GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

October 30, 2025

Mr. Edward Marcus
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

Re: Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report, 90 Fed. Reg. 44448 (Sept. 15, 2025): Docket Number USTR–2025–0016

Dear Mr. Marcus,

The Global Data Alliance[1] provides the following information in response to your request[2] for written submissions to the Trade Policy Staff Committee (TPSC) regarding significant trade barriers for inclusion in the National Trade Estimate on Foreign Trade Barriers (NTE Report).

The GDA is a cross-industry coalition of companies that support tens of millions of American jobs and that are active across all 50 US states in every sector of the US economy.

The GDA shares the view of the Office of the US Trade Representative (USTR) that the United States should be a "production economy" — that is "oriented around the production of manufactured goods, agricultural products, services, and knowledge."[3] 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. Such access also supports a strong cybersecurity posture, promoting threat visibility and the ability to detect security risks early. Such access is essential to the functioning of manufacturing plants, modern farms, and service providers in every sector,[4] including the agriculture,[5] automotive,[6] clean energy,[7] finance,[8] health,[9] logistics,[10] media,[11] pharmaceuticals,[12] and telecommunications[13] sectors.

Efforts to renew the US production economy have been 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." The PRC relied on such policies to justify blocking the cross-border transfer of information, mandate data localization, close its digital market, and undermine online economic opportunities — particularly for foreign enterprises and persons.

Today, many governments are advancing policies of data mercantilism and digital protectionism.[14] Proponents of such policies have cited to broad concepts of "digital sovereignty" or "Internet sovereignty" to justify blocking the cross-border transfer of information, mandating data localization, closing digital markets, interfering with the free flow of accurate information and ideas, 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. Since early 2025, USTR has made significant progress in addressing many of these barriers described below. Notable successes in (for example) Indonesia – which committed to remove its customs barriers on international data flows – are a welcome development. We greatly welcome the renewed efforts of the USTR to resolve unfair and non-reciprocal digital trade barriers in many US trading partners that hurt US strategic interests, US companies, and US workers. We look forward to working with USTR on these matters.

Submission of Global Data Alliance for
National Trade Estimate on Foreign Trade Barriers

This submission responds to USTR's solicitation of information relevant to the NTE Report, and contains the following major sections:

I. Executive Summary

A. NTE Statutory Criteria Relevant to Cross-Border Data Policy
B. Economic Benefits of Cross-Border Data Transfers
C. Economic Costs of Data Transfer Restrictions and Data Localization Mandates
D. Policy Arguments Relating to Data Transfer Restrictions and Data Localization Mandates
E. Cross-Border Data Policies in International Agreements
F. The GDA Cross-Border Data Policy Principles

II. Country-by-Country Analysis

Markets of Priority Interest

A. Brazil
B. China
C. European Union
D. India
E. Indonesia
F. Republic of Korea
G. Saudi Arabia
H. Türkiye
I. United Arab Emirates
J. Vietnam

Other Markets of Interest

A. Argentina
B. Bolivia
C. Chile
D. Kenya
E. Mexico
F. Nigeria
G. Pakistan
H. Philippines
I. South Africa
J. Taiwan
K. Thailand

I. Executive Summary

The seamless and responsible movement of information and data across borders is critical to allow the United States to maintain visibility and the ability to respond to crises around the world, as well as to bind the United States more closely with its partners and allies.

Enterprises and workers depend upon forward-looking cross-border data policies to innovate and work. Across every sector of the economy, and at every stage of the production value chain, data transfers are helping sustain economic activity – helping keep workers employed, reach new markets, and develop new products.[15] Cross-border data transfers contribute trillions of dollars to global GDP[16] with growth in every industry driven by data flows and digital technology.[17]

A. NTE Statutory Criteria Relevant to Cross-Border Data Transfers

Digital trade barriers and protectionism are growing at the very time that cross-border data transfers and digital connectivity are helping sustain economic activity and employment. USTR's review of trade barriers under Section 181 of the Trade Act of 1974 requires an identification and analysis of acts, policies, or practices that are reflective of this trend – namely those that constitute significant barriers to, or distortions of: (1) goods and services exports, (2) foreign direct investment, and (3) electronic commerce.[18] In Section II below, we highlight measures and policy trends of concern in several countries, including Brazil, China, India, Indonesia, Saudi Arabia, South Korea, and Vietnam, the European Union (EU), and several other countries of interest.

B. 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 make local industries more competitive.

1. Data Transfers Support US National Policy Objectives

The ability to transfer data in a trusted and secure manner across transnational digital networks is of central importance to the national policy objectives of the United States. cybersecurity,[19] fraud prevention,[20] anti-money laundering, anti-corruption, and other activities relating to the protection of health, privacy, security, safety, consumers, and the environment. They also support shared economic prosperity.[21]

2. Data Transfers Support US Industries Across all Sectors

75 percent of the value of data transfers accrues to companies in sectors such as manufacturing, agriculture, and logistics.[22] Indeed, cross-border data transfers are critical to economic and supply chain resilience across many sectors, including:

- Agriculture,[23]
- Automotive,[24]
- Clean energy,[25]
- Finance,[26]
- Healthcare and medical technology,[27]
- Logistics,[28]
- Media,[29]
- Pharmaceuticals,[30]
- Telecommunications,[31] and
- Many other sectors.[32]

Benefits to other sectors do not just include cross-border access to marketplaces, purchasers, suppliers, and other commercial partners in other jurisdictions. These cross-sectoral benefits also extend to core functional, R&D, and other operational aspects of business in each of the listed sectors.

3. Data Transfers Support US Innovation

Scientific and technological progress require the exchange of information and ideas across borders.[33] Many international organizations recognize the close nexus between cross-border data transfers and innovation. The G20 has underscored that the "[c]ross-border flow of data, information, ideas and knowledge generates … greater innovation,"[34] and the WTO has similarly emphasized that, "for data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies."[35] Likewise, UNCTAD has warned that barriers driven by "data nationalism" reduce "opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation."[36]

By their nature, data localization mandates and data transfer restrictions tend to impede the cross-border exchange of knowledge, technical know-how, laboratory analysis, scientific research, and other information. Data localization mandates and unnecessary data transfer restrictions hurt local innovation because a country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are integral to innovation and the dissemination of technology. These include: (a) scientific, research, and other publications; (b) manufacturing data, blueprints, and other operational information; and (c) digital tools for remote work, laboratory research, and other innovation-related applications.[37] Faced with higher costs to access or exchange information and an unpredictable environment for R&D investments, local industries face increasing innovation challenges. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for R&D.

4. Data Transfers Support the US Workforce

Data transfers support the US workforce's ability to remain productive through hybrid work arrangements that involve teleworking, virtual collaboration, and online training. As detailed in Box 2 below, US jobs that depend on data transfers are growing rapidly. Unfortunately, many such US jobs are under increasing threat as countries erect barriers to US digitally enabled goods and services, and the workers that design, produce, and deliver them. Such barriers hurt workers and impede foreign market access for US exports of aircraft, vehicles and other connected devices, as well as services, that depend upon Internet-, wireless-, and satellite-based communications and other IoT functionality for their sales, operation and support.

5. Data Transfers Support Every Stage of the Economic Value Chain

Data transfers are critical at all stages of the economic value chain.[38] More specifically, the ability to move data across borders responsibly contributes to the ability of companies of all sizes to access key technologies in the cloud and across national borders to innovate, invest, create jobs, and promote productivity, workplace safety, and environmental efficiency, at every stage of the production life cycle, as summarized below.

- R&D: Multinational R&D teams collaborate across borders to develop new products, cures, and other advances using cloud-based software solutions and research data produced globally.

- Market Forecasting: AI tools analyze data from around the world to identify patterns that can help predict market demand, customer design preferences, and risk factors relevant to global investment decisions.

- Safety and Productivity: Real-time analytics of sensor data across global production facilities, machinery, and other assets can alert operators before hazards or breakdowns can occur – allowing for predictive maintenance and safe, productive working conditions.

- Regulatory Compliance: Legal compliance teams gather data from global operations to demonstrate that products and services meet international regulatory requirements.

- Sales: From order fulfillment, to invoicing, to responding to customer feedbacks – businesses can meet global customer needs only if they can receive and respond to customer queries transmitted across borders.

- Inventory Control: Data analytics and AI can be used to adjust global inventories –avoiding shortages and freeing up resources for more productive uses.

- Supply Chain Management: Real-time electronic data exchange allows companies to authenticate documents seamlessly, optimize shipping routes, and manage transportation assets for purposes of time, cost, and energy efficiency.

- Post-Sale Service: Cross-border data transfer allow manufacturers to trace and recall products, and address service requests, transparently, safely, and quickly.

Box 1: Cross-Border Data Policy and US Small- and Medium-Sized Businesses[39]

Cross-Border Data Policy and US Small- and Medium-Sized Businesses

32.5 million US Small- and Medium-Sized Businesses (SMEs) account for:

- 99.9% of all US businesses
- 48% of all US workers (61.2 million workers)
- 90% of all US business openings (909,808 new openings and 9.1 million new jobs in 2019-2020)

Cross-Border Data Transfers Benefit SMEs

- SMEs account for 95% of all US exporting enterprises, with SME exports accounting for roughly 25% of all US exports and supporting over 6 million jobs (in 2017). With greater foreign market access, SMEs estimate that they could increase sales by 15-40% and hire between 10-50 new employees each.
- Digital tools help small businesses reduce export costs by 82 percent and transaction times by 29 percent
- Digital market openings promise relief for SMEs: While 95% of SMEs were negatively impacted by the COVID-19 pandemic, the pandemic also caused 70% of SMEs to accelerate efforts to become more digitally competitive.
- The most digitally advanced SMEs are growing 8 times faster than the least advance.
- SMEs with a strong digital presence grow twice as fast, and are 50% more likely to sell outside their region, relative to those with little or no digital presence.

Cross-Border Data Transfers Matter to SMEs

- 65% of SMEs move data across borders, with even higher percentages for those that export, per CSIS survey.
- SMEs highlighted divergent data privacy rules (40-60% of SME survey respondents) and data localization rules (30-40% of SME respondents) as key challenges.

C. 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 in terms of

jobs, exports, and investment. For both local enterprises and foreign-invested enterprises, such measures disrupt operations; raise the costs and challenges of providing services and manufacturing goods; and make it harder to invest and keep local workers employed. Among other things, such measures effectively deprive end-users of advanced services and put them at a competitive disadvantage compared with companies in other countries. We elaborate on each of these points below.

First, data localization mandates and unreasonable data transfer restrictions are **particularly damaging to local industries, including agriculture, logistics, and manufacturing (e.g., textiles)**. In fact, it has been estimated that 75% of the value of data transfers accrues to these industries.[40] Data transfers enable companies of all sizes to connect and find prospective customers in overseas export markets. Companies also depend upon the ability to integrate software and other emerging technologies at every stage of the production and value chain. Data-enabled software innovations are connecting suppliers, manufacturers, and service providers around the world, while accelerating efficiencies relating to product design, engineering, production, logistics, marketing, and servicing. Cross-border data transfer restrictions impede the ability to realize these efficiencies.

Box 2: Cross-Border Data Policy and the US Workforce[41]

Cross-Border Data Policy and the US Workforce

Cross-border data policy is a core aspect of US international competitiveness. An agile US workforce benefits from cross-border access to knowledge, information, and technology, and from an absence of data localization mandates and unnecessary data transfer restrictions. US jobs that depend on data transfers are growing rapidly, with:

- 67% of new US science, technology, engineering, and mathematics (STEM) jobs in computing and software;
- Nearly 16 million workers employed in software jobs in the United States;
- 1.5 million more such jobs open for American workers;
- 40% of US manufacturers urging additional upskilling for advanced manufacturing positions; and
- Numerous digital training opportunities available across all 50 US states, the private sector, community colleges, vocational schools, and apprenticeship programs.

