GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

October 26, 2021

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

Re: Request for Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers 86 Fed. Reg. 51436 (Sept. 15, 2021): Docket Number USTR–2021–0016

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.[3]

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 continuing imposition of restrictions on merchandise trade and the movement of persons.[4]

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.

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.[5]

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,[6] 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.[7] Furthermore, 75 percent of the value of data transfers reportedly accrued to traditional industries like agriculture, logistics, and manufacturing. [8] 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.[9] 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.[10]

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.[11]

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 access to the international marketplace and supply chains, including through improved global connectivity via satellite and terrestrial cabling, wireless technologies, and emerging telecommunication technologies (such as 5G, 6G, and low-earth orbit satellites);[12]
- The workforce's ability to remain productive through teleworking, virtual collaboration, and online training, as well as remotely delivered health care and other services;[13]
- 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, terrorist financing, etc.);[14]
- The ability of companies of all sizes to access key technologies in the cloud and across national borders to innovate,[15] 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.[16]
    - 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 feedback – 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.[17]
    - 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.[18]
    - 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)**.[19] In fact, it has been estimated that 75% of the value of data transfers accrues to traditional industries.[20] 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%.[21] 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%.[22] 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**.[23] 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, 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. The OECD's Trusted Government Access workstream and similar initiative also promise to promote greater international coherence in this area.

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, in fact, economic growth benefits from an increase — not a decrease — in connectivity. 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.

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. 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.[24] South Korea's Cloud Security Assurance Program (CSAP) requires use of local data centers for a broad range of cloud services.[25] 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[26] and draft implementing regulations impose improper data localization requirements. These guidelines raise significant market access concerns for companies offering software, IT, and data services overseas.

Among others, **Bangladesh,**[27] **Egypt**,[28] **Nigeria**,[29] **Pakistan,**[30] **Saudi Arabia,**[31] and **South Africa**[32] have also issued measures or proposals that raise questions and potential concerns from a cross-border data policy perspective. Finally, we continue 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 dramatically restrict 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 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 nominated by President Bolsonaro. The DPA has consistently followed its proposed workplan, holding public consultations and hearings on draft regulations. However, the lack of sufficient staff and budget 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. A key LGPD provision that still requires implementation by the DPA addresses international data flows and the DPA intends to start discussing the matter throughout the first semester of 2022. 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 2020, 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.[33] To date, this guidance has not been issued yet it is still being considered by the DPA. 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, its recent introduction highlights the importance of a continued bilateral dialogue with the Government of Brazil on the harmful effects of data localization policies.

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.[34] The latest version of the Guidelines adequate the language to the Data Protection Law (LGPD) and add new concepts such as "cloud broker". GDA submitted comments on first draft guidelines urging Brazil to remove the localization requirements. However, Brazil did not adopt these recommendations, and the final Guidelines include the localization requirements.[35]

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 (GSI). It will be important to ensure the any future cybersecurity regulations do not create unnecessary data transfer restrictions or data localization mandates. Members of Congress have been pressuring the Executive to promptly submit a specific bill dealing with cybersecurity after a GSI representative stated that such a bill was supposed to have been proposed in 2020 in conjunction with the National Information Security Policy, yet remains under revision.

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.[36] 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.

***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 Data Security Law (DSL), the Cyberspace Administration of China and sectoral regulators such as the Ministry of Industry and Information Technology are already developing draft guidelines to establish the requisite frameworks for data categorization and classification under the DSL The implementing rules and guidelines for DSL have been identified as a work item under the State Council's 2021 Legislative Work Plan. As China begins work 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.

***Cybersecurity Review Measures*:** On July 10, the Cyberspace Administration of China ("CAC") published the draft Cybersecurity Review Measures ("Measures") for public consultation. The proposed amendments are primarily targeted at Chinese technology companies seeking an overseas IPO listing. The draft Measures has expanded its scope to require both Critical Information Infrastructure operators as well as data processors to go through a cybersecurity review. Among the new risk assessment criteria proposed in the draft Measures, they include:

- data security risks involving core data, important data, or a large amount of personal information being stolen, disclosed, destroyed, or illegally used or transferred across borders;
- critical information infrastructure, core data, important data, or a large amount of personal information will be affected, controlled, or maliciously used by foreign governments after listing abroad

***Personal Information Protection Law*:** On August 20, the National People's Congress of the PRC (NPC) officially released the approved version of the Personal Information Protection Law ("**PIPL**") which will take 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); and

(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).

