GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

October 17, 2024

Ms. Laura Buffo
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, 89 Fed. Reg. 71775 (Sept. 3, 2024): Docket Number USTR–2024–0015*

Dear Ms. Buffo,

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 Global Data Alliance strongly endorses the efforts of the Office of the US Trade Representative (USTR) to facilitate digital trade and cross-border data transfers and to remove data localization mandates.

The Alliance is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. Global Data Alliance members share a deep and long-standing commitment to supporting economic development, building trust in the digital economy, and protecting personal data across regions, technologies, and business models. Alliance member companies rely on the ability to transfer data responsibly around the world to create jobs and make industries at home and abroad more competitive.

Cross-border data transfers power growth across the globe and all sectors of the economy — from farming, fisheries, and mining; to services of all types; to the manufacturing industries. Data transfers are critical for companies of all sizes — from micro, small, and medium-sized enterprises (MSMEs) to multi-national corporations (MNCs) — fostering innovation and economic development, creating jobs, and promoting productivity, safety, and environmental responsibility.

The global economy faces an increasingly challenging environment characterized by rising geopolitical tensions and divisions. Among like-minded countries, cross-border digital trade and data transfers hold the potential to ameliorate these effects. Unfortunately, some governments continue to advance policies of data mercantilism and digital protectionism that undermine this potential. 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 information and ideas, and undermining online economic opportunities to the detriment of domestic and foreign citizens, consumers, and companies alike. These trends underscore the critical importance of USTR and counterpart trade authorities sustaining and increasing their collaboration to reduce barriers to cross-border data transfers and digital trade.

**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

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.[3] Cross-border data transfers contribute trillions of dollars to global GDP[4] with growth in every industry driven by data flows and digital technology.[5]

### 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.[6] 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, as well as the European Union (EU).

### B. Benefits of Cross-Border Data Transfers

The cross-border movement of data is essential to economic response and recovery at a time of economic instability and uncertainty. 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,[7] fraud prevention,[8] 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.[9]

### 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.[10] Indeed, cross-border data transfers are critical to economic and supply chain resilience across many sectors, including:

- Agriculture,[11]
- Automotive,[12]
- Clean energy,[13]
- Finance,[14]
- Healthcare and medical technology,[15]
- Logistics,[16]
- Media,[17]
- Pharmaceuticals,[18]
- Telecommunications,[19] and
- Many other sectors.[20]

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.[21] 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,"[22] 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."[23] 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."[24]

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.[25] 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.[26] 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 data gathered from sensors embedded in 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 regulatory requirements for transparency, safety, and effectiveness.

- 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**[27]

**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 progressive SMEs are growing 8 times faster than the least progressive.
- 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 traditional industries.[28] 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[29]**

**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%.[30] 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%.[31] 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,[32] Japan,[33] New Zealand,[34] and Singapore.[35] 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;[36] the APEC Privacy Framework,[37] the APEC Privacy Recognition for Processors (PRP) system,[38] the APEC Cross Border Privacy Rules (CBPR) system,[39] the Global Cross-Border Privacy Rules Forum,[40] and the ASEAN Model Contractual Clauses.[41] 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.[42] 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.

**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.

## 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 are supportive of open markets. Consistent with prior regional and bilateral agreements among WTO members,[43] 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,[44] we urge the United States to continue to clarify that such restrictive data regulations should:

- Be necessary to achieve a legitimate public policy objective;[45]
- Not be applied in a manner that would result in arbitrary or unjustifiable discrimination or a disguised restriction on trade;[46]
- Not impose restrictions on transfers that are greater than necessary;[47]
- Not improperly discriminate among different economic sectors;[48]
- Not discriminate against other WTO member entities by modifying conditions of competition through the imposition of less favorable treatment on cross-border data transfers relative to domestic ones;[49]
- Be designed to be interoperable with other WTO members' legal frameworks to the greatest extent possible;[50] 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) the commitment to minimize trade-restrictive effects; and (4) due consideration for trading partner laws.[51]

## F. GDA's Cross-Border Data Policy Principles

The GDA has published a set of Cross-Border Data Policy Principles to help inform domestic and international policymaking in relation to measures that have an impact on cross-border data transfers.[52] The GDA respectfully submits that that US government may wish to reference these principles when evaluating the design, impact, and trade effects of relevant trading partner policies. 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

We have reproduced the Principles in more detail in the Annex to 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.

