for the AI Adoption Initiative, The Economics of Sovereign AI: Balancing Autonomy, Innovation, and Growth in the Asia-Pacific (May 2026), Figures 3, 24 and 25.

[50] Regulation (EU) 2016/679 (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[51] Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/

[52] Privacy Act 2020, https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[53] Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[54] OECD Privacy Framework (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[55] APEC Privacy Framework (2015), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[56] APEC Privacy Recognition for Processors (2021)

[57] APEC Cross Border Privacy Rules system, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

[58] Global Cross-Border Privacy Rules Forum (2022), https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[59] ASEAN Model Contractual Clauses (2021), at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf; See also, Singapore Personal Data Protection Commission, Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore (2022), at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en#:~:text=The%20ASEAN%20Model%20Contractual%20Clauses%20%28ASEAN%20MCCs%29 %20are,parties%20that%20protects%20the%20data%20of%20data%20subjects.

[60] See e.g., Ferracane et al., The Costs of Data Protectionism, VOX (2018); Ferracane et al., Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries? ECIPE Digital Trade Estimates Working Paper No. 1 (2019); Lund et al., Defending Digital Globalization, McKinsey Global Institute (2017).

[61] These commitments should be built on prior regional and bilateral agreements involving WTO members. These agreements include the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the Australia- Singapore Digital Economy Agreement (DEA), the Digital Economy Partnership Agreement (DEPA), the UK- Japan Economic Partnership Agreement, as well as the United States-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement, which contain the most advanced cross-border data provisions in any agreement.

[62] See e.g., UK-Singapore DEA Art. 8.61F(3); US-Japan DTA Art. 11.2; USMCA Art. 19.11.2.

[63] See e.g., UK-Singapore DEA Art. 8.61F(3)(a); US-Japan DTA Art. 11.2(a); USMCA Art. 19.11.2(a).
[64] See e.g., UK-Singapore DEA Art. 8.61F(3)(b); US-Japan DTA Art. 11.2(b); USMCA Art. 19.11.2(b).
[65] Cross-border and data localization provisions should apply to all services and financial services sectors with no exclusions, including for electronic payment services. See e.g., UK-Singapore DEA Art. 8.54.1; US-Japan DTA Art. 12-13; USMCA Chapter 17.
[66] See e.g., US-Japan DTA Art. 11, footnote 9; USMCA Art. 19.11, footnote 5.
[67] See e.g., UK-Singapore DEA Art. 8.61.E(6); US-Japan DTA Art. 15.3; USMCA Art. 19.8.4, 19.8.6.
[68] In the WTO context, these tenets – which trace back to the 1947 General Agreement on Tariffs and Trade – now apply to all multilateral trade rules, including those relating to goods, services, investment, technical regulations, and customs procedures. In the same spirit, WTO digital trade negotiators should explicitly extend these core tenets to trade rules relating to the cross-border movement of data.
[69] Bloomberg, WTO Talks End With No Deal to Extend E-Commerce Tariff Ban (Mar. 30, 2026), https://www.bloomberg.com/news/articles/2026-03-30/wto-talks-end-with-no-deal-to-extend-e-commerce-tariff-ban; Global Industry Statement on the WTO E-Commerce Moratorium and Work Programme (Sept. 14, 2026), https://globaldataalliance.org/wp-content/uploads/2026/09/09142026gdawtomora.pdf.
[70] GDA Cross-Border Data Policy Principles, https://globaldataalliance.org/wp-content/uploads/2021/07/03022021gdacrossborderdatapolicyprinciples.pdf
[71] *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
[72] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.
[73] *Ibid.*
[74] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[75] 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.
[76] 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.
[77] 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.

[78] 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.

[79] 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)
[80] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[81] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[82] *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.")

[83] *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

[84] 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.

[85] 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.

[86] 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.

[87] 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, the United States–Mexico–Canada Agreement (USMCA) (arts. 19.11–19.12), the US–Japan Digital Trade Agreement (arts. 11–12), and various other agreements negotiated by the United States, the European Union, and other partners. This positive trend should continue.