(7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43)

32 global associations raised these concerns in a letter submitted to China during the drafting process, but the concerns were not addressed.[37]

***Internet Medical and Health Information Security Management Specifications*:** The National Health Commission of the People's Republic of China has released a draft measures on Internet Medical and Health Information Security Management Specifications (国家卫生健康委统计信息中心关于征求《互联网医疗健康信息安全管理规范（征求意见稿）》标准意见). These draft measures contain data localization provisions modelled on the Data Security Law and draft Personal Information Protection Law. Similar to the approach taken in the Automotive Data Management Regulations, the measure requires storage of personal and important data in China, as follows:

> Personal information and important data collected and generated during the process and operation of Internet health care services should be stored in China. If, due to business needs, it is necessary to provide it abroad, a safety assessment shall be conducted in accordance with the methods formulated by the State Internet And Communications Department in conjunction with the relevant departments of the State Council, but if otherwise provided by laws and administrative regulations, it shall be administered in accordance with the relevant provisions.

***Automotive Data Management Rules; Connected Vehicle Data Security Requirements; Internet of Vehicles Data Rules*:** China has issued a range of restrictive data rules affecting the automotive sector. For example, the *Data Management Rules for Automotive Applications*, which became effective on October 1, 2021, require operators (e.g., automotive OEMs, etc.) to store personal data and important data in China. If strictly necessary, the operator may seek an exception from this rule based on an official approval for such transfer following a cross-border transfer security assessment conducted by government authorities. (ADMR, Art. 12). Operators are subject to strict legal obligations in connection with any transfer (supervising foreign data recipients; legal liability; data type, scope, use, and process limitations; governmental reporting requirements, etc.) (ADMR, Arts. 13-19). Similarly, under the *Connected Vehicle Data Security Requirements*, there is a strict prohibition of any cross-border transfer of Data relating to roads, buildings, topography, traffic participants, among others, and the vehicle location and track data, collected by a connected vehicle from the environment outside the vehicles through cameras, radar and other sensors (CVSDR, Art. 7.1). Lastly, under the *Notice on Strengthening Internet of Vehicle (IoV) Cybersecurity and Data Security, which are intended* to support the implementation of the *New Energy Vehicle Industry Development Plan (2021-2035)*, ICV manufacturing enterprises and IoV service platform operation enterprises are required to conduct a cross border data transfer security assessment if they wish to provide important data abroad.

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[38] 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. Broadly speaking, the impact of the CSL and related data regulations is to require that

important information and personal information collected in China (by CII operators and others) must be held in-country.

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 US service providers and negatively impact US jobs. European authorities are historically focused on data transfers to the United States. The Commission has recently applied similar levels of scrutiny to the United Kingdom and the Republic of South Korea as both Third Countries sought an adequacy decision, but has not yet done so to data transfers relating to other markets such as China or Russia. It also has yet to evaluate existing adequacy decisions granted to markets including Canada, Argentina, Israel and Uruguay.

On July 16, 2020, the European Court of Justice in the Schrems II case invalided the EU-US Privacy Shield agreement. The Court also confirmed the validity of Standard Contractual Clauses (SCCs) which remain 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. However, the Court also ruled that 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.

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.

In addition, the European Commission released a new set of SCCs in June 2021. The new set of SCCs contains general clauses that will be common to all future SCCs and in addition to the general clauses, controllers and processors should select between four different modules the most applicable to their situation. This is meant to allow the parties to tailor their obligations under the standard contractual clauses to their corresponding role and responsibilities in relation to the data processing at issue. The final SCCs anticipate that companies will assess the laws of the country to which data is transferred – and now specify that both the laws and "practices" of that country are relevant to such an assessment. Notably, the SCC implementing decision recognizes that companies may consider the absence of government access requests in their sector and their own practical experience in making these assessments. 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."