## 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.

## 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.

China has published numerous measures that require data localization or restrict data transfers including the Data Security Law, the Personal Information Protection Law, and the Cybersecurity Law, as well as numerous subsidiary measures, such as the outbound data transfer security assessment measures and (at the municipal or provincial level) various "negative lists" of data whose transfer must be restricted. Purported efforts at reform (such as the proposed Provisions on Promoting Cross-Border Data Transfers)[1] have done little to improve this situation.

While India's Digital Personal Data Protection Act does not contain onerous cross-border data transfer restrictions and localization requirements, India maintains other sectoral measures that do, such as India's Directive on Storage of Payment System Data issued by the Reserve Bank of India in 2018.[2]

In Indonesia, improper cross-border data restrictions or data localization requirements are found in the proposed implementation regulation for Indonesia's Government Regulation 71/2019, OJK Regulation 13/2020, and the draft Regulations concerning Public Scope Electronic System Operators.

Likewise, Vietnam's 2024 draft Personal Data Protection Law, its 2024 draft Data Law, its Cybersecurity Law,[3] and numerous implementing regulations and decrees, including Decree 53/2022 and Decree 72, impose improper data localization requirements or other cross-border data restrictions.[4] We have serious questions as to whether these restrictions violate Vietnam's commitments to the United States under the US-Vietnam Bilateral Trade Agreement[5] and in its WTO schedule of commitments under the General Agreement on Trade in Services (GATS).

Finally, GDA continues to monitor the application of measures in the **EU** that govern cross-border data transfers that could restrict cross-border data transfers with third countries. GDA is concerned with the final text (to be adopted formally by the EU Parliament and Council before the end of the year) on the EU

[1] http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm
[2] *Reserve Bank of India Storage of Payment System Data Directive (2018)* at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0 and *Ministry of Electronics and Information Technology Guidelines for Government Departments on Contractual Terms Related to Cloud Services* at: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.
[3] *Vietnam's 2018 Cybersecurity Law* at: https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-luat-an-ninh-mang-so-24-2018-qh14-164904-d1.html#noidung.
[4] For a list of the Vietnam's numerous data localization requirements and data transfer restrictions, please see GDA, Comments on Draft Decree superseding Decree No. 72/2013/ND-CP (Sept. 2023), at: https://www.bsa.org/files/policy-filings/09152023decree72.pdf
[5] https://vn.usembassy.gov/the-u-s-vietnam-bilateral-trade-agreement-bta-resources-for-understanding/

Health Data Space (EHDS) which mandates that Health Data Access Bodies, single data holders, and Union data access services store and process personal health electronic data within the EU for any personal data processing operations in preparation for a secondary use, such as pseudonymization and anonymization. Moreover, Articles 60, 61, 62, and 63 introduce additional restrictions on the transfers of electronic health data to third countries.

We summarize measures of concern in Brazil, China, the European Union, India, Indonesia, the Republic of Korea, and Vietnam below. Additionally, our members face challenges in Cambodia,[53] Saudi Arabia,[54] Turkey,[55] and the UAE[56] (among other economies).

### A. Brazil

We outline below issues worthy of future monitoring in Brazil's cross-border data policy landscape.

***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 a newer version was issued in late August 2021 still including server and data localization requirements that will negatively impact the procurement of cloud computing services by all federal agencies.[6] Following a consultation period, the final Guidelines continued to include the localization requirements.[7] A new Procurement Model for Software and Cloud Computing Services was published in October 2023 and became mandatory for procurement processes started after April, 2024, maintaining the localization requirements.

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

## 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.[57]

**Restrictions on Cross-Border Data Transfers**
The Government of China has put in place several 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)[8] 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).

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

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.[9]

***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.[10]

***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

[9] 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

[10] 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

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.

## B. 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." The European Strategy for Data adopted in February 2020 clearly endorses that the EU will maintain an open, but assertive approach to international data transfers and pledges that the EU will continue to address unjustified obstacles and restrictions to data transfers in bilateral discussions and international fora.