- With this dual growth in demand and available training opportunities, US advanced manufacturing jobs are growing in software engineering, computer-aided design and manufacturing (CAD/CAM), industrial machinery mechanics, and Computer Numerical Control (CNC) machinery operations.

- US workers across all export-intensive sectors earn an average 15% more than workers in other sectors. The highest export pay premium (19%) goes to workers in digitally-skilled and export-intensive manufacturing sectors.

US jobs are under increasing threat as countries erect barriers to US digitally enabled goods and services, and the workers that design, produce, and deliver them. By some reports, digital trade barriers have increased by over 800% since the late 1990s. Such barriers hurt workers and impede foreign market access for US exports of aircraft, vehicles and other connected devices, as well as services, that depend upon Internet-, wireless-, and satellite-based communications and other IoT functionality for their sales, operation and support.

Second, data localization mandates and unreasonable data transfer restrictions **raise the costs of international trade**. Data transfers are critical to reducing the costs to local firms of exporting to other markets. One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.[42] Likewise, 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%.[43] When countries impose unreasonable data transfer restrictions and data localization mandates, they prejudice their local industries' ability to realize these significant welfare-enhancing benefits and efficiencies.

Third, data localization mandates and unreasonable data transfer restrictions **hurt local innovation and competitiveness**. A country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are critical to growth and innovation, business operations, and

the transfer of technology. These include: (a) productivity-enhancing software solutions; (b) scientific, research, and other publications; and (c) manufacturing data, blueprints, and other operational information. Faced with higher software costs and an unpredictable environment for R&D investments, local industries face challenges keeping technological pace with foreign competitors — threatening both domestic and export market sales. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for investment and R&D.

Fourth, data localization mandates and unreasonable data transfer restrictions **undermine access to tailored data-enhanced analytics and insights that can help address economic and societal challenges**. A country that limits cross-border data transfers also may exclude itself from the development of data analytics and AI-driven technology solutions that can help address economic and other challenges. Local industries and economies can face competitive harm if they are deprived of the insights that come from consolidating local data sets within larger regional or global data sets for purposes of data analysis.

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

Several grounds are frequently cited as the basis for imposing data restrictions, but these grounds are often based on misconceptions or are cited to justify trade barriers that are more restrictive than necessary to achieve asserted policy objectives. 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 matters. We address several common arguments below.

Some argue that data restrictions are necessary to ensure **cybersecurity**. As discussed in Box 3 below, *how* data is protected is much more important to security than *where* it is stored. Companies may choose to store data at geographically diverse locations to reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. In addition, cross-border data transfers allow for 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.

Some also argue that data localization and data transfer restrictions are necessary for **privacy** reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. This is not the case. Data localization mandates and data transfer restrictions do not increase personal data protection. To the contrary, for a variety of reasons including, 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 the use of different transfer mechanisms that are not interchangeable. It is important that businesses be able to rely on a range of data transfer mechanisms, which may include, where relevant, adequacy decisions, certifications, codes of conduct, Binding Corporate Rules (BCRs), and Standard Contractual Clauses (SCCs). These mechanisms can help support global data transfers and can be designed with strong safeguards. These mechanisms are integrated into national laws including those of the EU,[44] Japan,[45] New Zealand,[46] and Singapore.[47] Broadly speaking, these types of mechanisms are consistent with the so-called "accountability principle," which allows personal data to be transferred across borders while maintaining standards of data protection found in the jurisdiction in which the personal data was first collected. This principle is described in the OECD Privacy Framework;[48] the APEC Privacy Framework,[49] the APEC Privacy Recognition for Processors (PRP) system,[50] the APEC Cross Border Privacy Rules (CBPR) system,[51] the Global Cross-Border Privacy Rules Forum,[52] and the ASEAN Model Contractual Clauses.[53] Where differences exist among data protection regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate global data transfers. Taking into account widely accepted privacy principles and industry best practices, governments should also aim

to ensure that privacy frameworks are interoperable and allow for the seamless flow of data across borders.

Some claim that data localization and data transfer restrictions are necessary to ensure that **regulators and law enforcement authorities have access** to data relevant to conduct investigations. The location of the data, however, is not the determining factor. Responsible service providers work to respond to lawful requests for data consistent with their obligations to their customers and to protect consumer privacy. If the service provider has a conflicting legal obligation not to disclose data, law enforcement authorities have several options: International agreements — including Mutual Legal Assistance Treaties (MLATs) or Agreements (MLAAs), multilateral treaties, and other agreements, such as those authorized by the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act — can establish foundations for mutual legal assistance and reciprocal transfers of law enforcement data. Courts may also issue requests to authorities abroad for the transfer of data through letters rogatory.

Finally, there is an emerging trend in some countries towards "data mercantilism," a policy perspective that is often associated with both data-related trade barriers, as well as other types of domestic preferences or measures discriminating against foreign products, services, enterprises or technologies. Data mercantilism appears to be premised upon the view that cross-border data restrictions or data localization mandates offer protectionist economic benefits. Such policies may be grounded in assumptions that cross-border data restrictions and data localization measures will foster the creation of jobs and "local champion" enterprises, and increased domestic innovation, investment, and GDP growth. However, these assumptions are not supported by economic evidence.[54] In fact, economic growth benefits from an increase — not a decrease — in connectivity. By some estimates, just over 50% of the world's population was connected to the Internet in mid-2017, and cross-border data restrictions or localization mandates (whether premised on "data sovereignty" or other grounds) serve only to limit the economic opportunities for those who are connected. Countries that unreasonably limit cross-border data transfers and impose data localization mandates isolate themselves from the global digital economy. Such self-imposed restrictions hinder economic development, reduce productivity, limits public policy options, and depress export competitiveness.

E. 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,[55] we urge the United States to return to negotiating cross-border data commitments relating to the following commitments – 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 impose requirements to use or locate computing facilities in their own territory as a condition for conducting business.
- Custom Duties: Parties shall not impose customs duties on electronic transmissions.

These commitments focus on the impact that data regulations may have on trade among trading partners, and do not prevent the US government from enacting rules to promote legitimate public policy purposes, such as privacy or cybersecurity. This is because the commitments focus on the cross-border impacts of data regulations – rather than their substantive privacy, cybersecurity, or other legal aspects.

To address the cross-border impacts of any data regulations that involve incidental restrictions on data transfers,[56] we urge the United States to continue to clarify that such restrictive data regulations should:

- Be necessary to achieve a legitimate public policy objective;[57]
- Not be applied to produce arbitrary or unjustifiable discrimination or disguised trade restrictions;[58]

- Not impose restrictions on transfers that are greater than necessary;[59]
- Not improperly discriminate among different economic sectors;[60]
- Not discriminate against other WTO member entities by modifying conditions of competition via less favorable treatment on cross-border data transfers relative to domestic ones;[61]
- Be designed to be interoperable with other national legal frameworks;[62] and
- Be developed in a transparent and accountable manner.

The bulleted list above reflects longstanding tenets of international law and practice, namely: (1) the freedom to pursue necessary public policy objectives; (2) the renunciation of discrimination against non-national persons, products, services, or technologies; (3) minimization of trade-restrictive effects; and (4) due consideration for trading partner laws.[63]

Box 3: Cross-Border Data Policy and Cybersecurity

Data transfers are critical to ensure high standards of cybersecurity. Conversely, cross-border data transfer restrictions and localization requirements undermine cybersecurity by:

1. **Creating unnecessary complexity and silos.** Data transfer restrictions and localization requirements force organizations to adopted a siloed-approach to data, often restricting the locus of certain data, but not others. This differentiation creates unnecessary technical complexity without any corresponding benefit to security. Simply put: artificial requirements to store data within borders strain the people, processes, and technologies an organization needs to manage its cybersecurity risk.

2. **Impeding real-time cyber awareness and responsiveness.** Data transfer restrictions and localization requirements impede visibility of cybersecurity risks, not only at the intra- and inter-organizational levels, but also at national and international levels. If cyber defenders cannot access threat indicators or other cybersecurity data collected in one jurisdiction, it becomes harder to address malicious cyber activity in other jurisdictions. On the other hand, the ability to transfer data across transnational digital networks threat responsiveness as it allows for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in real time.

3. **Undermining collaboration on detection and response.** Data transfer restrictions and localization requirements can impede cross-border collaboration, information sharing, and other coordinated network defense. When such restrictions and requirements isolate network defenders from each other, they cannot adopt a unified defensive posture against malicious actors that do not respect national borders. In short, data transfer restrictions can confer a permanent advantage on malicious actors.

4. **Weakening third party cybersecurity services**. Many organizations amplify their own cybersecurity risk management through third-party cybersecurity service providers. Best-in-class services depend access to cyber data from around the globe. Without this access, these services and their users become more vulnerable to compromise.

5. **Decreasing resiliency, concentrating cyber risk, and creating single points of failure.** Whether a particular geographic area is at high risk for a natural disaster or in a potential future war zone, having data efficiently distributed is a crucial component of resiliency. The misconception that keeping data only within national boundaries will increase its security can actually create significantly more risk.

6. **Using cybersecurity fear to drive other policy objectives.** Localizing data within a country – or blocking its transfer – has no functional cybersecurity benefit. Security is determined by the technical and operational protections that accompany the data, not the location. Transfer restrictions and localization requirements are often used to advance other objectives. Perhaps the most systemic problem with using cybersecurity laws to require localization, then, is that it diminishes the role of laws and policies that are truly designed to improve security.

F. GDA's Cross-Border Data Policy Principles

The GDA has published a set of Cross-Border Data Policy Principles (reproduced in the Annex) to help inform domestic and international policymaking in relation to measures that have an impact on cross-border data transfers.[64] The principles are as follows:

- 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

G. Conclusion

The Global Data Alliance welcomes the opportunity to provide this submission and looks forward to working with USTR to achieve meaningful progress in addressing the cross-border data policy concerns identified in this submission.

Box 4: Cross-Border Data & Healthcare

The Role of Health Data Transfers in Healthcare Research

- **Cross-border data analytics and R&D collaboration.** Cross-border data analytics can help speed the early identification of potentially useful drug candidates, shortening discovery timelines from years to months. The health data-sets and genomic data used in this analysis can come from multiple sources, such as clinical trials, data registries, and real-world evidence, but the required expertise, technology, and computer facilities often are not in the same country as where the data originates.

- **Cross-border digitization of clinical trial processes.** Cross-border data flows are essential to the conduct of clinical trials. Data flows are necessary to identify and establish clinical trial sites, identify clinical trial participants, and monitor the conduct of clinical trials. Cross-border data transfers also help companies address different countries' drug regulatory approval requirements.

- **Cross-border demographic representation.** Cross-border studies are also critical to ensuring that new products are safe and effective across different demographics, populations, and regions.

- **Cross-border regulatory collaboration.** Each country has their own national regulatory agency to ensure that a new medicine is safe and effective. As a result, even after the clinical trial data moves from the trial site to the clinical trial sponsor, it must also be able to flow to governments in whatever countries where the new medicine may be approved.

- **Cross-border data transfers and good pharmacovigilance practice (GVP).** Cross-border data transfers are also key to post-marketing surveillance through adverse event reporting; site inspections; and post-authorization safety studies in different countries.