The final SCCs also make two meaningful changes on government access concerns by: (1) narrowing the circumstances in which notification to supervisory authorities is required, and (2) deleting the draft language that would have required companies to "exhaust all available remedies" to challenge a request.

Nevertheless, the implications of the Schrems II ruling continue to significant bearing on US companies that operate in Europe and / or act as service providers for customers in Europe. The ruling has added significant 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. This uncertainty renders the conclusion of the negotiations of an enhance Privacy Agreement paramount to ensuring data can continue to flow across the Atlantic.

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. Once an agreement on an enhanced Privacy Shield is reached, the TTC should aim to formally incorporate aspects of international data transfers into its current discussions. Data transfers are critical to the success of many of the priorities set by the EU and the US in their respective policy agenda and to the TTC priorities.

Data Flows in Trade Agreements with Third Countries: In February 2018, the European Commission released data flows provisions for trade agreements, seeking to address concerns from Member States, trading partners, and industry that EU Free Trade Agreements ("FTAs") suffer from a lack of language on the free flow of data. This position is a positive step towards the EU endorsing binding trade commitments specifically focused on cross-border data transfers. However, it raises concerns due to its self-declaratory nature and potentially unlimited scope of exception with regards to privacy safeguards. At present the European Commission tabled this proposal in ongoing FTA negotiations with Australia and New Zealand, in which it is confronted to more advanced CP-TPP data flows provisions. The EU also tabled its language at the WTO Joint Statement Initiative talks on e-commerce.

In January 2021, the EU reached an agreement with the UK on digital trade provisions in the Trade and Cooperation Agreement governing EU-UK trade post-Brexit. The agreement translates for the first time in a trade agreement the EU's commitment to ensuring cross-border data flows to facilitate trade in the digital economy. While the agreed upon language on public policy exception remains further apart from more progressive provisions in USMCA or CP-TPP, it is considered by the European trade community as a positive step forward. Indeed, throughout 2020, several groups of Member States have repeatedly called on 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. Similar letters have also called for an "open strategic autonomy" posture that preserves internal data flows in order to support the bloc's digital growth ambitions. 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,[39] 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,[40] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[41] and payment processing regulations.[42] 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[43] (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)[44], 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."[45] "Data" is defined broadly, and the Directive is likely to affect both payment processors and their service providers.[46] 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.

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.[47] 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.[48] 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,[49] 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.[50] Korea has a strong IT market and a mature legal system. Although the Cloud Computing Promotion Act[51] 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 Flows and Server Localization: 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 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.[52] 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 South Korea remain.

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.[53] Since 2016, the CSAP has contained problematic physical network separation requirements.[54] As described in BSA's August 2019 comments,[55] 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.

South Korea's regulatory environment for 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.[56]

Personal Information Protection Regime: South Korea's personal information protection regime is one of the most stringent 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.

The PIPA is currently undergoing another round of amendments. In September 2021, a revised PIPA Bill was approved by the State Cabinet, and it is now waiting to be tabled at the National Assembly. The amendments aim to move South Korea's personal information protection regime closer to that of EU's General Data Protection Regulation and may aid South Korea's efforts in attaining an "adequacy" recognition from the European Commission. 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.

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 went into effect on January 1, 2019.

The scope 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.

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 continued to have concerning 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 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.

***Personal Data Protection Decree*:** It is reported that Vietnam's Ministry of Public Security (MPS) has submitted its revised draft Decree on Personal Data Protection (PDP Decree) to the Ministry of Justice (MOJ) for internal appraisal. This current version of the draft Decree is kept strictly confidential during the internal appraisal and no copy of it is available. There are speculations that the MPS/MOJ may be able to submit the draft PDPD to the Prime Minister's Office for their review by the **end of September / early October**. The current targeted timeline for the draft Decree on Personal Data Protection to take effect is in **December 2021**.

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 additional 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, 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 PDPD. The publication of this draft Decree, which is currently open for consultation, came as a surprise because the main PDPD is yet to be finalized. It does, however, provide insights in some of the key provisions under the PDPD such as data transfers, consent, data breach notification, etc. This draft Decree is expected to take effect in December 2021.

