GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

October 29, 2020

Edward Gresser
Chair of the Trade Policy Staff Committee
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Mr. Gresser,

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 unnecessary 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.

USTR's NTE Report review process is as necessary as ever, given the impact of COVID-19 on international trade policy around the world. COVID-19 has generated unprecedented economic hardship and instability, exacerbated by the widespread imposition of border closings, export restraints, and restrictions on merchandise trade and the movement of persons.[3]

Although digital trade could help offset the impacts of these trade barriers, some governments continue to advance policies of data mercantilism and digital protectionism that increase barriers to digital trade as well. 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 global outbreak of COVID-19 presents one of the most complex challenges governments have faced in modern times. The seamless and responsible movement of information and data across borders has come to play an increasingly important role in attenuating the impacts of the pandemic.

A. Cross-Border Data Transfers and COVID-19 Response and Recovery

With many governments implementing measures to increase social distancing within populations to reduce spread of the virus, the pandemic has rapidly forced many aspects of public life to a remote environment. Continued economic vitality and employment depend increasingly upon cross-border access to software and cloud computing services. As governments around the world continue to navigate and respond to the public health crisis, policymakers should maintain a strong commitment to the cross-border data transfer policies that will foster the economic response and recovery to COVID-19.

Enterprises and workers depend upon forward-looking cross-border data policies to help advance COVID-19 response and recovery efforts. This includes, most obviously, the remote work, remote health, and remote educational software tools that have helped provide resilience and operational continuity for the organizations upon which workforces, students, and patients depend. Many other scenarios illustrate the importance of cross-border access to technology and data transfers today – from biopharmaceutical researchers engaged in vaccine development and multi-regional clinical trials, to farmers who depend upon satellite and sensor-based weather forecasting and environmental analytics to make planting and harvesting decisions. 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.[4]

The continued relevance of USTR's NTE review process is seen in the impact of COVID-19 on international trade policy around the world. COVID-19 has generated unprecedented economic hardship and instability, exacerbated by widespread border closings, export restraints, and restrictions on merchandise trade and the movement of persons. Although digital trade could help offset the impacts of these trade barriers, some governments continue to advance policies of data mercantilism and digital protectionism that increase barriers to digital trade as well. 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 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 trade authorities in other countries increasing collaboration to reduce barriers to digital trade and investment.

B. Cross-Border Data Transfers — Statistical Overview

Cross-border access to technology and seamless movement of information online are critical to overcoming today's economic challenges in the face of increasing restrictions on merchandise trade and the international movement of persons. Even before COVID-19, cross-border data transfers were estimated to contribute trillions of dollars to global GDP,[5] and 60 percent of global GDP was expected to be digitized by 2022, with growth in every industry driven by data flows and digital technology.[6] Furthermore, 75 percent of the value of data transfers reportedly accrued to traditional industries like agriculture, logistics, and manufacturing. [7] Since March 2020, the importance of data transfers has only grown. For example, before COVID-19, an estimated 5%–15% of US employees worked remotely. As of mid-2020, roughly 50% of US employees, or more, are working remotely, with many relying on cross-border access to cloud-based remote work software solutions.[8] Similarly, remote health technology solutions, often accessed across national borders via the cloud, have become indispensable to protecting populations and economies in the COVID-19 era. Expected to grow by 700% by 2025, some regions are seeing even more rapid growth – up to 40-fold – for non-urgent telemedicine visits.[9]

C. 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.[10]

We highlight below measures and policy trends of concern in several countries, including Brazil, China, India, Indonesia, South Korea, Thailand, and Vietnam, as well as the European Union (EU).

D. 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**. Among other things, the ability to move data across borders responsibly contributes to:

- A country's global connectivity and its access to the international marketplace and supply chains;
- The workforce's ability to remain productive through teleworking, virtual collaboration, and online training, as well as remotely delivered health care and other services;
- Government regulators' ability to secure company compliance with regulatory requirements, including in relation to customs and trade, transportation and logistics, financial services (e.g., anti-money laundering, anti-corruption commitments), etc.
- 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.

E. 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.[11] 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.

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%.[12] 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%.[13] 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.

F. 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**. In fact, *how* data is protected is much more important to security than *where* it is stored. Data localization requirements and limits on data transfers often undermine data security. Cross-border data transfers are often important for cybersecurity for several reasons. 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.