The Role of Cross-Border Data Transfers in Healthcare Delivery

- **Cross-border data transfers and healthcare diagnosis.** Cross-border data transfers allow for the cross-referencing of larger trans-national data sets containing relevant diagnoses, facilitating more precise diagnoses and avoiding incorrect or unnecessary treatments.[1]

- **Cross-border data transfers and healthcare delivery via medical technologies.** Advances in healthcare therapy via medical technologies[1] depend on responsible access to health data from diverse sources. In the medical technology context, data transfers can be critical to: (a) providing relevant information to clinicians for purposes of monitoring safety and efficacy of ongoing treatments, (b) health economic analysis of therapy and patient outcomes, and (c) researching and engineering therapy improvements and innovations.

- **Cross-border data transfers and responsible AI in medical technologies.** The responsible integration of medical technologies with data analytics can help predict patterns and responses in healthcare delivery contexts. Cross-border data transfers play a critical role in allowing for the aggregation of larger, more representative datasets to which these analytical tools can be applied.[1]

- **Cross-border data transfers and remote health services.** Cross-border data enabled remote health services holds promise for improving patients outcomes.[1] This includes enabling cross-border access to overseas-based remote health platforms, portals, or other technologies that can offer the highest levels of security, privacy, and functionality.[1]

The Role of Cross-Border Data in Health Insurance

- **Cross-border data transfers & actuarial risk analysis:** Cross-border access to demographic, health, and financial data is necessary to develop sufficiently large data sets to build accurate prediction models, e.g., period and cohort life tables, for understanding risk levels.

- **Cross-border data transfers & insurance payment**. Cross-border data transfers allow insurers to cross-reference the authenticity of claims with international databases and different branches or partners of a firm for more efficient payouts. Manual data entry and payment processes increase operational costs and cannot track claim progress in real time, increasing the risk of fraud and human error. For instance, in the event of a natural disaster, cross-border transfers make real-time sharing and gathering of information about damages and one's deducible possible, expediting the payout to those affected and providing timely disaster recovery.

- **Cross-border data transfers & insurance affordability and product range.** Health data transfer restrictions and localization mandates deprive end customers of access to the full range of insurance options and increase costs. First, because insurers rely on centralized data analytics and processing to generate their full service options, such restrictions can mean that customers will have access to fewer insurance options and support systems. Second, the inability to share health data with reinsurers outside the country may also indirectly limit the capacity of local health providers to offer the care that they need.

II. Country-by-Country Analysis

The GDA provides below a country-by-country summary of measures of concern in relation to cross-border data transfer restrictions and data 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[65] 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, as well as other countries. We also summarize measures of concern is other markets of interest: Argentina, Bolivia, Chile, Kenya, Mexico, Nigeria, Pakistan, Philippines, South Africa, Taiwan, and Thailand.

Markets of Priority Interest

A. Brazil

We outline below issues worthy of future monitoring in Brazil's cross-border data policy landscape. Please see **here** for submissions on Brazil's cross-border data measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[66]

***Personal Data Protection and Cross-Border Data**:* On August 23, 2024, the Brazilian Data Protection Authority (ANPD) published Resolution CD/ANPD No. 19/2024 – Brazil's regulations governing international data transfers. The regulations promote streamlined and interoperable transfer mechanisms; recognize the importance of cross-border data transfers for various commercial and public policy goals; and advance principles of accountability and transparency. The Regulations address international data transfers in four scenarios:

- To countries or international organizations that provide adequate protection, as recognized by the ANPD, or
- When a controller guarantees protections consistent with the LGPD through the use of:
    - Specific contractual clauses (with new text for Brazilian SCCs contained in Annex II)
    - Standard contractual clauses
    - Global corporate standards

Data and Server Localization Requirements: The first Guidelines on Government Procurement of Cloud Services were issued in late 2018 and newer versions were issued in 2021 and 2023. These versions still include server and data localization requirements that negatively impact the procurement of cloud computing services by all federal agencies.[67] Following a consultation period, the final Guidelines continued to include the localization requirements.[68]

***"Data Economy" Legislative Proposal (Under Discussion):* National Data Economy Policy (under discussion):** The Brazilian Government is exploring a framework modeled or, at least partially inspired, on the EU Data Act that could impose special obligations on non-Brazilian firms' use of "non-personal" data. The effort is being led by Brazil's Industry Ministry (MDIC), who serves as coordinator of a Working Group within the Interministerial Committee for Digital Transformation (CITDigital). The policy (PNED) is currently undergoing interministerial alignment by the President's Chief of Staff and will soon be followed by a Call for Inputs. While not yet formal, this raises concern that broad data-sharing or onshoring requirements could be included, creating new barriers if enacted.

Restrictions on IoT Permanent Roaming: Brazil's National Telecommunications Agency (ANATEL) enforces a rule that restricts international machine-to-machine (M2M) and Internet of Things (IoT) service providers from using permanent roaming for more than 90 days. As a result, U.S. companies are faced with the choice of building local infrastructure in Brazil or being excluded from the market. This approach diverges from other practices of other leading regulatory systems, which generally permit ongoing M2M roaming to support seamless global service and prevent fragmentation in the rapidly evolving IoT sector. While permanent roaming can benefit local telecom operators and the Brazilian economy by leveraging domestic network resources, ANATEL reaffirmed its ban on permanent roaming in 2018 following public feedback, despite concerns raised by industry stakeholders.

B. China

We outline below several concerns and recommendations regarding cross-border data policies and measures in China. Many GDA members face a challenging commercial environment in China, particularly in relation to cross-border data transfers, which are subject to outright prohibitions in some contexts and significant legal uncertainty in other contexts.[69]

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.[70]

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

***Data Security Law*:** The Data Security Law (DSL), enacted on June 1, 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)[71] 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).

The GDA and 31 other global associations raised these concerns in a letter submitted to China during the drafting process, but the concerns were not addressed.[72]

***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.[73]

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

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

C. European Union

Over the past several years, the European Union has modernized its digital economy regulatory and policy framework relevant to software and data service providers, in particular with regards to privacy, cybersecurity, data transfers, and copyright. The new European Commission is actively pursuing an assertive digital policy agenda, guided by at times competing ambitions to promote Europe's "digital sovereignty" while pursuing "open strategic autonomy."

Calls for data localization or for measures that seek to ensure EU organizations are immune from application of third countries' legislation continue to gain traction at EU level and in some Member States.

While GDA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, and in harnessing the value of data, restrictive cross-border data policies – and especially any data localization mandates – may constitute *de facto* market access barriers or dramatically hinder the ability of organizations from the United States and other economies to move data across border.

Please see **here** for submissions on the European Union's numerous cross-border data restrictions and digital sovereignty measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[74]

Cross-Border Data Transfers: Measures that impede the transfer of data across borders impose substantial burdens on US service providers and negatively impact US jobs. European authorities are historically focused on data transfers to the United States. The various digital laws affecting data transfers (such as GDPR, Data Act, Data Governance Act) would benefit from simplification. The transfer tools need to remain practical and flexible. It is very important to ensure that the personal data regime is NOT extended to non-personal data for data transfers and avoid localization and protectionist pressures that impede with data transfers.

US-EU Data Privacy Framework: In 2023, the United States and the EU launched a new Transatlantic Data Privacy Framework (DPF) to replace its predecessor Privacy Shield framework. The DPF relies on an Executive Order (EO) on Enhancing Safeguards for United States Signals Intelligence Activities.[75] The EO creates new safeguards on US signals intelligence activities, establishes a new redress mechanism, and enhances US oversight of signals intelligence. In September 2025, the EU General Court upheld the validity of the DPF and dismissed the action for annulment brought by a French politician Latombe. However, further legal challenges to the DPF before the European Courts remain a possibility. The European Commission is set to carry out the second review of the DPF in 2027.

EU Standard Contractual Clauses for Data Transfers: The European Commission's Standard Contractual Clauses (SCCs) provide model terms for various data transfer scenarios. However, companies face significant burdens in conducting third-country Transfer Impact Assessments (TIAs), which are highly complex and should not fall disproportionately on individual businesses. Clause 14 of the SCCs requires detailed assessments of the legal framework in the importer's country, creating substantial resource demands – particularly for smaller companies – and uncertainty over what constitutes a "sufficient" TIA in the eyes of Data Protection Authorities. The absence of clear thresholds or guidance, combined with ambiguity over which party is responsible for the TIA, frequently complicates contract negotiations.

Cybersecurity Certification Scheme for Cloud Services (EUCS): In 2024, the EUCS framework continued to represent a concerning development given the original inclusion of sovereignty provisions that discriminate against non-national cloud service providers. On the one hand, the latest draft proposed for consideration to Member-States by the European Commission and the European Union Agency for Cybersecurity (ENISA) removed references to sovereignty requirements from the EUCS is positive. On the other hand, the possibility that Member States could still impose sovereignty requirements in national law on top of the technical requirements outlined (*see e.g.,* France's SecNumCloud) continue to present a challenge.[76] The EUCS discussions have been on hold for over a year now, and should only be settled with the upcoming review of the Cybersecurity Act (CSA) which gives mandate to ENISA to draft the scheme. The concern is that some Member-State will push to include sovereignty requirements in the law already, leaving ENISA no room to diverge from them when the new certification schemes will be drafted.

Public procurement reform: As part of its broader strategic sovereignty agenda in the digital, industrial, and security domains, the EU is preparing to review its public procurement framework. The forthcoming EU Public Procurement Act, expected in Q2 2026, aims to strengthen Europe's capacity to produce clean technologies domestically and to attract greater investment within the Union. The proposed "Made in Europe" criteria would also apply to the procurement of sensitive products, prioritizing European suppliers. These legislative changes could make the participation of non-EU service providers in public tenders particularly difficult.

Cloud and AI Development Act and Quantum Act: Following the announcement of the European Commission's 2026 Work Program, the EU is intensifying its focus on reducing strategic dependencies. Specifically, it aims to assert greater control over critical technologies – including batteries, cloud services, artificial intelligence, and quantum computing – as well as raw materials and energy production, through diversified supply chains and the introduction of new legislative frameworks that may restrict the participation of non-EU businesses. The forthcoming Cloud and AI Development Act (expected in Q1 2026) and Quantum Act (expected in Q2 2026) are positioned as key instruments to advance the EU's digital sovereignty. The CAIDA risks excluding non-European Cloud and AI providers by introducing so-called "sovereignty criteria" for public procurement, alongside hard-to-measure sustainability requirements, namely related to the energy consumption of data centers. The core elements of such criteria remain at this stage rather vague, and even in the upcoming proposal they might be subject to significant shifts, depending on the political proclivities of lead negotiators.

EU Data Act: The Data Act introduces new requirements for data transfers that go above and beyond GDPR's established framework for data transfers. This becomes challenging for companies handling mixed data sets as it creates impediments to transfer non-personal data, resulting in administrative burden. More specifically, BSA is concerned with the provisions (Arts. 28 and 32) in the EU Data Act relating to cross-border data transfers. We continue to recommend that the Commission either remove these provisions, or at a minimum, clarify the ambiguity and breadth of the text of Article 32.1 of the Data Act to make clear that "conflicts" with EU law or member state law are only expected to arise if the corresponding law expressly precludes the transfer of data to a particular third country jurisdiction. Conversely, if data transfers or access are halted in an unpredictable and broad manner, it could raise questions regarding the international obligations and the ability of EU and foreign entities to engage in cross-border commerce, R&D, and other activities.