However, calls for data localization or for measures that seek to ensure EU organizations are immune from third countries' extraterritorial legislation continue to have traction at EU level and in some Member States, especially in the wake of the CJEU *Schrems II* decision and in light of the increased reliance on global digital technologies during the pandemic.

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.

The EU-US Trade and Technology Council can be an important asset to the transatlantic digital policy debate. The GDA encourages both sides to use the TTC to exchange on common priorities and seek joint outcomes on international data transfers. More particularly, authorities from the United States and the EU should work intensively to ensure the continuity of transatlantic data transfer mechanisms, and refrain from adopting policies that unnecessarily impede cross-border data transfers to one another.

***EU Standard Contractual Clauses for Data Transfers:*** The European Commission released a new set of SCCs in June 2021. It is anticipated that another SCC will be issued in late 2024 or 2025. SCCs contain general clauses that are common to all transfer scenarios, as well as tailored modules applicable to different transfer scenarios. A particular challenge with the current SCC framework is the obligation for companies to undertake detailed legal assessments for each country to which data is transferred. Paragraph 20 states that: "different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer." More detailed and consistent EU guidance on third country legal frameworks would be welcome.

***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 proposed by the European Commission and the European Union Agency for Cybersecurity (ENISA) to remove references to sovereignty requirements from the EUCS is positive. On the other hand, the possibility that member states will be able to impose sovereignty requirements in national law on top of the technical requirements outlined (*see e.g.,* France's SecNumCloud) continue to present a challenge.[11] It will be important to ensure that, once the EUCS enters into force, any discriminatory national schemes are phased out, consistent with the EU Cybersecurity Act.

***EU Data Act:*** GDA continues to be concerned with drafting ambiguities in the draft EU Data Act relating to cross-border data transfers. We continue to recommend that the Commission clarify the ambiguity and breadth of the text of Article 27.1 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.

[11] See discussion on this point in Euractiv, Reuters.

***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.[12]

***EU Health Data Space:*** Between 2022 and 2023, the GDA published several papers regarding the European Health Data Space (EHDS).[58] 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 moved forward, the GDA will continue to monitor its implementation for the active imposition of unnecessary data transfer restrictions.

[12] 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

## C. India

### Overview/Business Environment

The commercial environment for GDA members remains challenging in India,[59] in part due to an increase in restrictive cross-border data policies. Several government authorities, including the Ministry of Electronics and Information Technology (MeitY), the Reserve Bank of India (RBI), the Department for Promotion of Industry and Internal Trade (DPIIT), and the Department of Telecommunications (DOT), have advanced policies and proposals impacting cross-border data policy matters. Growth and innovation in India are increasingly at risk due to the increase in data localization requirements. These requirements are included in various policies ranging from legacy regulations on government-owned weather data,[60] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[61] and payment processing regulations.[62] These policies undermine the economic benefits to India and Indian companies – as well as India's trading partners – of increased Indian economic engagement with global markets. These policies also jeopardize cybersecurity, privacy, innovation, and other policy imperatives in India. We discuss several relevant measures below.

#### *Personal Data Protection Bill*

In Fall 2023, India's Digital Personal Data Protection (DPDP) Act was passed as law by Parliament. As compared with data transfer provisions in the draft Bill, the provisions in the final Act are significantly improved. Nevertheless, they continue to raise significant concerns. The Act presumes that personal data may be transferred outside of India. However, the Act creates broad and vague authorities for the Central Government to restrict transfers by data fiduciaries without setting clear guardrails around those powers. This is a critical issue for companies that rely on international data transfers and require a stable, predictable legal framework that supports transfers. However, the government has indicated that this power may be used sparingly, in exceptional circumstances.

More specifically, the Central Government is given broad authority to "restrict the transfer of personal data by a data fiduciary for processing to such country or territory outside India" upon notification. (Sec. 16(1).) In addition, the Bill does not restrict other laws from restricting transfers of personal data, which could create fragmented rules for transfer across different industries. (Sec. 16(2).)

Only a small number of scenarios are clearly outside the scope of any potential data transfer restrictions, including when personal data is necessary for enforcing any legal right or clam; personal data is processed in the interest of preventing, detecting, investigating, or prosecution of an offense under Indian law, processing is in the context of a merger, or when the processing is pursuant to a contract with a non-Indian customer and relates to personal data of non-Indian residents. The Government of India is expected to conduct a public consultation on the implementing rules. The Government of India is expected to conduct a public consultation on the implementing rules. We urge the Government of India to provide some guardrails or guidelines to the cross-border data provisions of the PDPD Act in order to provide certainty to the industry.