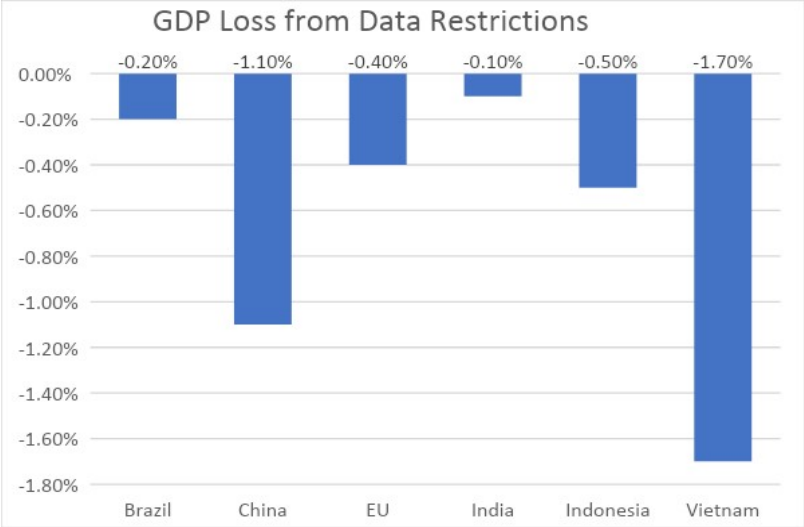
Some also argue that data localization and data transfer restrictions are necessary for **privacy** reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. This is not the case. Data localization mandates and data transfer restrictions do not increase 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 are critical to support global data flows and are built with strong safeguards. 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.[14] 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, as illustrated in the graphic below.[15]

Estimated Impact on GDP from Data Transfer Restrictions and Data Localization Mandates[16]



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 policies and depress export competitiveness.

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 Global Data Alliance 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 activity and respond effectively to the COVID-19 pandemic,
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.

Sustained attention to these issues is critical. Some markets, including **China, India, South Korea, Indonesia, and Vietnam**, have adopted, or have proposed, rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory.

Among several Chinese measures that restrict the ability to transfer data across borders, the draft 2017 Critical Information Infrastructure Protection regulations — as further elaborated in 2020 guidelines — would effectively require all cloud computing services providers (CSPs) to store data in-country.[17] China's draft Personal Information Protection Law[18] appears to contain stricter data localization requirements and data transfer restrictions than even China's 2017 Cybersecurity Law. India too has imposed data localization requirements, including through India's Directive on Storage of Payment System Data issued by the Reserve Bank of India in 2018, which imposes data and infrastructure localization requirements.[19] South Korea's Cloud Security Assurance Program (CSAP) requires use of local data centers for a broad range of cloud services.[20] The proposed implementation regulation for Indonesia's Government Regulation 71/2019 and OJK Regulation 13/2020 also contain data localization requirements. Likewise, Vietnam's 2018 Cybersecurity Law[21] and draft implementing regulations impose data localization requirements.

Additionally, **Egypt**,[22] **Nigeria**,[23] and **Pakistan**[24] have each issued measures in 2020 that raise questions and potential concerns from a cross-border data policy perspective. Although we do not address these three countries in additional detail below, it is important to continue monitoring these developments.

The Global Data Alliance also continues to monitor the application of measures in the **EU** that govern cross-border data flows, as well as the EU's bilateral and plurilateral trade negotiations and developing policies and legal jurisprudence, which could impact cross-border data flows with third countries.

We summarize measures of concern in Brazil, China, the European Union, India, Indonesia, the Republic of Korea, and Vietnam below.

A. Brazil

We outline below concerns and recommendations regarding Brazilian policies and measures impacting cross-border data flows.

Personal Data Protection Legislation. The Brazilian Congress approved the Brazilian Personal Data Protection Bill (known in Brazil as LGPD) in August 2018, and the law effectively came into force in September 2020. Legislation authorizing the creation of the Data Protection Agency (DPA) was approved in July 2019 and its structure was detailed through a Decree published in August of 2020. In October 2020, members of the DPA's Board of Directors were announced by President Bolsonaro and confirmed by the Senate. However, the DPA has yet to launch its activities as other administrative measures are still pending, including measures officially transferring the four of the five directors from their current government agencies to the DPA. The lack of an operational DPA creates legal uncertainty regarding the implementation of the Personal Data Protection Law which could, among other things, impair cross-border data flows that are critical to market access for companies selling goods and services in Brazil. One of the provisions of the LGPD that requires implementation by the DPA is the one addressing international data flows. In particular, the DPA must implement several of the most important grounds for transferring data outside Brazil, including issuing adequacy determinations, approving standard contractual clauses, and approving global corporate rules (akin to Binding Corporate Rules). To ensure legal certainty, in early September, the Global Data Alliance sent the Brazilian government a letter requesting that, until such regulations are in place, guidance be issued confirming that companies may continue to responsibly transfer data internationally based on global best practices that are consistent with the overall LGPD objectives.[25] To date, this guidance has not been issued. We encourage the US Government to continue engaging with Brazil in this important issue.