Data Transfers in Trade Agreements with Third Countries: In 2024, the European Commission advanced new provisions on cross-border data transfers for purposes of its free trade agreement negotiations. These new provisions are an improvement over prior cross-border data transfer norms. However, additional room for improvement remains – particularly in relation to self-judging exceptions text relating to privacy matters.

For example, on July 1, 2024, the EU–Japan agreement on cross-border data flows entered into force. The agreement establishes necessity and proportionality tests for measures taken to achieve legitimate public policy objectives and requires parties to enable cross-border data transfers. At the same time, it allows broad exceptions for data protection and privacy, which could still be interpreted too broadly.[77]

Digital Operators Resilience Act (DORA): As of January 17, 2025, an EU regulatory framework on digital operational resilience, the 'Digital Operational Resilience Act' (DORA) applies. This regulation aims at ensuring that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. The proposed legislation will require all firms to ensure that they can withstand all types of Information and Communication Technology (ICT) - related disruptions and threats and the proposal introduces an oversight framework for ICT providers, such as cloud computing service providers (CSPs) and Internet Service Providers (ISPs).

This legislation, which builds on the European Banking Authority guidelines for outsourcing to cloud providers (Regulatory Technical Standards – RTSs) , could have potentially negative consequences for CSPs and ISPs to financial services companies, and the current recommendations from the guidelines would become mandatory. Those would include, among others, the imposition of model contract clauses that would cover inspection and audit rights, termination rights and exit strategies; a new EU supervisory body to oversee CSPs and ISPs, or large penalties for non-compliance. Moreover, non-EU headquartered providers may be subject to higher levels of scrutiny.

Data Transfers in Trade Agreements with Third Countries: In 2024, the European Commission advanced new provisions on cross-border data transfers for purposes of its free trade agreement negotiations. These new provisions are an improvement over prior cross-border data transfer norms. However, additional room for improvement remains – particularly in relation to self-judging exceptions text relating to privacy matters.

For example, April 29, 2024, the EU Council adopted the protocol adding this new cross-border data flows provisions to the EU-Japan Economic Partnership Agreement. The protocol introduces proportionality and necessity tests for legitimate public policy objectives, and requires parties to provide for instruments enabling cross-border transfers. Once the agreement has been ratified by Japan, and the EU and Japan have notified each other about the completion of their internal procedures, the agreement can enter into force.[78]

EU Health Data Space: On January 8, 2025, the Council formally adopted the final regulation of the European Health Data Space (EHDS). The GDA engaged closely with the Commission on the data localization mandates and cross-border data restrictions proposed in earlier drafts of the EHDS. The final restrictions now in effect are less onerous in several respects from earlier proposals. The final restrictions are excerpted below:

- Article 86 - Member States shall ensure that a particularly high level of protection and security is in place when processing personal electronic health data for primary use... In this respect, this Regulation shall not preclude a requirement under national law, ... that, ... the storage of personal electronic health data referred to in Article 14 of this Regulation for the purpose of primary use be located within the Union, in compliance with Union law and international commitments.

- Article 87 - Health data access bodies, trusted health data holders and the Union health data access service shall store and process personal electronic health data in the Union when performing pseudonymisation, anonymisation and any other personal data processing operations referred to in Articles 67 to 72... By way of exception from paragraph 1 of this Article, the data referred to in that paragraph may be stored and processed in a third country, or a territory or one or more specified sectors within that third country, where such country, territory or sector is covered by an adequacy decision adopted pursuant to Article 45 of Regulation (EU) 2016/679.

- Article 88 - Non-personal electronic health data made available by health data access bodies to a health data user in a third country ... , to authorised participants in a third country or to an international organisation,... shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation (EU) 2022/868 where the transfer of such non-personal electronic data to third countries presents a risk of re-identification through means going beyond those reasonably likely to be used, in particular in view of the limited number of natural persons to whom those data relate, the fact that they are geographically scattered or the technological developments expected in the near future.

- Article 89 - Digital health authorities, health data access bodies, authorised participants in the cross-border infrastructures provided for in Articles 23 and 75 and health data users shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent the transfer of non-personal electronic health data held in the Union to a third country or an international organisation, including for governmental
- access in a third country, where such transfer would create a conflict with Union law or the national law of the relevant Member State.

- Article 90 - Transfer of personal electronic health data to a third country or an international organisation shall be granted in accordance with Chapter V of Regulation (EU) 2016/679. Member States may maintain or introduce further conditions on international access to, and transfer of, personal electronic health data, including limitations, in accordance with Article 9(4) of Regulation (EU) 2016/679, in addition to the requirements laid down in Article 24(3) and Article 75(5) of this Regulation and in Chapter V of Regulation (EU) 2016/679.

- Article 91 - Health data access applications and health data requests submitted by a health data applicant established in a third country shall be considered eligible by health data access bodies and

> the Union health data access service if the third country concerned: (a) is an authorised participant on the basis of having a national contact point for secondary use covered by an implementing act referred to in Article 75(5); or (b) allows Union health data applicants access to electronic health data in that third country under conditions that are not more restrictive than those provided for in this Regulation...

Between 2022 and 2024, the GDA published several papers regarding the European Health Data Space (EHDS).[79] The GDA White Paper underscores the importance of the cross-border exchange of non-personal health data to developing new biopharmaceutical treatments and improving medical outcomes for patients within the EU and beyond. The comments urged the Commission to avoid imposing in the EHDS restrictive cross-border data policies that would have far-reaching and unintended consequences. The White Paper also includes detailed evidence and case studies regarding the importance of data transfers to cross-border: (1) biopharmaceutical R&D, (2) clinical trial processes, (3) demographic representativeness in R&D, (4) regulatory collaboration, (5) good pharmacovigilance practice, (6) healthcare diagnosis, (7) deployment of medical technologies in healthcare delivery, (8) responsible AI-based health applications, and (9) remote health services. Although the EHDS has now been finalized, the GDA will continue to monitor its implementation for the active imposition of unnecessary data transfer restrictions.

D. India

Overview/Business Environment

The commercial environment for GDA members remains challenging in India, in part due to an increase in restrictive cross-border data policies.[80] 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 American 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,[81] regulations on machine-to-machine (M2M) systems,[82] and payment processing regulations[83], to proposed rules for the Digital Personal Data Protection Act.[84]

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.[85]

Digital Personal Data Protection Act – Draft 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. Unfortunately, the Draft Rules designed to implement the Law,[86] published in January 2025, introduce new authorities to require data localization and restrict international data transfers. Specifically, Rule 12(4) empowers the government to require data localization for "significant data fiduciaries" and Rule 14 establishes a broad power to restrict data transfers to third countries.

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.[87]

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),[88] 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."[89] "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.[90] 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.[91] While MeitY issued subsequent "Frequently Asked Questions (FAQs) on the Directions", it still did not address concerns around localized log storage.[92]

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 fulfil reporting obligations. While the CSCRF came into effect on 1 January 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.

Framework for Adoption of Cloud Services by Regulated Entities: In March 2023, SEBI introduced the "Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)".[93] The Framework is applicable to regulated entities that use cloud service providers ("CSPs" or "service providers") to conduct their businesses. In Section 6, under Principle 3 of the Framework, CSPs must store and process data for regulated entities (REs) within data centers that are prescribed by MeitY.

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 prevent 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. As India is a key market, it is of utmost importance that global FIs can implement their global cloud strategies in India in a way that is consistent and limits frictions. Global FIs typically consolidate their systems in a single global hub, which offers services to the rest of the firm. Local data storage/processing require discrete technological builds, further segregating local systems from global hubs. This exposes FIs to greater cybersecurity risks by creating a more decentralized environment that needs to be safeguarded, which further inhibits central oversight and information sharing across borders. In addition, local processing will negatively impact FIs' global operation, their ability to undertake activities at a global level and cross-border service offering.

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

RBI - Master Direction on KYC and Video based Customer Identification Process (V-CIP): In May 2021, RBI amended its Master Direction (MD) on KYC dated February 25, 2016 and added, amongst other requirements, a 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.[94] 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.[95] CSPs participating in the initiative must have "data center facility within India".[96]

***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.[97] 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.

India's Position on the Moratorium on Customs Duties on Electronic Transmissions: India has been a leader of efforts to undermine the multilateral Moratorium on customs duties and related requirements on electronic transmissions – a stance that directly threatens US export interests relating to film, financial services, music, publications, software, and many other sectors. We urge the United States to ensure that India aligns itself with the US position of support a permanent Moratorium, as reflected in the Administration position established in the America First Trade Policy and other core policy statements.

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.[98] In December, the Committee published the revised report.[99] In our written comments, GDA highlighted numerous concerns including mandatory sharing of proprietary non-personal data, restrictions on cross-border data transfers and local storage requirements.[100] This proposal no longer appears to be under active consideration, but it will be important to ensure that no similar measure reappear.

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.

E. Indonesia

The commercial environment in Indonesia is challenging for GDA member companies,[101] as Indonesia has developed or is developing policies that make it increasingly difficult to access the Indonesian market with digitally-enabled products and services.

Please see **here** for submissions on Indonesia's numerous cross-border data restrictions and digital sovereignty measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[102]

Duties on Digital Products: In mid-2025, the United States and Indonesia announced that Indonesia would withdraw measures that authorized the imposition of customs requirements on digital transmissions. GDA welcomes this announcement, and looks will continue to monitor Indonesia's implementation of the agreement. This bilateral agreement will hopefully put an end to this history that began with the February 2018 issuance by the Ministry of Finance (MOF) of Regulation 17, which amended Indonesia's Harmonized Tariff Schedule (HTS) to add Chapter 99 "[s]oftware and other digital products transmitted electronically."[1] These globally unprecedented requirements mandated compliance for digital transmissions with all customs laws that attach to tangible imports, along with the payment of 10 percent value-added tax (VAT) and 2.5 percent income tax. These rules were further supplemented by Regulation 190, which required the filing of import declarations for data moving across transnational digital networks.

Personal Data Protection: In mid-2025, the United States and Indonesia announced that Indonesia would deem the United States to be a jurisdiction offering adequate standards of personal data protection – a major positive development. This development comes against the backdrop of the Personal Data Protection (PDP) Law, enacted on October 17, 2022. Unfortunately, even though the Law has taken effect, neither the implementing regulations nor the regulation directing the establishment of the DPA have been issued. We are concerned that there will be no grace period for organizations to adjust to the new rules, and this has been confirmed informally at meetings with KOMDIGI (formerly KOMINFO).

GR71*:* Government Regulation 71/2019, revising GR 82/2012, requires public and private sector electronic system operators (ESOs) to register their electronic systems and requires private sector ESOs to facilitate "supervision" by government agencies, including by granting access to electronic systems and data for monitoring and law enforcement purposes. Our latest interactions with KOMDIGI on this confirm that they are contemplating amendments to GR71 that seek to encourage investment in data centers through data localization regulations. However, no draft amendments have been released.

GR71's implementing regulations continue to be a significant barrier to digital trade. Public Scope ESOs are defined to also include public administration which goes beyond national security and intelligence data. KOMDIGI's implementing Regulation No. 5/2022 requires private sector ESOs to register with KOMDIGI through an Online Single Submission (OSS) system or face significant penalties for non-compliance including blocking by KOMDIGI. Failure to comply with government takedown orders for a potentially broad category of "prohibited electronic information" can also result in blocking.

Data Localization in the Financial Sector: The Bank of Indonesia still requires core/important financial transactions to be processed domestically. The Financial Services Authority (OJK) has incrementally allowed some electronic processing systems to be based offshore for banking services, insurance services, multi-financing services, and lending-based technology, but for the most part, the policy remains highly restrictive and burdensome for global companies trying to operate within Indonesia.