#### *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.[13] In December, the Committee published the revised report.[14] 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.[15] Such mandatory obligations are counterproductive throughout the data ecosystem, and present additional complications if applied to "data processors," including

[13] Report by the Committee of Experts on Non-Personal Data Governance Framework, August 2020, https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf
[14] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dec 2020, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf
[15] 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

enterprise software and cloud service providers. The framework proposes additional compliance obligations for businesses by creating a new regulator in addition to the proposed Data Protection Authority (DPA) under PDP 2019 and the proposed e-commerce regulator. The mandatory data-sharing framework proposed in the NPD framework is in addition to the sharing requirements proposed in the PDP 2019, which was withdrawn by MeitY by August 2022. There is a suggestion that such provisions may be revisited in the proposed Digital India Act or through amendments to the IT Act. Such proposals can have a chilling effect on innovation and investment in the digital economy. We urge India to avoid the proposal of such measures in the future.

### *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. It is expected that a new draft policy will be released in 2020. It is likely that the revised policy will retain localization requirements.

### *Directive on Storage of Payment System Data*

In April 2018, the RBI issued the Directive on Storage of Payment System Data (Directive)[63], requiring payments firms to store data solely in India and ensure that any data processed abroad be deleted within 24 hours. (Directive), imposing data and infrastructure localization requirements that required 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."[64] "Data" is defined broadly, and the Directive is likely to affect both payment processors and their service providers.[65] The RBI directive imposed short deadlines and has required significant capital investments for companies to comply, and has seen resulted in a range of severe enforcement measures taken against certain financial service providers in 2021.

## D. Indonesia

The commercial environment in Indonesia is challenging for GDA member companies,[66] as Indonesia has developed or is developing policies that make it increasingly difficult to access the Indonesian market with digitally-enabled products and services.

***Duties on Digital Products:*** In February 2018, the Ministry of Finance (MOF) issued Regulation 17, which amended Indonesia's Harmonized Tariff Schedule (HTS) to add Chapter 99 "[s]oftware and other digital products transmitted electronically."[16] Although Chapter 99 is currently duty free, Chapter 99 effectively treats electronic transmissions as imports, to which customs requirements apply, including requirements to comply with all customs laws that attach to imports, prepare and file import declarations, and pay 10 percent value-added tax (VAT) and 2.5 percent income tax. Indonesia supplemented these provisions with a new Regulation 190, which imposes a customs tariff currently set at 0% and requires the filing of import declarations for data moving across transnational digital networks – the first such measure of its kind anywhere in the world.

***Personal Data Protection***: Indonesia has been developing a draft Personal Data Protection (PDP) Bill since 2014 and successfully enacted the PDP Bill on October 17, 2022. Based on GDA's reading of the law, it draws from several principles and aspects of the European Union's General Data Protection Regulation (GDPR), focusing on five main areas: data collection, data processing, data security, data breach, and the right for individuals to have their personal data erased. GDA's chief concerns with the law relate to potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors. The law provides for a two-year grace period for data controller and data processors to adjust their practices to comply with the law. A data protection authority that reports to the President will be set up within this period. Unfortunately, with only a short time before the Law will take 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 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 KOMINFO 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 ESPs are defined to also include public administration which goes beyond national security and intelligence data. No further clarity has been made on the circumstances by which data can be stored and processed offshore in the case of Public Scope ESP including the guidelines that KOMINFO will use when reviewing every individual data offshoring request by Private Scope ESPs. KOMINFO's implementing Regulation No. 5/2022 requires private sector ESOs to register with KOMINFO through an Online Single Submission (OSS) system or face significant penalties for non-compliance including blocking by KOMINFO. Failure to comply with government takedown orders for a potentially broad category of "prohibited electronic information" can also result in blocking.

***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.

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

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.

***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 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.

## E. Republic of Korea

### Overview/Business Environment

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.[67] Korea has a strong IT market and a mature legal system. Although the Cloud Computing Promotion Act[68] came into force on September 28, 2015, data residency, physical network separation, and other restrictive data-related requirements for industry sectors, such as government/public services, finance, healthcare, and education, hamper cross-border data transfers in these sectors.