[88] 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.

[89] 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

[90] 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 June 19, 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.

[91] 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

[92] 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/

93Brazil, 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.

[94] 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

[95] 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

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

[97] 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

[98] 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

[99] AmCham EU, The Transatlantic Economy 2026, ch. 2 (Digital Commerce and Connectivity), at 47–48 (Mar. 2026) (citing US Bureau of Economic Analysis data), https://transatlantic.amchameu.eu/wp-content/uploads/2026/03/Transatlantic_Economy_2026_Chapter_2_Digital-Commerce-and-Connectivity.pdf. In 2024, US digitally deliverable services exports to Europe totaled $361 billion (49.5 percent of the US total), and exports to the EU totaled approximately $225 billion.
[100] Global Data Alliance, Submissions in the European Union (2020–2026), https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-eu&sector=&language=&posts_filtered=1; Global Data Alliance, GDA Cross-Border Data Policy Index (2023), https://globaldataalliance.org/resource/cross-border-data-policy-index/.
[101] *See generally*, GDA Cloud Scorecard – 2018 India Country Report, https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

[102] *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

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

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

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

[106] 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
[107] 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
[108] National Data Sharing and Accessibility Policy-2012 (NDSAP-2012), at https://dst.gov.in/sites/default/files/gazetteNotificationNDSAP.pdf
[109] Storage of Payment System Data Directive

[110] Storage of Payment System Data Directive

[111] Storage of Payment System Data Directive

[112] No. 20(3)/2022-CERT-In, MeitY, at https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[113] BSA concerns on the CERT-In Directions on Information Security Practices at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

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

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

[116] 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

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

[118] Report by the Committee of Experts on Non-Personal Data Governance Framework, August 2020, https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf
[119] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dec 2020, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf
[120] 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
121 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.
122 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.
123 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.

124 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 July 16, 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.
125 Bank Indonesia, Regulation No. 10 of 2025 on Payment System Industry Regulation, effective March 31, 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.
126 Agreement Between the Government of the United States of America and the Government of the Republic of Indonesia on Reciprocal Trade (signed Feb. 19, 2026), Annex III, art. 2.29. Under this framework, Indonesia committed to continue allowing international payment networks of US companies to process domestic credit card and e-commerce transactions across borders under the exemption provisions of its regulations; not to require financial data to be processed onshore, provided that regulators have immediate, direct, complete, and ongoing access to the data; and to allow internationally accepted chip standards for domestic card transactions, including contactless debit. Because the Agreement is pending entry into force, however, those commitments are not yet operative, and Bank Indonesia's approval pathway remains the governing rule. We recommend that USTR monitor whether Bank Indonesia codifies a standing exemption for offshore processing consistent with Article 2.29.
127 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 March 1, 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.
128 *See generally*, GDA Cloud Scorecard – 2018 Korea Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Korea.pdf
129 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
130 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.

131 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.
132 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
133 Korea clears exporting map data for Google, ends 19-year dispute, The Korea Herald (Feb. 27, 2026) (reporting the conditional approval of the export of 1:5,000-scale map data), https://www.koreaherald.com/article/10684189.
134 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.
135 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.
136 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.
137 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.
138 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.
139 Clyde & Co, SDAIA Publishes Draft Amendments to the Implementing Regulations of the PDPL (Oct. 8, 2026), https://www.clydeco.com/en/insights/2026/10/sdaia-publishes-draft-amendments-to-the-pdpl (consultation open Oct. 6 – Nov. 5, 2026; proposed arts. 23 and 34); Al Tamimi & Co., SDAIA Opens Public Consultation on Proposed Amendments to the PDPL Implementing Regulation (Oct. 2026), https://www.tamimi.com/news/sdaia-opens-public-consultation-on-proposed-amendments-to-the-pdpl-implementing-regulation/.
140 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).
141 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.