Local Content Requirements for Software*:* Indonesia's Ministry of Industry issued regulation No.22/2020 (IR22) on the Calculation of Local Content Requirements (LCR) for Electronics and Telematics, with a government target to achieve 35% import substitution by 2025. IR22 provides specific and extensive requirements for manufacturing and development for both digital and non-digital physical products. The government has signaled an intention to build on this LCR requirement and add similar LCRs for software and applications, which would impact companies that provide services over the internet, including cloud

[1] *Regulation No. 17/PMK.010/2018 (Regulation 17)* (Indonesian) at: https://jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf

services. In addition to that, Presidential Instruction Number 2 Year 2022 requires government agencies to plan, allocate, and realize at least 40% of the national budget for goods/services to utilize MSMEs and Cooperative products from domestic production.

Cloud Services: Indonesia's regulatory framework is among the least conductive for the adoption of public cloud technology in the financial services industry. The biggest barriers are in the form of data localization, burdensome requirements to seek prior regulatory approval, and the lack of differentiation in the materiality of workloads. To begin, the financial regulator (OJK) does not permit transactions to be processed offshore in sectors like such as multi-financing and lending based technology. These rules are reportedly motivated in part by regulators' lack of trust in multilateral law enforcement systems. Second, the OJK requires financial institutions to go through a lengthy approval process before moving workloads to the public cloud. This applies to commercial banks planning to operate an electronic system outside Indonesia and financial institutions that plan to outsource the operation of their data centers or disaster recovery centers. Additionally, Regulation No. 9/POJK.03/2016 only allows commercial banks to outsource "support work" (i.e., activities that are low risk, do not require high banking competency and skills qualification, and do not directly relate to operational decision-making). These workloads that can be outsourced are all subject to the same regulatory requirements, with no differentiation in terms of materiality, unlike in other jurisdictions, such as Australia and Singapore.

F. Republic of Korea

The overall commercial environment in the Republic of Korea (Korea) for GDA members is mixed on the subject of cross-border data transfers and data localization.[103] Korea has a strong IT market and a mature legal system. On the other hand, digital protectionism – reflected in data residency mandates, physical network separation requirements, and other restrictive data-related requirements for industry sectors, such as government/public services, finance, healthcare, and education – severely hampers digital trade and the cross-border exchange of knowledge, information and data with Korea.

Please see **here** for submissions on South Korea's numerous cross-border data restrictions and digital sovereignty measures and **here** for its ranking in the GDA Cross-Border Data Policy Index.[104]

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 US 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 US 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 US 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 US service providers at a competitive disadvantage to domestic competitors and limits progress on the broader US digital trade agenda.

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 US 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 US 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 in Annex I 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 US 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 US service providers.

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. In the ongoing negotiations with Korea, the US should extract explicit and enforceable commitments from Korea to align the CSAP with global norms and enable market access for trusted US service providers. These commitments should include the following: (1) Classifying a larger share of public institution data systems as Low tier and remove references to personal information in the CSAP; and (2) Aligning certification requirements for Low and Medium tier data systems with international best practices by eliminating requirements for physical network separation, data residency, use of Korea-developed encryption algorithms, and local personnel presence. CSAP should also accept internationally 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 for BSA members to serve the South Korean market. Although the National Assembly has continued to amend the Personal Information Protection Act (PIPA) and the European Commission and South Korea have mutually 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: In the Korea-US Free Trade Agreement, South Korea committed to allowing financial institutions to transfer data to foreign affiliates and to permit certain data processing and other functions to be performed outside of Korea. Nevertheless, 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.[105] Moreover, South Korea's network segregation rules, which require internal and external networks to be physically segregated,[106] 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.[107]

Cross-Border Data Restrictions in the Insurance Sector: US 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, US reinsurers remain unable to transfer data outside of Korea.

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

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 now mandates local storage for many types of data – especially for government, critical infrastructure, and personal data – and is increasingly requiring foreign companies to localize operations (e.g. by setting up regional HQs) if they want to serve the Saudi market.

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.[108]

Essential Cybersecurity Controls (2018): Saudi Arabia's National Cybersecurity Authority (NCA) issued the Essential Cybersecurity Controls Regulation requiring that all government agencies, state-owned companies, and operators of Critical National Infrastructure (CNI) host their data and IT systems inside Saudi Arabia. Specifically, Controls require that an "organization's information hosting and storage must be inside the Kingdom of Saudi Arabia" (ECC-1:2018, 4-2-3-3). ECC-1:2018, 4-1-3-2 sets another localization requirement relating to cybersecurity services, stating that "cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia". These mandates cover sectors from financial services and healthcare to oil & gas. The rule, in effect, bars these organizations from using offshore data centers or cloud services for sensitive data. For US companies, it means partnering with local data center providers or losing access to a wide swath of the Saudi B2B market. The localization mandate increases costs and reduces efficiency for Saudi institutions as well, since they cannot freely adopt global cloud solutions.

Cloud Computing Cybersecurity Controls (2020): The NCA followed up with cloud-specific rules that extend localization to service providers. The Cloud Cybersecurity Controls require cloud service providers to deliver certain key services only from within Saudi Arabia. For example, all customer data storage, backup/disaster recovery systems, and monitoring systems for cloud offerings must reside on Saudi soil. This effectively forces service providers to build local cloud regions in Saudi or work through a locally hosted partner. More specifically, Cloud Cybersecurity Controls CCC-1:2020 2-3-P-1-10 & 11 require that companies provide cloud computing services from within KSA, including systems used for storage processing, disaster recovery centers, and systems used for monitoring and support. While this measure does allow for level 3 and 4 data to be hosted outside KSA, it depends on securing an exception.

Personal Data Protection Law (2023): Saudi Arabia's PDPL (first enacted 2021, amended 2023) places tight restrictions on transferring personal data abroad. Controllers must obtain a permit from the Saudi data authority (SDAIA) to send personal data outside Saudi, unless the destination is on an approved list or a narrow exception applies. The law also requires organizations to register databases and meet onerous record-keeping rules. In practice, until Saudi Arabia issues clear adequacy decisions, most personal data (e.g. customer or employee data held by companies) must be kept in-country. This creates compliance burdens for multinational firms – for instance, a U.S. company can't centralize its Saudi customer data processing in a regional hub without SDAIA's permission. Such approvals are uncertain and slow, so many firms opt to localize data storage in Saudi, benefiting domestic data center operators.

Financial Sector Localization: Saudi regulators have also targeted the financial/payments sector for data sovereignty. The Saudi Central Bank (SAMA) has mandated localization of certain electronic payment processing functions that global card networks provide. By 2022, Saudi Arabia pushed major U.S. payment networks to route transactions through local systems; it also joined other Gulf states in developing domestic card schemes to reduce reliance on foreign networks. Additionally, a 2021 policy will ban companies that don't locate their regional headquarters in Saudi from government contracts – indirectly pressuring large tech firms to move regional data and offices to Riyadh. These measures serve Saudi's strategic aim of data control, but they act as market access barriers by forcing costly localization and disadvantaging firms that are regional (e.g. UAE) hubs.

Internet of Things: Saudi Arabia's IoT regulations require that all SIM cards in IoT devices used or imported into the country be issued by a locally licensed operator. While the rules do not explicitly mention permanent roaming, this effectively prohibits the use of foreign or roaming SIMs for IoT services, including connected devices such as vehicles.

H. Türkiye

Türkiye has ramped up data localization through both new laws and strict enforcement of existing regulations. While Türkiye's general data protection law mirrors the EU's, the government has gone further, mandating that banking and public data stay within Türkiye's borders. We provide below a summary of Türkiye's many digitally protectionist barriers. 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, critical categories of information and data—including population, health, and communication records, as well as genetic and biometric data—must be securely stored within Türkiye.[109] The Circular also prohibits public institutions and organisations from storing their data on cloud services, except where those services are operated on the institution's own private infrastructure or by local service providers under its control. Consequently, private-sector vendors that process or store data on behalf of public entities are effectively required to host such data on servers located in Türkiye. This approach is mirrored in the Information and Communication Security Guide.[110]

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 US firms' market access, but also means higher costs and less flexibility for Türkiye's financial sector (which can't fully leverage global cloud economies of scale). 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 11(4) of this measure requires banks to keep in Türkiye their primary information systems (comprising all 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; effectively private or BRSA-only community clouds hosted domestically. BRSA can also restrict transfers abroad of customer/bank secrets on economic/national security grounds.[111]

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.[112]

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.[113]

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.[114]

Communiqué on Information Systems Management VII-128.9 (2018) and the new **VII-128.10** (Official Gazette No. 32840, 13 Mar 2025; effective 30 Jun 2025). Article 26(1) of this measure

requires entities subject to Capital Markets Board oversight—including, among others, publicly listed companies and pension investment funds—must 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. Public companies retain some exemptions from earlier CMB decisions. 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.[115]

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. Personal data cannot be sent outside Türkiye unless the destination country is officially approved as having "adequate" data protection or the Turkish Data Protection Board grants special permission. As of 2025, Türkiye has recognized very few countries as adequate (and notably not the United States). In absence of an adequacy decision, a company must either obtain each data subject's explicit consent *after* informing them of risks, or submit binding corporate rules/contractual clauses for the Board's approval – a process that is cumbersome and rarely granted. 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. The trade impact is a fragmentation of corporate IT systems and a de facto barrier to Turkish–US data exchange, especially given the lack of a US–Türkiye adequacy arrangement.

***IoT and Telecom Data*:** Türkiye also localizes certain telecommunications data. For instance, in 2019 the ICT regulator (BTK) issued a decision limiting permanent international roaming for IoT devices and requiring that all related IoT data be kept in Türkiye. More specifically, IoT services using embedded SIM cards (eSIMs) must be programmed or manufactured by local mobile network operators or their vendors; all data must be stored within Türkiye; international roaming for foreign SIM cards is limited to 120 days. This rule has consequences far beyond mobile telephony. For example, connected car services or smart device platforms must use Turkish mobile networks and store data locally, rather than managing them from a global cloud. It serves as another example of Turkish authorities interposing local-presence requirements that predominantly affect foreign service providers (which typically centralize such operations).

Regulation on Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector: According to Article 5(2) of this measures, traffic and location data are, as a rule, not permitted to be transferred abroad, purportedly for national security reasons.[116]

Information and Communication Security Guide: This Guide sets out specific security obligations for the electronic communications industry, requiring that domestic communication flows remain within Türkiye. It expressly prohibits both the transfer of subscriber and traffic data outside the country and any re-routing of such data through foreign systems back into Türkiye.[117]

***Social Media Law No. 7253 (2020)*:** Türkiye amended its Internet Law in 2020 to compel social network providers (with over 1 million daily Turkish users) to appoint a local representative and store users' data in Türkiye. This law has effectively forced major platforms to build local data facilities for Turkish user content or partner with Turkish data centers. It raises compliance costs and subjects foreign platforms to Turkish jurisdiction for user data, facilitating government content control.[118]

Internet of Things: Türkiye's Information and Communication Technologies Authority (BTK) has set regulations that restrict international permanent roaming for IoT devices to a maximum of 90 days within a 120-day period. Additionally, all devices using e-SIMs must use profiles from locally licenses operators, and related data and infrastructure must be hosted within Türkiye. These requirements, effective since February 2020, present challenges for global IoT service providers seeking to operate in the Turkish market.