Aside from implementation concerns regarding the (currently in force) LGPD, a bill proposing modifications to Brazil's Personal Data Protection Law was introduced in the Brazilian House of Representatives in late September 2020. That bill includes new data localization requirements. Although it is unlikely this bill will move through the legislative process anytime soon, its recent introduction highlights the importance of a continued bilateral dialogue with the Government of Brazil on the harmful effects of data localization policies.

Guidelines on Government Procurement of Cloud Services. The Guidelines on Government Procurement of Cloud Services were issued in late 2018 and include server and data localization requirements that negatively impact the procurement of cloud computing services by all federal agencies. The subsequently issued final Guidelines also included these localization requirements.

National Cybersecurity Strategy. We continue to monitor ongoing discussions relating to a National Cybersecurity Strategy, which have been led by the Cabinet for Institutional Security of the Presidency of the Republic. It will be important to ensure the any future cybersecurity regulations do not create unnecessary data transfer restrictions or data localization mandates.

B. China

We outline below several concerns and recommendations regarding cross-border data policies and measures in China. Many Global Data Alliance 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.[26]

Since 2017, the Government of China has issued numerous policies and standards having a direct and restrictive impact on the ability to transfer data across borders, both into and out of China. Many – but not all – of these measures were designed to implement the Cybersecurity Law (CSL or the Law), which became effective in that same year.[27] Measures implementing the Cybersecurity Law – such as the Cybersecurity Classified Protection Scheme – may either exacerbate or mitigate those impacts, depending upon their ultimate design and construction. Even beyond China's CSL work program, there are many challenging new policies. For example, in 2020, China has announced several policies, including the Data Security Law[28], the Unreliable Entities List[29], and the Global Data Security Initiative that not only could further impede the ability of foreign companies to transfer data (including their own data) into and out of China, but also could create problematic models of restrictive cross border data policies that other countries may choose to emulate.

The Global Data Alliance supports continued efforts to improve bilateral and regional economic dialogue, including through APEC, aimed at developing workable and constructive solutions on these cross-border data policy matters.

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[30] The CSL contains significant restrictions on the ability to transfer data out of China.[31] The Cyberspace Administration of China (CAC) and other authorities continue to issue measures and standards to implement the CSL. Many of these measures leave important issues vague and unclear (e.g., the definition of critical information infrastructure (CII) or "important information"), or appear to expand the scope of the law — exacerbating the negative impact of these rules on the software industry (e.g., requiring that all personal information and important information collected in China, and not just by CII operators, must be held in-country).

Cybersecurity Classified Protection Scheme: In May 2020, China posted the final version of the Cybersecurity Classified Protection Scheme (CCPS),[32] a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL. The CCPS comes into effect on November 1, 2020. The CCPS is a continuation of the Multi-level Protection Scheme (MLPS).[33] Like the MLPS, the CCPS ranks the importance of network and information systems, based on their importance to China's national security, social order, public interests, and the interests of individuals and organizations. The CCPS also excludes access to foreign technology to the networks of moderate to high national importance, despite ambiguity regarding the definitional scope these terms.

China continues to release supporting standards and guidance on implementing the CCPS. For example, the September 22, 2020 "***Guiding Opinions on Implementing CCPS and CII Protection Scheme***"[34] which includes specific data localization mandates and data transfer restrictions, requiring that, "[p]ersonal information and important data collected and generated by the operators throughout their operation in China shall be stored in China, and where cross-border transfer is required for business reasons, such transfer shall follow relevant rules and undergo a security assessment.