[142] Communications, Space and Technology Commission, Internet of Things (IoT) Regulations, Decision No. 556/1446 (July 31, 2024), para. 5-4, https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1602.
[143] 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.
[144] 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/.
[145] Regulation on Banks' Information Systems and Electronic Banking Services, Official Gazette No. 31069 (March 15, 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.
[146] 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 (December 1, 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.
[147] 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" (January 24, 2023), https://cms-lawnow.com/en/ealerts/2023/01/data-localisation-requirements-in-turkiye.
[148] Regulation on Internal Systems in the Insurance and Private Pension Sectors (November 25, 2021). See Moroğlu Arseven, "Turkey Announces the Regulation on Internal Systems in Insurance and Private Pension Sectors" (February 1, 2022), https://www.morogluarseven.com/news-and-publications/turkey-announces-the-regulation-on-internal-systems-in-insurance-and-private-pension-sectors/.
[149] Capital Markets Board, Communiqué on Procedures and Principles Regarding Information Systems Management (VII-128.10), Official Gazette No. 32840 (March 13, 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.
[150] https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim.
[151] Personal Data Protection Law No. 6698, art. 9, as amended by Law No. 7499 (effective June 1, 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.
[152] Information and Communication Technologies Authority (BTK), Decision No. 2019/DK-TED/053, February 12, 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.
[153] 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.
[154] 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).
[155] 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.
[156] Mondaq, Türkiye's Cybersecurity Board Determines Critical Infrastructure Sectors: A Major Step in the Implementation of the New Cybersecurity Regime (2026), https://www.mondaq.com/turkey/cybersecurity/1796950/t%C3%BCrkiyes-cybersecurity-board-determines-critical-infrastructure-sectors-a-major-step-in-the-implementation-of-the-new-cybersecurity-regime (discussing Law No. 7545 on Cybersecurity, Official Gazette (Mar. 19, 2025), arts. 7 and 16).
[157] Legal 500, Türkiye Encourages the Use of Local Card Schemes (2025), https://www.legal500.com/intelligence/turkey/finance-and-banking/t%C3%BCrkiye-encourages-the-use-of-local-card-schemes (discussing Presidential Decree No. 2025/1 on the Use of Cards Issued by Local Card Schemes, Official Gazette (Jan. 16, 2025)).
[158] *See* TROY website, Frequently Asked Questions (2026), https://www.troyodeme.com/en/about-troy/faqs
[159] *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.
[160] *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.

[161] *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.
[162] *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.
[163] See Abu Dhabi Department of Health, Circular No. 191/2026, Adoption of Multi-Cloud Approach and On-Site Physical Backup Availability (Sept. 25, 2026), DoH Circulars, at: https://www.doh.gov.ae/en/resources/Circulars; Global Data Alliance, *Comments on Abu Dhabi Department of Health Circular No. 191/2026* (October 2026).
[164] UAE Government, The National Cloud Security Policy (issued February 6, 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 (May 5, 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 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.
[165] 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 (July 20, 2026), https://aep.ae/en/news-media/press-releasesarticles/mansour-bin-zayed-inaugurates-jaywan-uae-s-first-national-card-scheme/.
[166] 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.
[167] Global Data Alliance, Submissions in Vietnam (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=&location=loc-vietnam&sector=&language=&posts_filtered=1
[168] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/

[169] Ernst & Young Vietnam, Legal Alert: Decree No. 356/2025/ND-CP Providing Detailed Guidance for Implementation of the Personal Data Protection Law (Mar. 2026), https://www.ey.com/en_vn/technical/tax/tax-and-law-updates/legal-alert-march-2026-decree-no-356-2025-nd-cp-providing-detailed-guidance-for-implementation-of-personal-data-protection-law.
[170] The GDA has recommended narrowing the Core and Important Data definitions, removing the private-sector localization requirements, recognizing 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.