I. United Arab Emirates

While the UAE advertises itself as a data hub, certain regulations – especially for public sector and sensitive 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 Law No. 45/2021) came into effect in 2022 and introduced rules for cross-border personal data transfers. Under this law, personal data may only be transferred outside the UAE if the destination country is deemed to provide an "adequate" level of protection, or if the exporting company has put in place other safeguards (e.g. standard contracts or consent)bigid.com. In practice, firms often need to notify or seek approval from the UAE Data Office for transfers to non-listed countries. This is a new compliance step that particularly affects US businesses, since – absent an official UAE-US adequacy arrangement – data flows to US headquarters or cloud servers must rely on case-by-case safeguards.[119]

***Health Data Law (2019) – Medical Data Localization*:** The UAE's Health Data Law (Federal Law No. 2 of 2019) prohibits storing or processing UAE patients' health data outside of the UAE by default. Hospitals, clinics, and insurers must keep health records on servers located in the UAE.[120] In 2021, UAE authorities introduced exceptions (e.g. for telemedicine, insurance claims, research) which can be granted on a case-by-case basis by health regulators. However, the general rule stands: unless an exception is approved, patient data cannot leave the UAE. This has led healthcare providers and global pharma companies to use local data centers for clinical and patient management systems. The rule protects patient privacy but also acts as a localization barrier – foreign health IT and cloud providers must partner with local hosts. Notably, Abu Dhabi's Department of Health even banned cloud use for any health data unless explicitly exempted. These restrictions limit the adoption of global health data solutions and complicate international clinical trials or health analytics involving UAE data.[121]

***National Cloud Security Policy (2022–2025)*:** In September 2025, the UAE's Cyber Security Council issued a new National Cloud Security Policy that, while easing some prior restrictions, still enforces a form of data sovereignty for government-related workloads. The policy now allows foreign cloud providers to serve most government and regulated industry data *if* they maintain local UAE data centers. "Secret" or highly sensitive government data, however, must reside on "fully sovereign" UAE infrastructure (i.e. cloud systems operated by Emirati entities under exclusive UAE jurisdiction). This framework means that US service providers can compete for UAE public sector projects *only* if they invest in local data centers. Even then, informal procurement preferences often favor the UAE's state-backed cloud firms (e.g. G42). For foreign competitors, the cost of entry is high and certain top-secret projects remain off-limits. In essence, the UAE has localized a chunk of its cloud demand, boosting local cloud capacity but reducing some of the efficiencies of a truly global cloud marketplace.[122]

***Financial Data & Banking Regulations*:** The UAE's central bank and sector regulators have also issued guidelines that imply local handling of certain financial data. For example, some UAE banking rules require that customer and transaction records be accessible in the UAE at all times, limiting outsourcing to overseas processing centers.[123] Also, the UAE has joined the GCC trend of building domestic payment processing: by 2022 it launched a plan to route UAE card transactions through a local scheme, partly to ensure transaction data stays in-country as a safeguard against foreign sanctions. While not an outright ban on data exports, this trend toward local financial infrastructure can edge out foreign payment providers and compel them to localize data storage to continue operating in the UAE.

Internet of Things: In the UAE, IoT services must be provided through locally licensed telecom operators with SIMs and eSIM profiles required to be locally provisioned for long-term IoT deployments. This is one example of Gulf countries enforcing strict controls over IoT connectivity to ensure that data remains local.[2]

[2] Oman applies similar rules, prohibiting permanent roaming for IoT devices using foreign SIMs. Qatar requires IoT services to meet local standards for data handling, cybersecurity, and lawful interception. While

J. Vietnam

As of October 2025, Vietnam continues to advance severe trade restrictions on US digital exports and US 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 American workers and American enterprises — making it more difficult for Americans to export digitally-enabled services and goods to Vietnam — affecting US services and manufacturing workers; US artists and creators; and US designers, engineers, programmers, and researchers.

Vietnam's actions run directly counter to the Administration's efforts to advance a "production economy" built on "robust and realist trade policy [that] can create jobs, promote innovation, strengthen the national defense, raise wages, and foster [a] manufacturing renaissance" in the United States.[124]

Over the past several years, Vietnam has enacted, implemented, and proposed various measures that raise concerns from a cross-border data policy perspective. Remarkably, despite the strong and unified concerns raised by US 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. Sought to enshrine in law — and bring into full force and effect — restrictions and mandates that hurt US workers and enterprises that were only proposed as of January 2025; and
3. Introduced wholly new restrictions and mandates that hurt US workers and enterprises — e.g., Decree 102 — that did not even 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.[125]

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.[126]

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

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

Decree 147: Vietnam's Decree No. 72/2013/ND-CP (**Decree 72**) enacted in July 2013, originally mandated that all aggregated information websites, social media platforms, and online content and game providers maintain at least one server in Vietnam "serving inspection, storage, and provision of information at the request of competent state management agencies". This requirement, initially vague

---

short-term roaming remains technically permitted, these frameworks collectively ensure that IoT connections and data profiles are managed and localized within each country's borders.

and infrequently enforced, became increasingly burdensome and prescriptive after the 2018 Cybersecurity Law, which formally obligated both domestic and foreign service providers of personal and user-generated data to store such data in Vietnam and establish a local legal presence requirement. Under Decree 147/2024/ND-CP (**Decree 147**), effective December 2024, these 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 are currently set out in its PDP Decree (i.e., Decree 13/2023/ND-CP), which took effect on July 2023. However, Vietnam's National Assembly recently passed the Personal Data Protection Law (**PDP Law**) on June 26, 2025. The PDP Law will enter into force on January 1, 2026. The relationship between the PDP Decree and the PDP Law has not been clearly addressed, and it is likely that the PDP Decree will remain in effect until it is explicitly replaced by a new Decree issued under the PDP Law. The PDP Decree imposes restrictive data transfer and data localization requirements on industries and businesses subject to it. In particular, there are burdensome requirements for personal data processors to register with the Personal Data Protection Commission (**PDPC**) for cross-border transfers of personal data with very detailed requirements for registration, and for the PDPC to carry out annual assessments or audit-like exercises on cross-border data transfers by data transferring entities. These obligations are impractical and may create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

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

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

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

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

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

Data Law and Draft Implementing Decree: Vietnam's Law on Protection of Consumer Data in the Digital Environment (**the Data Law**) was promulgated in 2023 and is expected to take 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 will enter 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.

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

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

Moratorium on Customs Duties on Electronic Transmissions: Vietnam has committed in some of its regional trade agreements not to impose customs duties on electronic transmissions, yet its degree of support for the multilateral Moratorium on such customs duties remains uncertain. We urge the United States to ensure that Vietnam supports in practice the US defense of the Moratorium, as reflected in the America First Trade Policy and other US policy documents.

Other Economies of Interest

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

A. Argentina

Argentina does not recognize the United States as an "adequate" destination for personal data.[127] Under Disposition 60-E/2016, transfers of personal data from Argentina to the United States are only lawful if additional safeguards are in place, since the United States lacks a single comprehensive federal privacy law – but rather relies on a mix of federal and state privacy and consumer protection standards. This creates a trade barrier for US firms, which must navigate onerous contract and compliance steps that foreign competitors (from economies deemed adequate) do not face. The restriction increases operational complexity and costs for Argentine companies too, as data flows to US business partners and service providers (for analytics, HR, etc.) are delayed and legally uncertain.

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

B. Bolivia

Bolivia has moved toward strict data localization for government data. Under the Plan de Implementación de Software Libre y Estándares Abiertos (PISLEA) 2025–2030, Bolivian public agencies are *required to keep all "non-public" state data on servers located within Bolivia*.[129] 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 countryes.scribd.com. (By contrast, only *public* or openly published data are exempt and may be stored or backed up abroades.scribd.com.) The definitions of "public" vs. "non-public" data are broad and vague, essentially treating most government-held information as non-public unless explicitly open. This localization mandate, coupled with the requirement that government entities use open-source systems, 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 marketplace.

Please see **here** for Bolivia's ranking in the GDA Cross-Border Data Policy Index.

C. Chile

Chilean banking regulations impose localization-like obligations for critical data. The Chilean Financial Market Commission (CMF) published rules ("RAN Chapter 20-7") (Recopilación Actualizada de Normas 20-7) on outsourcing requires that banks maintain a *real-time local copy* of certain important data even when using cloud or overseas services. In fact, if a bank outsources "significant or strategic" processing abroad, it must also keep a contingency data processing center in Chile with up-to-date data to ensure continuity. This essentially means critical banking records mirrored domestically. The Chilean regulator did relax this rule slightly in 2019 by creating a narrow exception (for banks with very robust risk management) to the local site requirement, but most institutions still must comply. The effect of RAN 20-7 is to force banks toward local infrastructure: few qualify for the exception, so banks using global cloud providers must set up Chilean backup facilities. In sum, Chile's CMF (Financial Market Commission) mandates that critical financial data remain accessible in Chile, which safeguards regulatory oversight but adds cost and deters reliance on purely foreign cloud storage.[130]

Please see **here** for Chile's ranking in the GDA Cross-Border Data Policy Index.

D. Kenya

Kenya has introduced several measures that require data localization. Under the Computer Misuse and Cybercrimes Act[131] 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 & Cybercrimes Committee).[132]

Separately, the Data Protection Act (2019)[133] 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 2022[134] 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, etc., which means a broad swath of public-interest data cannot be solely hosted abroad.

Most recently, in December 2024 Kenya issued a National Cloud Policy (effective 2025)[135] that *encourages* data residency and sovereignty best practices. While not an outright ban, this Cloud Policy urges government agencies and businesses to consider local hosting for sensitive government information and critical infrastructure data when adopting cloud solutions.

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.[136]

E. 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. US 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.[137] 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.[138] 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 US 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 so-called "kill switch" mechanisms for "blocking" data transfers and digital access to Mexico for certain US companies.[139] 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.[140] 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.[141]

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.[142]

F. 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.[143]

In addition, Nigeria's draft National Cloud Policy 2025[144] 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 US 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.[145]

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.[146]

G. Pakistan

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

First, Pakistan has released several drafts of a Data Protection Bill that contain provisions mandating data localization and restricting the cross-border flow of "sensitive" and "critical" data raise concerns (*see* Bill Section 27(1)), as do the broad powers granted to a proposed National Commission for Personal Data Protection to create new regulations. Most recently, Pakistan's Ministry of Information Technology and Telecommunication (MoITT) published an updated Draft of the Personal Data Protection Bill in 2023.[147] That Bill received Cabinet approval in July 2023, but has not yet been enacted. The bill's broad and vague definitions of sensitive and critical data could significantly hinder cross-border data flows and impede free trade.

Second, the MoITT also launched a "Cloud First Policy" in 2022.[148] Notably, this policy contains a strong presumption in favor of data localization requirements on broad classes of government data ("restricted," "sensitive," and "secret"), and there is only a narrow possibility of derogations.[149]

Third, in the financial sector, the State Bank of Pakistan (SBP), which is the nation's central bank, enforces strict data residency rules for regulated institutions.[150] SBP policy prohibits banks and other financial institutions from hosting core banking systems or sensitive financial workloads on offshore clouds. According to SBP's outsourcing framework, only non-critical workloads may be placed with overseas cloud providers, while any "material" (core) data processing abroad requires case-by-case SBP approval. This effectively means that key banking data must remain on local servers unless an exemption is explicitly granted by SBP.

Fourth, under Pakistan's Prevention of Electronic Crimes Act, transmission of certain information is prohibited without user consent, subject to severe penalties (including imprisonment), and data transfers are more broadly prohibited to certain economies, such as India, Israel, and Taiwan.[151]

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.[152]

H. Philippines

Local industry stakeholders and some government agencies have advocated vigorously for localization mandates in recent years.[153] 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 draft 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 US service providers providing services to the Philippines government.