***Data Security Law*:** In July 2020, China released the draft *Data Security Law of the People's Republic of China*.[35] The draft law is extremely broad and undefined, and it remains unclear how the law would interact with existing legal frameworks. The law would apply to "any entity that carries out data activities" and encompasses aspects of data security, as well as promoting data development and utilization, protecting the legitimate rights and interests of the citizens and organizations, and safeguarding China's sovereignty, security, and development interests. The Data Security Law contains provisions of concern to companies with sales or operations in China, claiming broad extraterritorial jurisdiction, outlining fines of up to 1 million yuan, criminal liability, and other undefined penalties against companies on vague grounds, including threatening harm to "national security, public interest or the legal rights of citizens or organizations of China."[36]

Personal Information Protection Law: On October 21, 2020, the National People's Congress released the first draft of the Personal Information Protection Law (**Law**). The Law appears to include stricter localization requirements and data transfer restrictions than the Cybersecurity Law of China, with key areas in the Law relevant to cross-border data transfers including:

- Mandatory security assessments: The Law states that personal operators of Critical Information Infrastructure (CII) and those processing the personal information whose volume reaches the thresholds specified by the CAC should go through the security assessment
- Local data storage requirements: Personal operators of CII and processors also must store the personal information collected and generated in China
- Residency Requirements: The Law requires overseas personal information processors to set up an office or designate a representative in China to be responsible for personal information protection-related affairs
- Extraterritoriality: the Law will be applicable to personal information processing activities that take place outside of China for the purpose of providing products or services to Chinese natural persons, or for the purpose of analyzing and evaluating the behavior of domestic natural persons
- Strict penalties: In case of an illegal act that infringes upon the rights and interests of individuals in personal information, having serious circumstances, the illegal gains shall be confiscated and a fine of no more than 50 million yuan or no more than 5 percent of the turnover in the previous year shall be imposed.

Global Data Security Initiative: On September 8, 2020, China announced its Global Data Security Initiative (GDSI)[37] as part of China's response to the "Digital Cooperation Roadmap"[38] by the Secretary-General of the United Nations on June 11, 2020, and the US Clean Networks Initiative. The GDSI espouses eight initiatives for the global digital economy system, covering cross-border data transfers and other issues. The GDSI seeks to advance a Chinese view of cross-border data policy, data governance, supply chain security, and other matters. It is currently unclear what role the GDSI will play in international negotiations, but there are concern that it might be used to advance international policies that would further restrict cross-border data transfers and support data localization mandates.

Unreliable Entities List Regulation: On September 19, 2020, China's Ministry of Commerce released the "Provisions on the Unreliable Entity List" (UEL)[39] – establishing procedures for a blacklist of foreign companies with penalties that could include restricting data transfers into or out of China, or to engage in other commercial transactions. The UEL, first proposed in May 2019, allow the Government of China to place foreign entities on an 'Unreliable Entity List' if they "endanger national sovereignty, security or development interests of China", or "suspend normal transactions with an enterprise, other organization or individual of China," or take discriminatory measures against such an entity. This can be done following an investigation or unilaterally. Once on the list, which will be public, restrictions could be placed on the activities of enterprises, organizations, and individuals in China. These include restricting import and export activities, restricting or prohibiting investment in China, banning entry or limiting travel of personnel related to the foreign entity, restricting or revoking work permits, imposing fines, and any other measures that China deems necessary. Once on the list, there is no clear process for removing an entity.

C. European Union

Over the past five years, the European Union has modernized its digital economy regulatory and policy framework relevant to electronic communications, software and data service providers, in particular with regards to telecoms, privacy, cybersecurity, data flows, and copyright.

The new European Commission has started to roll out an assertive digital policy agenda, guided by an ambition to grow Europe's "digital sovereignty." This concept is defined in various ways and with varying degrees of restrictiveness across the Commission and Member States, from "open strategic autonomy" to "technological sovereignty." The European Strategy for Data adopted in February 2020 clearly endorses that the EU will maintain an open, but assertive approach to international data flows and pledges that the EU will continue to address unjustified obstacles and restrictions to data flows in bilateral discussions and international fora. There are some calls for data localization in Europe especially in the wake of the CJEU *Schrems II* decision, such as Council declarations on the need to create an EU Cloud Federation, contributing to the emergence of projects such as GAIA-X.

Global Data Alliance 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 to the benefit of European citizens and the European economy. However, some of the measures under consideration may constitute *de facto* market access barriers, including in the areas of data privacy, cybersecurity, data governance, artificial intelligence, and cloud resilience in the financial sector (the so-called the 'Digital Operational Resilience Act' (DORA)).

As the incoming European Commission develops and implements new policy proposals, the Global Data Alliance asks that trade authorities from the United States and the EU work intensively to ensure the continuity of transatlantic data transfer mechanisms, and refrain from adopting policies that impede cross-border data transfers.

Cross-Border Data Flows: Measures that impede the flow of data across borders impose substantial burdens on companies with international operations. In the transatlantic context, some commentators have observed an unleveled playing field where data transfers to certain countries, in many cases close economic and political allies of the EU, are scrutinized or restricted, yet no similar scrutiny or restrictions are imposed on countries where data privacy, cybersecurity, and other data collection practices are much more opaque.