***Cross-Border Data Transfers and Server Localization:*** It remains very difficult for commercial cloud services providers (CSPs) to offer cloud services to entities in South Korea's very broadly defined public sector. This is due to onerous certification requirements imposed by the Korea Internet Security Agency (KISA) under the Cloud Security Assurance Program (CSAP) on CSPs that provide cloud services to public sector agencies and requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data onshoring apply to healthcare sectors.[17]

Recent amendments to the CSAP in 2023 created a tiered system that classifies public sector data systems into three grades — "High", "Medium", and "Low" — depending on the sensitivity of data handled. Under these amendments, CSPs certified to manage public sector data systems at the "Low" level are not required to use physical network separation and instead may use logical network separation to keep customer workloads distinct. However, all three levels of CSAP classification will continue to require CSPs to ensure data residency and use only Korea-developed encryption algorithms (i.e., ARIA and SEED) rather than those more widely used and vetted internationally. As such, the amendments do not adequately address the technical and administrative burdens presented by CSAP, and significant barriers to providing cloud computing and related services in South Korea remain. Given the emergence of different third party security assessment requirements in Australia and Japan, it would be helpful to promote greater alignment and potentially cross-recognition of these requirements.

***Physical Network Separation:*** Although the Government of Korea is committed to promoting the adoption of cloud computing, security concerns by the National Intelligence Service (NIS) have resulted in policies requiring physical network separation. Physical network separation requirements prevent or discourage government agencies and other regulated sectors (e.g., healthcare) from adopting commercial cloud computing and related services.

In 2016, the Ministry of the Interior and Safety (MOIS) and the Ministry of Science and ICT (MIST) adopted the CSAP, announcing certain revisions in 2019.[18] Since 2016, the CSAP has contained problematic physical network separation requirements.[19] In other mature markets, physical network separation requirements are rarely applied throughout the public sector, including in workloads or institutions that handle non-sensitive (and sometimes, public) data, such as public universities. The uniformly applied physical network separation 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 multi-tenant cloud services. As described in GDA's August 2019 comments,[20] these requirements will have a negative impact on South Korea's digital ecosystem and curtail its ability to participate effectively in the global digital economy — raising the cost of providing services and inhibiting the choice of technology available to end-users and procuring entities. The costs associated with such additional infrastructure will need to be recovered, which would ultimately increase the costs for end consumers.

---

[17] On June 1 of 2020, a new certification framework that includes CSAP requirements was applied to electronic medical records. *See* Enforcement Decree of the Medical Service Act (Article 10-5: Standardization of Electronic Medical Records) (indicating that "matters subject to standardization to be determined and publicly notified by the Minister of Health and Welfare pursuant to Article 23-2 (1) of the Act shall be as follows: "2. Facilities and equipment necessary for the safe management and preservation of electronic medical records under Article 23 (2) of the Act").

[18] *See* https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939.

[19] As of the 2019 amendments, the physical network separation requirements stipulate that, "the physical location of the cloud system and data shall be restricted to in country and cloud service area for public institutions shall be physically separated from the cloud service area for private institutions."

[20] Comments available at: https://www.bsa.org/files/policy filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.

South Korea's regulatory environment for the use of cloud services in the financial services sector has improved somewhat of late. The Financial Services Commission (FSC) recently approved the use of personal credit information by public cloud services and may be considering additional measures to expand the ability to manage financial data on the public cloud. However, the FSC specifically requires that such data be maintained on servers located in South Korea.[21]

***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 certain GDA members to serve the South Korean market.

In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[22] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[23] and the Credit Information and Protection Act.[24] The primary result of the legislative package is to consolidate the legal protection and enforcement provisions for personal information primarily in the PIPA, and to elevate the Personal Information Protection Commission (PIPC) to a central government-level agency under the Prime Minister.

The PIPA has subsequently undergone further amendments. and the European Commission has issued "adequacy" recognition to South Korea. However, more work is required to reform South Korea's personal data protection regime. There should be a clearer distinction between data controllers versus 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 enhance investment and innovation in emerging technologies, like data analytics and machine learning, while ensuring that personal information is appropriately and adequately protected.