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.

I. 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.[154] 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.[155] The policy's local-first approach suggests that future regulations could increase local storage requirements in other sectors as well – a trend to watch.

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.[156]

J. 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.[157]

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 (expected to be finalized in 2025) underscores Taiwan's cautious approach: certain health-related personal data cannot leave Taiwan at all, or only under strict conditions.[158]

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.[159] 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.

K. **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.

GDA Cross-Border Data Principles (excerpts)

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.[160]

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.[161] Sixty percent of global GDP is expected to be digitized by 2022, and six billion consumers and 25 billion devices are expected to be digitally connected by 2025.[162] Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.[163] The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance.[164] Many Regional Trade Agreements (RTAs) reflect this presumption.[165]

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;[166]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[167]
- 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;[168] and
- Include other procedural safeguards and due process.[169]

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.[170]

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 RTAs negotiated to date, principles of non-discrimination and national treatment are critical to advancing an international policy consensus on data transfers.[171]

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 RTAs negotiated to date[172] 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.[173]

This analysis is important because **how** data is protected is typically more salient than **where** it is stored. As outlined above and in many RTAs 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.[174] 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,[175] security,[176] and safety.[177] 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.[178]

[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] *See* USTR, Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report, 90 Fed. Reg. 44448 (Sept. 15, 2025), at: https://www.federalregister.gov/documents/2025/09/15/2025-17782/request-for-comments-on-significant-foreign-trade-barriers-for-the-2026-national-trade-estimate

[3] USTR, 2025 Trade Agenda (March 2025), at: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2025/march/us-trade-representative-announces-2025-trade-policy-agenda

[4] Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf

[5] Global Data Alliance, *GDA Website – Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/

[6] Global Data Alliance, *GDA Website – Automotive* (2022), at: https://globaldataalliance.org/sectors/automotive/

[7] Global Data Alliance, *GDA Website – Energy* (2022), at: https://globaldataalliance.org/sectors/energy/

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

[9] Global Data Alliance, *GDA Website – Healthcare* (2022), https://globaldataalliance.org/sectors/healthcare/

[10] Global Data Alliance, *GDA Website – Supply Chain Logistics* (2022), https://globaldataalliance.org/sectors/supply-chain-logistics/

[11] Global Data Alliance, *GDA Website – Media and Publishing* (2022), https://globaldataalliance.org/sectors/media-publishing/

[12] Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/

[13] Global Data Alliance, *GDA Website – Telecommunications* (2022), https://globaldataalliance.org/sectors/telecommunications/

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

[15] *See* Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), at https://www.globaldataalliance.org/downloads/GDAeverysector.pdf ; See Global Data Alliance, *Jobs in All Sectors Depend Upon Data Flows* (2020), at https://www.globaldataalliance.org/downloads/infographicgda.pdf

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

[17] *Ibid.*

[18] 19 USC 2411 *et seq.*

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

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

[21] 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

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

[23] Global Data Alliance, *GDA Website – Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/

[24] Global Data Alliance, *GDA Website – Automotive* (2022), at: https://globaldataalliance.org/sectors/automotive/

[25] Global Data Alliance, *GDA Website – Energy* (2022), at: https://globaldataalliance.org/sectors/energy/

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

[27] Global Data Alliance, *GDA Website – Healthcare* (2022), https://globaldataalliance.org/sectors/healthcare/

[28] Global Data Alliance, *GDA Website – Supply Chain Logistics* (2022), https://globaldataalliance.org/sectors/supply-chain-logistics/

[29] Global Data Alliance, *GDA Website – Media and Publishing* (2022), https://globaldataalliance.org/sectors/media-publishing/

[30] Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/

[31] Global Data Alliance, *GDA Website – Telecommunications* (2022), https://globaldataalliance.org/sectors/telecommunications/

[32] Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf

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

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

[35] *See Trade Policy Review of India*, Secretariat Report, *supra* note 5.

[36] UNCTAD Digital Economy Report 2021, *supra* note 2.

[37] See Global Data Alliance, Cross-Border Data Transfers and Remote Work (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf; See Global Data Alliance, Cross-Border Data Transfers and Remote Health Services (Sept. 2020) https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf

[38] Global Data Alliance, *Global Data Alliance Infographic: Jobs in All Sectors Depend Upon Data Flows* (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf

[39] 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.

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

[41] 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/

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

[43] 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
[44] Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

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

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

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

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

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

[50] APEC Privacy Recognition for Processors (2021)

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

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

[53] 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.

[54] *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).

[55] 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.

[56] 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

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

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

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

[60] 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.

[61] *See e.g.,* US-Japan DTA Art. 11, footnote 9; USMCA Art. 19.11, footnote 5.

[62] *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.

[63] 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.

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

[65] Closely related to localization mandates and cross-border restrictions affecting various types of financial data are measures that impede the provision of financial services across borders. We list several of the challenges faced by some GDA members in the financial services sector below:

Brazil: The Brazilian Central Bank's (BCB) oversees not only the development of policy that affects all payment schemes in the Brazilian market, but also the development and regulation of PIX, a real-time payment scheme (including its participation rules and licenses), which went live on November 16, 2020. Pix compete directly with

other market players. This situation has produced outcomes in which it is made more difficult for foreign providers to offer cross-border payment services.

Chile: General Instruction No. 5 (“ICG No. 5”) issued by the Chilean Competition Tribunal (TDLC) and upheld by the Supreme Court have produced structural limitations on the ability of foreign EPS' ability to update their rules, standards, and scheme fees without prior agreement from licensees or approval from the National Economic Prosecutor’s Office (FNE) - this impeding the ability to offer cross-border payment services.

Costa Rica: The Central Bank of Costa Rica (BCCR) has restricted cross-border payment services since March 2020, when the Congress of Costa Rica enacted Law 9831 granting the BCCR authority to set price control measures to the card payments system, including a wide range of electronic service providers with operations in Costa Rica. The BCCR’s regulation of inbound cross-border payments favors Costa Rican entities to the detriment of US banks and EPS suppliers.

China: When China joined the WTO in 2001, it committed to allowing non-Chinese EPS companies to compete and do business in its domestic market on equal terms with Chinese companies, including by processing renminbi-denominated transactions in China. While U.S. EPS suppliers have continued to process “cross-border” transactions in China for decades, which primarily involve purchases by individuals traveling to and from China as of October 2025, only two EPS suppliers have secured the license to operate in the domestic market.

India: The United States has continued to raise concerns relating to informal and formal policies with respect to electronic payments services that appear to favor Indian domestic suppliers over foreign suppliers. The National Payment Council of India (NPCI) is a quasi-government agency that operates the largest domestic payment system in the country, including Unified Payments Interface (UPI) and RuPay (debit and credit) cards. In the past several years, the Government of India has taken many direct and indirect actions that give preferential treatment to NPCI, creating a non-level playing field for international EPS providers.

Indonesia: Bank Indonesia should not undertake regulatory requirements that hinder US electronic payment services (EPS) companies from processing data internationally and introducing innovations in risk and security to the Indonesian market. Specifically, Under Article 71 (6) of Bank Indonesia Regulation (PBI) 23/7/2021, Bank Indonesia has the discretion to exempt transactions from onshore processing requirements.\

Mexico: USMCA Chapter 17 (Annex 17-A) contains high-standard Financial Services commitments related to cross-border trade, including application of the national treatment and market access obligations for electronic payment services (EPS), which Mexico has not yet fully implemented in relation to the draft regulation on retail payment networks led by Comision Nacional Bancaria y Valores (CNBV) and the Central Bank (Banxico) and draft regulation on clearinghouses led by Banxico. This situation impedes cross-border payment services into Mexico.

Oman: The Central Bank of Oman (CBO) launched the domestic payment scheme ALMAL in September 2025 to reduce issuing and processing costs, particularly for SMEs. While we support these objectives, mandating co-badging as a condition of participating in this market raises concerns.

Pakistan: The State Bank of Pakistan (SBP) is pushing to have its domestic payment system, 1LINK, process domestic transactions despite no regulatory mandate or circular in place. The SBP is driving this through an Industry-Led Steering Committee, which comprises issuing banks, 1LINK, fintech, and the Pakistan Banks Association. This is a marked change from when the SBP was previously allowing banks to choose their payment network rather than be pushed to use one domestic network only, and it impedes the cross-border financial services.

South Africa: Foreign payment system operators were required to localize domestic processing infrastructure to comply with the amendments of the Payment Association of South Africa (PASA) Payment Clearing House (PCH) System Operator Criteria (focusing on domestic processing) effective from August 1, 2025. The policy requires that, for domestic transactions, payment service operators must authorize, clear and settle transactions through infrastructure that is established and maintained in South Africa.

Türkiye: Türkiye continues to contemplate extraterritorial authority over US electronic payment services companies and their clients domiciled outside of Türkiye. Specifically, Türkiye is considering regulation of inbound

cross-border payments, and such regulation would be more burdensome and restrictive on foreign EPS providers and their clients, than it is on domestic companies.

Vietnam: Domestic Processing Mandate (SBV Circular 18/2024/TT-NHNN): This circular, which replaces previous regulations, codifies and reinforces a domestic processing mandate. It requires that all domestic card-present transactions conducted on the networks of US electronic payments companies must be routed through the National Payment Corporation of Vietnam (NAPAS). This mandate limits competition, preventing U.S. companies from using their own global processing infrastructure for domestic transactions, and favors a state-owned entity.

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

[67] https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684
[68] Comments available at:
https://www.bsa.org/~/media/Files/Policy/Filings/CommentsGDA_CloudProcurement.pdf

[69] 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

[70] 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

[71] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[72] 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
[73] 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

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

[75] White House, Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (Oct. 2022), at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

[76] See discussion on this point in Euractiv, Reuters

[77] The EU-Japan negotiations concluded in principle on October 28, 2023; both Parties signed the Agreement on January 31, 2024; and the EU Parliament gave its consent to the protocol on March 14, 2024

[78] The EU-Japan negotiations concluded in principle on October 28, 2023; both Parties signed the Agreement on January 31, 2024; and the EU Parliament gave its consent to the protocol on March 14, 2024
[79] GDA 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

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

[81] *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

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

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

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

[85] 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

[86] 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

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

[88] Storage of Payment System Data Directive

[89] Storage of Payment System Data Directive

[90] Storage of Payment System Data Directive

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

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

[93] Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs), https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html

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

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

[96] 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

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

[98] Report by the Committee of Experts on Non-Personal Data Governance Framework, August 2020, https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf
[99] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dec 2020, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf
[100] 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
[101] *See generally*, GDA Cloud Scorecard – 2018 Indonesia Country Report, at: https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Indonesia.pdf

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

[103] *See generally*, GDA Cloud Scorecard – 2018 Korea Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Korea.pdf
[104] Global Data Alliance, Submissions in Indonesia (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=korea&sector=&language=&posts_filtered=1

[105] 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.

[106] 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.