On July 16, the European Court of Justice ruled in the Schrems II case on the validity of Standard Contractual Clauses (SCCs). SCCs are one of the main mechanisms under EU law to legally transfer personal data from the EU to third countries, especially in the absence of an adequacy decision.

The Court decision found that:

- The use of SCCs for the transfer of personal data to recipients established in third countries is valid;
- However, controllers and processors are required to verify, on a case-by-case basis, whether the law of the third country where the recipient is based ensures an "essentially equivalent" level of protection of the personal data transferred. This assessment must take into consideration both (1) the contractual clauses / additional safeguards agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned, and (2) any laws of that country that make the recipient unable to ensure an essentially equivalent level of protection, including as regards any access by the public authorities of that third country to the personal data transferred;
- The EU-US Privacy Shield is annulled and can no longer be used for transfers to the US.

The Court decided that unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to SCCs, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country, including due to possible public authorities' access to that data.

This case has significant bearing on companies that operate in Europe and / or act as service providers for customers in Europe. Companies are awaiting guidance from European Supervisory Authorities on the nature of additional safeguards they should put in place to meet the Court's requirements. This comes amid a

revision of the SCCs by the European Commission to fully align then with the GDPR. The ruling also adds uncertainty with regards to the robustness and durability of the SCCs, a mechanism used by 90 percent of companies that transfer data internationally to some 180 countries. The complexities of the privacy framework underpinning personal data flows creates a gordian knot that trade policy should look to help detangle as quickly as possible. Therefore, a digital trade agreement should be a top priority between the two economies, including robust digital trade provisions, and complementing negotiations for an enhanced Privacy Shield that enables companies to operate on both sides of the Atlantic with trust and security, and without interruption.

Data Flows in Trade Agreements with Third Countries: In February 2018, the European Commission released data transfers provisions for trade agreements, seeking to address concerns from Member States, trading partners, and industry that EU Free Trade Agreements ("FTAs") lacked trade negotiating proposals on cross-border data transfers. This position was a positive step towards the EU endorsing binding trade commitments specifically focused on cross-border data transfers. However, it raised concerns due to its self-declaratory nature and potentially unlimited scope of exception with regards to privacy safeguards. To date, the European Commission has reportedly tabled this negotiating proposal in ongoing FTA negotiations with the UK, Australia, and New Zealand. The EU also tabled this negotiating proposal at the WTO Joint Statement Initiative talks on e-commerce.

In January 2020, a quorum of 17 Member States called for the Commission to adopt a high-level of ambition on data flows in the WTO e-commerce negotiations, even if it means diverging from the EU position as formally set by the negotiating directives. By adopting forward-looking data flows provisions, the EU would be able to retain its influence on the multilateral stage and to continue to effectively push back against localization efforts in third countries. It would also bring it closer to its main trading partners—first and foremost the United States—and address some of the friction between trade and privacy following the CJEU Schrems II case.

D. India

Overview/Business Environment

The commercial environment for Global Data Alliance members remains challenging in India,[40] 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,[41] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[42] and payment processing regulations.[43] 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: The Personal Data Protection Bill, 2019[44] (PDP 2019) was introduced to the Indian Parliament in December 2019 and, although changes have been made to the previous version of the bill, a number of serious concerns remain. These concerns include requirements to localize critical data in India; requirements to maintain copies of sensitive data in India; and a lack of clarity regarding the definition and scope of critical or sensitive data, among other issues.

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.

Non-Personal Data Governance Framework*:* On September 2019, MeitY constituted a Committee of Experts to develop a governance framework for non-personal data (NPD Framework), resulting in the issuance of a report in August 2020. The Global Data Alliance highlighted in its written comments concerns regarding the Framework's restrictions on cross-border data flows and local storage requirements. The framework would impose other 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.

Directive on Storage of Payment System Data: In April 2018, the RBI issued the Directive on Storage of Payment System Data (Directive)[45], 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."[46] "Data" is defined broadly, and the Directive is likely to affect both payment processors and their service providers.[47] The RBI directive imposed short deadlines and has required significant capital investments for companies to comply. In a recent development, the RBI, in a submission to the Personal Data Protection (PDP) Parliamentary committee, requested that financial data not be classified as Sensitive Personal Data and that RBI be exempted from the PDP bill – a move that could result in more sector-specific data regulation by RBI.