In April 2024, Korea's Personal Information Protection Committee (PIPC) published its PIPA Compliance Guidelines for Overseas Businesses (Guidelines). The Guidelines and the associated press release can be accessed at this link. In brief, the Guide is intended to make clear the legal obligations that will apply to overseas businesses under the recently revised PIPA. The Guidelines address three categories of overseas businesses: (1) overseas businesses that provide goods or services to Korea data subjects; (2) overseas businesses that process personal information of Korea data subjects in a way that affects them; and (3) overseas businesses that have a business establishment in Korean territory.

.

[21] E.g., 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.
[22] *Personal Information Protection Act* (2017). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.
[23] *Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act)* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.
[24] *Credit Information and Protection Act* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.

## F. Vietnam

Over the past several years, Vietnam has enacted, implemented, and proposed various measures that raise concerns from a cross-border data policy perspective. The enactment of the Cybersecurity Law in June 2018, and current efforts to develop implementing rules, only exacerbate the existing challenges and threaten to undermine the ability of foreign companies to operate in, or do business, with Vietnam.[69]

***Cybersecurity***

On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). The Law went into effect on January 1, 2019.

The Law raises serious concerns and will likely significantly impact the ability of many GDA members to provide software products and services in Vietnam. The breadth of the Law far exceeds cybersecurity protection and extends to a broad regulation of the Internet generally. The Law 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 Law is a significantly negative development in Vietnam's market access environment for the software sector.

On August 15, 2022, the Ministry of Public Security (MPS) published the final Decree No. 53/2022/ND-CP (Decree 53) that took effect from October 1, 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.

***Personal Data Protection Decree***

Following two rounds of public consultations on the draft PDP Decree, in September 2021, the MPS submitted their revised draft PDP Decree to the Ministry of Justice (MOJ) for internal appraisal. However, this version of the draft PDP Decree was kept strictly confidential.

With the issuance of Resolution 27 in March 2022 approving the substantive content of the latest draft PDP Decree, the MPS was assigned to consult the National Assembly on the draft. The draft PDP Decree was expected to be passed in May 2022 following review by the National Assembly. However, this process has been delayed. GDA understands that the draft PDP Decree is still pending at the National Assembly Standing Committee because the lawmakers are waiting on the Central Politburo's comments, which has delayed its passage till now (October 2022).

The MPS has also been assigned to take charge and coordinate with the MOJ to propose the formulation of a Personal Data Protection Law after the PDP Decree has been passed

Based on previous iterations of the draft PDP Decree, the PDP Decree will likely impose restrictive data transfer and data localization requirements. In addition, there are also burdensome requirements for personal data processors to store data transfer history for three years, register with the Personal Data Protection Commission (PDPC) for cross-border transfers of sensitive 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 personal data processors. These obligations are not only impractical, they may also create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

***Draft Decree on Administrative Penalties in the Field of Cybersecurity***

On September 23, 2024, the MPS also released a draft Decree on Administrative Penalties in the field of Cybersecurity, to be adopted on the basis of the Cybersecurity Law. Among others the draft details a number of infractions to the draft PDP Decree. The publication of this draft Decree, which is currently open

for consultation, came as a surprise because the main PDP Decree is yet to be finalized. It does, however, provide insights in some of the key provisions under the PDP Decree such as data transfers, consent, data breach notification, etc. The latest draft was published in May 2024 and slated to take effect on June 1, 2024, but it has yet to be officially promulgated.

***Decree 72***

In July 2021, the Ministry of Information and Communications (MIC) issued a draft decree to amend both Decree No. 72/2013/ND-CP (Decree 72) on the management, provision and use of Internet services and online information and Decree No.27/2018/ND-CP (Decree 27) which amended and supplemented several articles in Decree No.72. The Decree has undergone several iterations. The latest consultation occurred in September 2023.[25] The proposed amendments aim to allow the government to tighten control over livestreaming activities that generate revenue on social networks and impose obligations on cross-border social network service providers in Vietnam.