[107] 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

[108] 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&sector=&language=&posts_filtered=1

[109] CMS Law, Data localisation requirements in Turkiye (Jan. 24, 2023) at https://cms-lawnow.com/en/ealerts/2023/01/data-localisation-requirements-in-turkiye

[110] *See e.g.,* Global Data Alliance, *Comments on Turkish Data Transfer Requirements* (2024), at https://globaldataalliance.org/wp-content/uploads/2024/05/05202024gdatkdatareg.pdf. Furthermore, a 2019 Presidential Circular on Information and Communication Security Measures introduced localization requirements on government workloads deemed “strategic”. In 2020, the Digital Transformation Office published Guidelines clarifying that the scope of the localization requirements included critical information and data; however, the loosely defined residency obligations under the Presidential Circular remains a regulatory challenge as the legislation overrides the DTO Guidelines. Strict data localization also applies in the financial services sector, where the Banking Regulation and Supervision Agency requires primary and secondary information systems to be hosted in Turkey. The Central Bank of Turkey implements similar restrictions on cloud outsourcing and prohibits the use of cloud for certain workloads. The Turkish Data Protection Law (DPL) permits the transfers of personal information to jurisdictions deemed adequate, subject to the explicit consent of the data subject or after obtaining permission from the data protection authority (KVKK). However, Turkey has not yet decided on countries deemed adequate for international transfers. The adequacy decision has been postponed several times since 2021.

[111] See generally, Erdem & Erdem, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (March 17, 2020) at https://www.erdem-erdem.av.tr/tr/bankalarin-bilgi-sistemleri-ve-elektronik-bankacilik-hizmetleri-hakkinda-yonetmelik; Esin Attorney Partnership, New Regulation on Bank IT Systems and Electronic Banking Services (March 18, 2020) at https://www.esin.av.tr/2020/03/18/new-regulation-on-bank-it-systems-and-electronic-banking-services/; Chambers and Parnters, 2022 TMT Guide - Turkey Law and Practice (March 16, 2022), at https://www.morogluarseven.com/news-and-publications/chambers-and-partners-tmt-2022-guide-law-and-practice-turkey-chapter/; Google Cloud Services, Turkey BRSA - Regulation on Banks’ Information Systems and Electronic Banking Services (2025) at https://services.google.com/fh/files/misc/brsa_is_regulation_googleworkspace_compliancemapping.pdf; BTS and Partners, Long-Awaited Regulation On Information Systems Of Banks And Electronic Banking Services Has Finally Arrived (March 27, 2020) at https://www.bts-legal.com/insights/publications/long-awaited-regulation-on-information-systems-of-banks-and-electronic-banking-services-has-finally-arrived/

[112] Digital Policy Alert, Turkiye - Implemented Communiqué on the Management and Supervision of the IT Systems of Payment and Electronic Money Institutions and Data Sharing Services of Payment Service Providers in Payment Services Area (Dec. 1, 2021), at https://digitalpolicyalert.org/event/3560-implemented-communique-on-the-management-and-supervision-of-the-it-systems-of-payment-and-electronic-money-institutions-and-data-sharing-services-of-payment-service-providers-in-payment-services-area; Herguner Law Firm, Amendments to Payment Services Regulation (Oct. 7, 2023) at https://herguner.av.tr/en/amendments-to-payment-services-regulation/; CMS Law, Turkey's Central Bank adopts new secondary legislation on payment services and e-money (Feb. 9, 2022), at https://cms-lawnow.com/en/ealerts/2022/02/turkey-s-central-bank-adopts-new-secondary-legislation-on-payment-services-and-e-money; Esin Attorney Partnership, New Rules for Data Sharing Services of Payment Services (Oct. 13, 2023), at https://www.esin.av.tr/2023/10/13/new-rules-for-data-sharing-services-of-payment-services/

[113] CMS Law, Data localisation requirements in Turkiye (Jan. 24, 2023) at https://cms-lawnow.com/en/ealerts/2023/01/data-localisation-requirements-in-turkiye

[114] Moroglu Arseven Firm, Turkey Announces the Regulation on Internal Systems in Insurance and Private Pension Sectors (Feb. 1, 2022), at https://www.morogluarseven.com/news-and-publications/turkey-announces-the-regulation-on-internal-systems-in-insurance-and-private-pension-sectors/

[115] See Eisin Attorney Partnership, New IT Regulations by CMB (March 26, 2025) at https://www.esin.av.tr/2025/03/26/new-it-regulations-by-cmb/; See also, https://spk.gov.tr/data/636df0c51b41c61a944eb99a/Bilgi%20Sistemleri%20Y%C3%B6netimi%20Tebligi.pdf; https://spl.com.tr/wp-content/uploads/2025/03/Bilgi-Sistemleri-Yonetimine-Iliskin-Usul-Ve-Esaslar-Tebligi-VII-128.10.pdf

[116] CMS Law, Data localisation requirements in Turkiye (Jan. 24, 2023) at https://cms-lawnow.com/en/ealerts/2023/01/data-localisation-requirements-in-turkiye

[117] CMS Law, Data localisation requirements in Turkiye (Jan. 24, 2023) at https://cms-lawnow.com/en/ealerts/2023/01/data-localisation-requirements-in-turkiye

[118] CMS Law, Data localisation requirements in Turkiye (Jan. 24, 2023) at https://cms-lawnow.com/en/ealerts/2023/01/data-localisation-requirements-in-turkiye

[119] BigID, Operationalizing UAE PDPL Compliance (July 11, 2025) at https://bigid.com/blog/operationalizing-uae-pdpl-compliance-with-bigid/

[120] US Department of Commerce, UAE Regulations Limit Cross-Border Health Data Flows (2025) at: https://www.trade.gov/market-intelligence/united-arab-emirates-regulations-limit-cross-border-health-data-flows

[121] *See e.g.,* Global Data Alliance, *Comments on Abu Dhabi Healthcare Information and Cybersecurity Standard* (2024), at: https://globaldataalliance.org/wp-content/uploads/2024/10/10162024gdaabdhealthdata.pdf The cross-border data restrictions found in the Abu Dhabi Health Cyber Standard undermine US jobs in many sectors, including those referenced above. As a result of these restrictions, US service providers will no longer be able to offer services directly to Abu Dhabi without fully localizing their operations. By blocking US market access to a growing and important market, Abu Dhabi's actions raise concerns with respect to the UAE's international commitments vis-à-vis the United States. Furthermore, these restrictions undermine the ability of Americans to benefit from healthcare or their global health insurance coverage while traveling to, or residing in, Abu Dhabi, as the restrictions would prevent providers verifying coverage eligibility with their insurers, and those persons from sharing their own health data with their doctors, clinics, or insurance providers located outside of Abu Dhabi and the UAE. The restrictions will also impact the ability to provide medical treatment to persons resident in Abu Dhabi – in part because health data from Abu Dhabi can no longer be used in research, medical device servicing, or remote healthcare delivery. Denying Abu Dhabi and UAE citizens, residents, and travelers access to international medical advances and healthcare will impose health-related costs on those persons.

[122] JMC, Data Localization - More Complex than Georgraphic Location (2024) AT https://jmb.ae/cloud-migration-secrets-revealed-what-uae-tech-leaders-dont-want-you-to-know-about-sovereign-data-

requirements/#:~:text=The%20UAE%27s%20data%20localization%20requirements,controlled%20infrastructure%20solutions

[123] Clifford Chance, Doing Business in the Middle East: Data Transfers in the UAE and the KSA (March 2025) at https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/03/doing-business-in-the-middle-east--data-transfers-in-the-uae-and-ksa.html#:~:text=Doing%20Business%20in%20the%20Middle,border%20transfers

[124] USTR, 2025 Trade Agenda (March 2025), at: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2025/march/us-trade-representative-announces-2025-trade-policy-agenda

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

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

[127] Argentina, Adopted Order 60-E/2016 approving standard contractual clauses for data transfers and list of countries providing adequate levels of data protections (2016), at https://digitalpolicyalert.org/event/13475-adopted-order-60-e2016-approving-standard-contractual-clauses-for-data-transfers-and-list-of-countries-providing-adequate-levels-of-data-protections

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

[129] *See* https://www.scribd.com/document/450730509/PISLEA

[130] 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

[131] Government of Kenya, Computer Misuse and Cybercrime Act - Critical Information Infrastructure and Cybercrime Management (2024), https://nc4.go.ke/the-computer-misuse-and-cybercrime-criticalinformation-infrastructure-and-cybercrimemanagement-regulations-2024/

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

[133] *See* Government of Kenya, Data Protection Act of 2019, at https://www.odpc.go.ke/wp-content/uploads/2024/02/TheDataProtectionAct__No24of2019.pdf

[134] Government of Kenya, Data Protection Regulations (2021) at https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf

[135] Government of Kenya, National Cloud Policy (2024), at https://ict.go.ke/sites/default/files/2024-12/Kenya%20Cloud%20Policy%20-%202024.pdf

[136] 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

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

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

[139] *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

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

[141] 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

[142] 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

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

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

[145] 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/

[146] 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

[147] *See* Ministry of Information Technology and Telecommunication, *Personal Data Protection Bill* (2023), at https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

[148] *See* MOITT, *Pakistan Cloud First Policy* (2022), at https://moitt.gov.pk/SiteImage/Misc/files/Pakistan%20Cloud%20First%20Policy-Final-25-02-2022.pdf; *See also,* https://tabadlab.com/wp-content/uploads/2022/06/Tabadlab-First-Response-Cloud-First-Policy.pdf

[149] On the one hand, Section 7.2 ("Government Cloud") defines this terms as involving infrastucture that "can only be located in Pakistan." Likewise, Section 7.3 ("Private Cloud") defines this term as "cloud infrastructure provisioned for exclusive use by a single organisation or private sector enterprise" ... "can only be located in Pakistan either on premise or off premise of the organization that owns it." On the other hand, the Policy also states that it "acknowledges the capabilities and economies of scale obtained when there are no data residency requirements in place," and notes that private sector companies "usually have the option to restrict their data to a particular geographic region." However, the policy also cautions that, "[w]ith no data residency requirement in place, the data belonging to GOP [the Government of Pakistan] may be stored outside the boundaries of Pakistan and there is a possibility that GOP loses access to its data or the data may be subject to the laws of other countries. However, whenever there are legitimate use-cases requiring cross-border data flows, then the relevant stakeholders may consult with the Cloud Office to ensure appropriate security standards and controls are in place for such data flows."

[150] State Bank of Pakistan, Framework on Outsourcing to Cloud Service Providers (2023), at sbp.org.pk/bprd/2023/C1-Annix-A.pdf

[151] DLA Piper, *Transfer of Personal Data in Pakistan* (2024), at https://www.dlapiperdataprotection.com/index.html?t=transfer&c=PK

[152] 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

[153] 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 localization 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 localization might be operationalized following the language in the published Act.

[154] 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

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

[156] 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

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

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

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

[160] *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

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

[162] *Ibid.*

[163] *Ibid.*

[164] In recent years, these trends have become even more pronounced. *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf (showing that before 2020, 5–15 percent of US employees worked remotely; as of mid-2020, more than 50 percent of US employees do); Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (Sept. 2020), https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf (showing that remote health services are expected to grow by 700 percent by 2025, and some regions have seen even more rapid growth—up to 40-fold—for non-urgent telemedicine visits).

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

[166] 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. *See e.g.,* USMCA Arts. 28.9 and 28.11.

[167] 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. *See e.g.,* USMCA Art. 28.5.

[168] 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.

See e.g., USMCA Arts. 28.7, 28.9, and 28.10.

[169] 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.

See e.g., USMCA Art. 28.13.

[170] 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)

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

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

[173] *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.")

[174] *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

[175] 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.

[176] 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.

[177] 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.

[178] To date, many countries have made, or are negotiating, such commitments under international agreements, including under the United States-Mexico-Canada Agreement (USMCA), the US-Japan Digital Trade Agreement, 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 US-Japan Digital Trade Agreement, and the WTO Joint Statement Initiative digital trade negotiations. This positive trend should continue.