Cloud Computing: In 2019, MeitY established the Working Group on Cloud Computing (Working Group). The Working Group is tasked with formulating a framework for promoting and enabling cloud services in India. It is also tasked with examining the cybersecurity and privacy aspects related to cloud computing.[48] Unfortunately, reports indicate that the Working Group may propose broad data localization requirements for CSPs providing services both to the public and private sectors in its recommendations to MeitY.[49] The recommendations have still not been published by MeitY.

National Cybersecurity Strategy: The Government of India is also working on the National Cyber Security Strategy (NCSS) that should be released in 2020. It will be important to ensure that the initiative promotes a robust cybersecurity environment in India while refraining from limiting the ability of companies to move data across borders or restricting companies' ability to encrypt data.

E. Indonesia

The commercial environment in Indonesia is challenging for Global Data Alliance member companies,[50] as Indonesia has developed or is developing policies that make it increasingly difficult to access the Indonesian market with digitally-enabled products and services.

Regulation 71 on the Operation of Electronic Systems and Transactions: The Government of Indonesia issued Government Regulation 82 of 2012 on the Operation of Electronic Systems and Transactions (GR82) in October 2012, and two implementing regulations under GR82 in subsequent years. These imposed data and IT infrastructure localization mandates.

In October 2019, the Government of Indonesia issued Government Regulation 71 on the Operation of Electronic Systems and Transactions (GR71) to supersede and replace GR82. GR71 simplifies data categories into public and private sector data. The regulation explicitly clarifies that public sector data must be managed, stored, and processed in Indonesia, but there is no similar restriction on private sector data, which can be managed, stored, and processed anywhere, however providing scope for sectoral regulators to define sector-specific requirements, such as financial sector data. Indonesia's reflection of the broad principle in GR71 that "private electronic systems operators" may place their systems and data outside of Indonesia is a positive development. This principle is important because the procedures and protections applied to ensure privacy, security, and investigatory access are more important to achieving these three objectives than the location at which the data is stored.

While the Global Data Alliance welcomes GR71's recognition of the principle that private systems operators should be permitted to make their own determinations on optimal data storage locations, the Global Data Alliance is concerned about open-ended language in GR71 that appears to imply that specific Indonesian ministries may in the future choose to derogate from this principle in (as yet) undefined circumstances. The financial sector regulators (Bank Indonesia and OJK) have already indicated that they will continue to impose previous localization mandates with regards to private sector financial institutions that they regulate, regardless of the GR71 mandates that have otherwise called for alignment.

Implications of the changes on business operations (especially with respect to public sector customers) are still to be determined, particularly given the new e-Commerce regulation issued in November 2019, which seems to impact companies' ability to move personal data across borders (please see additional details below).

Personal Data Protection: Indonesia has been developing a draft Personal Data Protection (PDP) Bill, since 2014. The PDP Bill appears to draw from several principles and aspects of the European Union's General Data Protection Regulation (GDPR). The Global Data Alliance's concerns with the draft Bill relate to data transfer restrictions, that prohibit controllers are prohibited from transferring personal data outside of Indonesia unless one of four conditions is met: (1) the transfer is to a country or organization with a level of protection "equal or higher" than in the act, (2) there is an international agreement with the relevant country, (3) there is an agreement with the controller or a warranty that the controller will protect data in line with the act, or (4) consent of the personal data owner.

E-Commerce Regulation: In November 2019, the Government of Indonesia issued GR80, a new e-commerce regulation. This regulation reportedly contains various concerning provisions relating to physical presence and registration. Of particular concern are provisions in GR 80 that reportedly stipulate that personal data cannot be transferred offshore, unless the receiving nation is deemed by the Ministry of Trade as having the same level of personal data standards and protection as Indonesia. This requirement is overly restrictive, as it does not appear to account for other internationally recognized transfer mechanisms, including transfer pursuant to APEC CBPRS, or according to standard contractual clauses, binding corporate rules, certifications, marks, or other approaches. The measure should be amended to eliminate such provisions, or at least align with those of the draft PDP Bill.

F. Republic of Korea

Overview/Business Environment

The overall commercial environment in the Republic of Korea (Korea) for Global Data Alliance members is mixed on the subject of cross-border data transfers and data localization.[51] Korea has a strong IT market and a mature legal system. Although the Cloud Computing Promotion Act[52] 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.

Cloud Security Assurance Program: Although the Cloud Computing Promotion Act came into force on September 28, 2015, it remains very difficult for commercial cloud services providers (CSPs) to offer cloud services to entities in 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.[53] Furthermore, we understand that certain non-government entities in the healthcare and education sector are now encouraged to adopt the CSAP, which has proven impossible for foreign CSPs to become certified. Thus significant barriers to providing cloud computing and related services in Korea remain.