Several provisions of the draft bear specifically on financial sector and other regulated data:

- Article 6.4 identifies as Core or Important Data any data with a direct and immediate impact on, among other things, finance and banking, energy, and telecommunications, subjects such data to strict localization treatment, and prohibits its transfer outside Vietnam save for Government-approved exceptions.
- Article 24 requires data on the operation of technical infrastructure in the "key national domains" – finance and banking, energy, health, education, telecommunications, and transport – to be classified and protected at the Important or Core level at a minimum, and requires information systems in those domains to integrate technical solutions for real-time connection monitoring with the Ministry of Public Security's centralized monitoring system; Article 35.2 requires managers of Important Data to connect to that system and share alert information.
- Article 28.1 requires Core and Important Data in the named sectors to be stored in data centers in Vietnam, and permits the use of international cloud services only where a real-time backup is maintained in Vietnam under the "supreme control" of Vietnamese state agencies. Articles 28.3 and 28.4 would compel foreign enterprises that violate Vietnam's data security or personal data protection laws to establish local infrastructure and storage, and would permit technical measures such as bandwidth restrictions and suspension of access to data flows within Vietnam.
- Article 32.2 requires prior appraisal and written approval by the Ministry for transfers of Important and Core Data, and Article 57.2 provides for fines of up to 5 percent of an organization's revenue in Vietnam for particularly serious violations involving such data, with the possibility of fines calculated on group global turnover, also capped at 5 percent, for multinational corporations.

The collective effect of these provisions would be that ordinary financial sector data held by US firms and their customers could be classified at the highest tiers because of the sector in which the customer operates rather than the sensitivity of the data, and that global service architectures that rely on cloud services outside Vietnam would require a Vietnam-based backup under state control.

[171] Tilleke & Gibbins, Vietnam Introduces Sectoral List of High-Risk AI Systems (2026), https://www.tilleke.com/insights/vietnam-introduces-sectoral-list-of-high-risk-ai-systems/ (discussing Decision No. 33/2026/QD-TTg (June 30, 2026)).
[172] State Bank of Vietnam, Circular No. 53/2026/TT-NHNN (Sept. 30, 2026), as summarized in LuatVietnam, Circular No. 53/2026/TT-NHNN: AI Automated Payments for Individual Customers Must Not Exceed VND 100 Million per Day, https://luatvietnam.vn/legal-

updates/circular-no-53-2026-tt-nhnn-ai-automated-payments-for-individual-customers-must-not-exceed-vnd-100-million-per-day-892-113479-article.html.

[173] State Bank of Vietnam, Circular No. 18/2024/TT-NHNN on Bank Card Operations, art. 22(2) (effective July 1, 2024), https://english.luatvietnam.vn/tai-chinh/circular-18-2024-tt-nhnn-bank-card-operations-358546-d1.html.

[174] Central Bank of the Republic of Azerbaijan, Regulation on Maintaining Payment Operations and on Payment Instruments, Decision No. 12/3 (Mar. 13, 2024), art. 3.18, https://uploads.cbar.az/assets/Regulation%20on%20maintaining%20payment%20operations%20and%20on%20payment%20instruments_.pdf.

[175] 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

[176] 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

[177] Under this bill, opt-in consent will be required for any data processing that aims to influence decisions or behaviors regardless of the actual impact on a person. This imposes the same requirements for personalized content recommendations or ads as for data to be used for profiling in employment services - two very different risk tiers - and will make it very challenging to provide personalized content recommendations or advertising-supported services in the market. Additionally, the bill's definition of personal information includes inferred data. This will create challenges for AI model training in Canada, which often relies on data inference.

[178] Other issues that may have nexus to cross-border data transfers inclusion of "inferred data" within the scope of the bill's definition of personal information. This framing could create challenges for AI model training in Canada, which often relies on data inference.

[179] 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

[180] 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).

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

[182] *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

[183] 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=2026040763&seq=1

[184] American Chamber of Commerce in Kazakhstan, Data Localization Issue Brief (May 15, 2026), https://amcham.kz/wp-content/uploads/2026/05/2026-05-15_AmCham_DataLocalization_Issue-Brief_ENG_v5.pdf; Law of the Republic of Kazakhstan No. 94-V on Personal Data and Its Protection (May 21, 2013), art. 12, https://adilet.zan.kz/eng/docs/Z1300000094.