Not only does Decree 72 reinforce the data localization requirements found in other Vietnamese laws, GDA is also particularly concerned that the scope of covered entities could potentially include enterprise service providers even though many of the intended regulations are targeted at consumer-facing entities. There is also a new chapter under Decree 72 requiring providers of data center services to register with the MIC and contains additional obligations for data service providers to develop and implement technical plans and solutions to promptly detect and prevent illegal activities. These requirements place unnecessary and impractical burdens on data center service providers who may have to re-engineer their networks to afford them access to their enterprise customers' sensitive data which would be contrary to their contractual and other legal obligations.

***Personal Data Protection Law***

On September 24, 2024, Vietnam published the draft Personal Data Protection Law. The PDPL contains a large number of new restrictions on the ability to transfer data across borders. The draft law is scheduled for enactment in May 2025, with an effective date of January 1, 2026. The draft law imposes obligations to conduct transfer impact assessments, to make impact assessments available to government authorities, and to face severe penalties (including cancellation of the authority to transfer data) for any violations. The definitional scope of "data transfer" is very broad.

- 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 the sharing of 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."

[25] https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-superseding-decree-no-722013nd-cp

## 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.[70]

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.[71] 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.[72] Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.[73] The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance.[74] Many Regional Trade Agreements (RTAs) reflect this presumption.[75]

**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;[76]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[77]
- 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;[78] and
- Include other procedural safeguards and due process.[79]

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.[80]

**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.[81]

**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[82] 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.[83]

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.[84] 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,[85] security,[86] and safety.[87] 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.[88]

[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. GDA | The Software Alliance administers the Global Data Alliance. *See* Global Data Alliance, *About the Global Data Alliance* (2020), at: https://www.globaldataalliance.org/downloads/aboutgda.pdf

[2] *See* USTR, Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report, 87 Fed. Reg. 56741 (Sept. 15, 2022), at: https://www.federalregister.gov/documents/2022/09/15/2022-19896/request-for-comments-on-significant-foreign-trade-barriers-for-the-2023-national-trade-estimate

[3] *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

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

[5] *Ibid.*

[6] 19 USC 2411 *et seq.*

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

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

[9] 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

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

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

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

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

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

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

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

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

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

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

[20] 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

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

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

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

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

[25] 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

[26] 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

[27] 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.

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

[29] 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/#:~:text=Additionally%2C%20export-

intensive%20industries%20pay%20more%2C%20on%20average%2C%20than,who%20work%20in%20manufacturing%20industries%20that%20don%E2%80%99t%20export.

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

[31] 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

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

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

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

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

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

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

[38] APEC Privacy Recognition for Processors (2021)

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

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

[41] 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.

[42] *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).

[43] 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.

[44] 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

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

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

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

[48] 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.

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

[50] *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.

[51] 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.

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

[53] *See e.g.,* Global Data Alliance, Comments on the Draft Personal Data Protection of Cambodia (Oct. 2023), at: https://globaldataalliance.org/wp-content/uploads/2023/10/10052023gdacambodiadatapro.pdf The draft Personal Data Protection Law (drafted by Ministry of Post and Telecommunications) restricts transfer of personal data outside of Cambodia in Article 22 which is not only rare for privacy laws to include but will inhibit the growth of cross border businesses that involve personal data (i.e. e-commerce, remittances) in Cambodia.

[54] *See e.g.,* Global Data Alliance, *Comments on the Draft Standard Contractual Clauses of the Kingdom of Saudi Arabia* (2024), at: https://globaldataalliance.org/wp-content/uploads/2024/08/08302024gdasasccs.pdf

[55] *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; with the latest timeline for the announcement being Q4 2024.

[56] *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.

[57] 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

[58] 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

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

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

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

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

[63] Storage of Payment System Data Directive, *op. cit.*

[64] Storage of Payment System Data Directive, *op. cit.*

[65] Storage of Payment System Data Directive, *op. cit.*

[66] *See generally*, GDA Cloud Scorecard – 2018 Indonesia Country Report, at: https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Indonesia.pdf

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

[68] *Act on the Development of Cloud Computing and Protection of its Users (Cloud Computing Promotion Act)* (2015). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#liBgcolor1

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

[70] *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

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

[72] *Ibid.*

[73] *Ibid.*

[74] With COVID-19, 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 COVID-19, 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).

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

[76] 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.

[77] 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.

[78] 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.

[79] 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.

[80] 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)

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

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

[83] *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.")

[84] *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

[85] 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.

[86] 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.

[87] 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.

[88] 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.