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.

On July 23, 2019 the Ministry of the Interior and Safety (MOIS) and the Ministry of Science and ICT (MIST) announced revisions to the CSAP.[54] The program requires 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." This requirement will have a negative impact on 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.

Regulation on Supervision of Electronic Financial Transactions: The Regulation on Supervision of Electronic Financial Transactions (RSEFT)[55] was amended on October 5, 2016 to permit the use of cloud services by financial services institutions (FSIs). The amendment allows certain data to be stored on public cloud services. 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, FSC specifically requires that such data be maintained on servers located in Korea.[56]

Personal Information Protection Regime: Korea's personal information protection (PIP) regime is one of the most restrictive in the region. In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[57] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[58] and the Credit Information and Protection Act.[59] 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. These developments may aid Korea's efforts to negotiate an "adequacy" recognition from the European Commission, but questions remain regarding the impact on cross-border data transfers.

G. 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.[60]

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). The Law, which went into effect on January 1, 2019, raises several concerns from a cross-border data policy perspective. The Government of Vietnam had indicated its intention to issue regulations implementing the Law by the end of 2019, but the implementing regulations are still pending. The latest draft of the implementing regulations was not released for public consultation and reportedly continue to contain problematic data localization requirements. Although the draft Decree allegedly did not require foreign entities to store data in Vietnam, the draft gave the government the power to impose data localization and local presence requirements on foreign entities should a company fail to comply with a request under the Law from the Ministry of Public Security (MPS). It remains particularly concerning as these requirements can be applied irrespective of whether illegality is established or a company has control over the data being used in violation, therefore posing a risk for Article 26 being triggered arbitrarily.

The draft also allegedly included a requirement for all local entities to store data locally. This is a concerning requirement that effectively enforces localization on foreign entities as a condition of doing business with local entities. These localization requirements remain a concern to the software industry at large.

[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 include BSA members and American Express, Amgen, AT&T, Citi, ITB360, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, Roche, United Airlines, Verizon, Visa, and WD-40 Company. These companies 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. BSA | 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] 85 Fed. Reg. 55925, September 10, 2020.

[3] World Trade Organization, WTO Report Finds Growing Number of Export Restrictions in Response to COVID-19 Crisis (April 2020), https://www.wto.org/english/news_e/news20_e/rese_23apr20_e.htm.

[4] *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

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

[6] *Ibid.*

[7] *Ibid.*

[8] *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf

[9] *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (Sept. 2020) https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf

[10] 19 USC 2411 *et seq.*

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

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

[13] 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

[14] *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).

[15] https://hbr.org/2017/07/60-countries-digital-competitiveness-indexed

[16] https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf

[17] *Critical Information Infrastructure Protection Regulations (Draft for Comment)*, July 11, 2017 (Chinese) at: http://www.cac.gov.cn/2017-07/11/c_1121294220.htm.

[18] The draft Law consists of 8 chapters and 70 articles and can be found here: http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808175265dd401754405c03f154c.

[19] *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.

[20] *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.

[21] *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.

[22] In July 2020, Egypt enacted its first general privacy legislation, the Data Protection Law. The Law, which limits the grounds for data transfers, is due to take full effect following the passing of Executive Regulations, expected in or before April 2021.

[23] On 19 August 2020, the Nigerian Identification Management Commission published a draft Data Protection Bill. The Bill is intended to replace the existing Data Protection Regulation, issued by the Nigerian IT Ministry in 2018. The bill does not clearly establish the legal mechanisms for cross-border data transfers, which could engender regualtory uncertainty regarding an organization's ability to transfer data across international borders.

[24] In February 2020, Pakistan published a draft Data Protection Bill which includes two potential data localization requirements and which leaves key terms (e.g., scope of "critical data") undefined. The bill requires data mirroring for all personal data and local processing of all critical personal data , and prohibits the transfer of that data abroad. *See* Global Data Alliance, *Comments to the Ministry of Information Technology and Telecommunication of the Islamic Republic of*

Pakistan on The Personal Data Protection Bill 2020 (May 15, 2020), at www.globaldataalliance.org/downloads/051420pakistanpdpbill.pdf

[25] Global Data Alliance, *Letter to Government of Brazil re LGPD Implementation and International Data Transfers* (Sept. 9, 2020), at https://www.bsa.org/files/policy-filings/09092020bsagdalgpdimplement.pdf