[185] Since introduction of Kazakhstan's draft online platform law, the Parliament has been considering two options for establishing a local presence requirement for online platforms: one that would require local registration of an entity or representative office, and one that would require appointment of a legal representative in Kazakhstan. The first option would require foreign operators to maintain a formal corporate presence in Kazakhstan as a precondition for offering their services, restricting the cross-border supply of services offered by online platforms and imposing significant administrative, financial, and compliance burdens. The second option would create other market access conditions for operating in the country.

[186] Separately, in December 2025, Japan enacted a supplementary budget funding METI's "Content Industry Growth Investment Support Project" (IP360), providing approximately ¥35 billion (approximately $233 million) in subsidies to support the government's goal of ¥20 trillion in overseas revenue for Japan-origin content by 2033. Eligibility is limited to "Japan-origin" content produced and owned by Japanese entities or nationals. Large-scale production support requires at least 50 percent Japanese equity and excludes costs for work outsourced to foreign entities, and distribution platform support is generally unavailable to entities established under foreign law. By conditioning public support on the nationality of the company and the origin of the content, IP360 creates an uneven playing field for US-based entities. Similar requirements imposed on digital infrastructure would also raise concerns.

[187] 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/

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

[189] 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.

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

[191] 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.

[192] 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 (May 2, 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 (May 16, 2025), https://bowmanslaw.com/insights/kenya-establishing-the-regional-digital-hub-key-highlights-of-the-cloud-policy-2025/

[193] 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. 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.

[194] 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 May 15, 2026), https://www.odpc.go.ke/draft-guidance-notes/.

[195] 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

[196] 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/

[197] 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

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

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

[200] *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

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

[202] 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

[203] 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

[204] Nepal Rastra Bank, Consultative Document on National Payment Switch (NPS) and the National Payment Ecosystem: Master Reference Document (Oct. 2025), https://www.nrb.org.np/psd/consultative-document-on-national-payment-switch-nps-and-the-national-payment-ecosystem-master-reference-document.

[205] 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

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

[207] 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/

[208] Central Bank of Nigeria, Circular PSS/DIR/PUB/CIR/001/004 on Market Structure Requirements, Data Localisation, Ultimate Beneficial Ownership Disclosure and Systemic Oversight Measures (June 15, 2026), cl. 2, https://regalert.today/document/ffc123b8-cb7d-4767-8857-b79bebce2a39/text; Aluko & Oyebode, CBN Issues Circular on Market Structure, Data Localisation and Systemic Oversight in Nigeria Payments (June 24, 2026), https://aluko-oyebode.com/insights/cbn-issues-circular-on-market-structure-data-localisation-and-systemic-oversight-in-nigeria-payments/; Chambers and Partners, CBN Introduces New Requirements for Nigeria's Payments Ecosystem (July 7, 2026), https://chambers.com/articles/cbn-introduces-new-requirements-for-nigerias-payments-ecosystem.

[209] 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

[210] 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.

[211] 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.

[212] 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.

[213] 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.

[214] 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/.

[215] 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

[216] 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.

[217] Executive Order No. 119, s. 2026, Updating the Government Data Classification, Establishing a Data Residency Framework, and for Other Purposes, §§ 2, 4, 7, 12, 15 & 19, https://www.lawphil.net/executive/execord/eo2026/eo_119_2026.html; Baker McKenzie, Philippines: New Data Classification and Residency Framework (July 2026), https://www.bakermckenzie.com/en/insight/publications/2026/07/philippines-new-data-classification-and-residency-framework.

[218] 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

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

[220] 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

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

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

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

[224] Kursiv Uzbekistan, Uzbekistan Builds Its Own National Switch to Lock Down Digital Payments (Nov. 30, 2025), https://uz.kursiv.media/en/2025-11-30/uzbekistan-builds-its-own-national-switch-to-lock-down-digital-payments/.

[225] Daryo, Uzbekistan to Launch National Payment Switch in 2027 (July 30, 2026), https://daryo.uz/2026/07/30/uzbekistan-to-launch-national-payment-switch-in-2027/.