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

[27] *Cybersecurity Law of the People's Republic of China*, November 11, 2016 (CSL) (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm. Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[28] *Data Security Law of the People's Republic of China (Draft for Comment),* July 2020, Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/

[29] *Provisions on the Unreliable Entity List*, September 19, 2020, at: http://english.mofcom.gov.cn/article/policyrelease/questions/202009/20200903002580.shtml

[30] CSL, *op.cit.*

[31] Article 37 of the 2017 Cybersecurity Law (CSL) provides that "[c]ritical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment…". https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[32] *Cybersecurity Classified Protection Regulations (Draft for Comment)*, June 27, 2018 (CCPS) (Chinese), at: http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html?from=timeline&isappinstalled=0

[33] *Administrative Measures for the Multi-level Protection Scheme of Information Security*, June 22, 2007 (MLPS) (Chinese), at: http://www.mps.gov.cn/n2254314/n2254409/n2254431/n2254438/c3697388/content.html

[34] *Guiding Opinions on Implementing CCPS and CII Protection Scheme,* September 2020 (English) at: https://www.mps.gov.cn/n6557558/c7369310/content.html. The Guiding Opinions state in Section IV entitled "Strengthen the protection of important data and personal information", that "[o]perators shall establish and implement a security protection system for important data and personal information, make a backup of important networks and databases in critical information infrastructure for disaster recovery, adopt critical technical measures including identity authentication, access control, crypto protection, security audit, security isolation and trusted verification, to effectively protect the security of important data throughout its life cycle. Personal information and important data collected and generated by the operators throughout their operation in China shall be stored in China, and where cross-border transfer is required for business reasons, such transfer shall follow relevant rules and undergo a security assessment."

[35] *Data Security Law of the People's Republic of China (Draft for Comment),* July 2020, Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/

[36] The penalties outlined in the Law are of concern in part because of the ambiguity of the Law's provisions relating to cross-border data transfers. For example, Article 10 of the Law provides that the government shall "advance the safe and free cross-border flow of data," while Article 5 provides that the government shall "ensure the law-based, orderly, and free flow of data." The Law provides does not define what "law-based," "safe," and "orderly" mean; what specific legal requirements or restrictions apply to data transfers; what legal penalties apply to any breaches of those requirements; or what transparency and procedural fairness safeguards exist for regulated persons. Additionally, Article 33 of the Law imposes certain obligations in cases in a foreign law enforcement authority seeks access to data stored in China, and Article 31 requires entities engaged in "online data processing [to]… obtain a business operation permit or go through filing procedures," but provides few, if any, details on the substantive or procedural elements of these requirements. Article 33 of the Data Security Law provides that, "Where an overseas law enforcement agency asks for the data stored within the territory of the People's Republic of China, the relevant organization or individual shall report to the relevant competent department and obtain approval before providing it. Where the request for domestic data by a foreign law enforcement agency is prescribed in an international treaty or agreement concluded or joined by the People's Republic of China, such provisions shall apply."

[37] *Global Data Security Initiative*, September 2020, (Chinese) at: http://www.xinhuanet.com/world/2020-09/08/c_1126465834.htm .The full text of the speech at: http://www.xinhuanet.com/world/2020-09/08/c_1126466972.htm. Also reported with full Chinese language version at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative/

[38] *Digital Cooperation Roadmap*, July 21, 2020, at: https://www.un.org/en/content/digital-cooperation-roadmap/

[39] *Provisions on the Unreliable Entity List*, September 19, 2020, at: http://english.mofcom.gov.cn/article/policyrelease/questions/202009/20200903002580.shtml

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

[41] *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

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

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

[44] India *Personal Data Protection Bill (2019) at:* http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

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

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

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

[48] Data Security Council of India Annual Report 2017-2018 at https://www.dsci.in/sites/default/files/documents/resource_centre/Annual-Report-2017-18.pdf

[49] Kris Gopalakrishnan-headed panel seeks localization of cloud storage data in possible blow to Amazon, Microsoft at: https://tech.economictimes.indiatimes.com/news/corporate/kris-gopalakrishnan-headed-panel-seeks-localisation-of-cloud-storage-data-in-possible-blow-to-amazon-microsoft/65278052

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

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

[52] *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

[53] E.g., under the Enforcement Decree of the Medical Service Act (Article 10-5: Standardization of Electronic Medical Records). 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;"

[54] As announced at: https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939

[55] *Regulation on Supervision of Electronic Financial Activities (RSEFT).* http://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B0%90%EB%8F%85%EA%B7%9C%EC%A0%95

[56] 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.

[57] *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

[58] *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

[59] *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

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