MIC Decisions 1145 and 783: In 2020, under the auspices of Vietnam's National Digital Transformation Strategy by 2025, the Ministry of Information and Communications (MIC) issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, for state agencies and smart cities

projects. These measures may create a preferential framework for domestic cloud service providers , and measures currently characterized as “voluntary” will be treated as *de facto* requirements.

Decree 72: On July 6, 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 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, there is also a particular concern that the scope of covered entities could potentially sweep in enterprise service providers. 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.

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

[2] 86 Fed. Reg. 51436 (Sept. 15, 2021), https://www.govinfo.gov/content/pkg/FR-2021-09-15/pdf/2021-19934.pdf

[3] *See* Global Data Alliance, *Cross-Border Data Transfers & Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021), https://globaldataalliance.org/downloads/05062021econdevelopments1.pdf

[4] 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.

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

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

[7] *Ibid.*

[8] *Ibid.*

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

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

[11] 19 USC 2411 *et seq.*
[12] *See* Global Data Alliance, *Cross-Border Data Transfers & Telecommunications and Network Technologies* (2021) https://globaldataalliance.org/downloads/10042021cbdttelecom.pdf

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

[14] *See* Global Data Alliance, *Cross-border Data Policy Principles* (2021) https://globaldataalliance.org/downloads/03022021gdacrossborderdatapolicyprinciples.pdf

[15] *See* Global Data Alliance, *Cross-border Data Transfers & Innovation* (2021) https://globaldataalliance.org/downloads/04012021cbdtinnovation.pdf

[16] *See* Global Data Alliance, *Cross-Border Data Transfers & Biopharmaceutical R&D* https://globaldataalliance.org/downloads/09092021cbdtbiopharma.pdf

[17] *See* Global Data Alliance, *Cross-Border Data Transfers & Supply Chain Management* (2021) https://globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf

[18] *See* Global Data Alliance, *Cross-Border Data Transfers & Supply Chain Management* (2021) https://globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf

[19] *See* Global Data Alliance, *Cross-Border Data Transfers & Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021), https://globaldataalliance.org/downloads/05062021econdevelopments1.pdf

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

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

[22] 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
[23] *See* Global Data Alliance, *Cross-border Data Transfers & Innovation* (2021) https://globaldataalliance.org/downloads/04012021cbdtinnovation.pdf

[24] *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.

[25] *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.

[26] *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.

[27] *See* Global Data Alliance, *GDA Comments on Bangladesh Draft Cloud Computing Policy,* May 12, 2021, at: https://www.globaldataalliance.org/downloads/05122021gdabdcloudpol.pdf

[28] 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.

[29] 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.

[30] 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

[31] On September 24, 2021, Saudi Arabia published a new Personal Data Privacy Law (PDPL), which will become effective March 23, 2022. Companies must bring themselves into compliance by March 2023. Article 29 of the PDPL reportedly contains strict cross-border data restrictions – namely that "except in cases of extreme necessity relating to a threat to the life of the data subject, controllers may not transfer personal data outside the Kingdom unless the transfer is required to comply with an agreement to which the Kingdom is party, to serve Saudi interests, or for other purposes set out in the executive regulations, provided that a series of strict conditions set in Articles 29(1)-(4) are met. *See generally,* OneTrust Data Guidance, Saudi Arabia: New Personal Data Protection Law – What you need to know (Sept. 2021), at: https://www.dataguidance.com/opinion/saudi-arabia-new-personal-data-protection-law-%E2%80%93-what

[32] *See* Global Data Alliance, Comments to the Republic of South Africa on The Proposed Data and Cloud Policy (April 2021), at: https://www.globaldataalliance.org/downloads/05122021gdasafrdatacloud.pdf

[33] 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
[34] https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684

[35] *See* BSA, *Cloud Procurement Comments*, https://www.bsa.org/~/media/Files/Policy/Filings/CommentsBSA_CloudProcurement.pdf.

[36] 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
[37] 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

[38] CSL, *op.cit.*

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

[40] *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

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

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

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

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

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

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

[47] 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

[48] 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

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

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

[51] *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

[5252] 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").

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

[54] 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."

[55] *See* BSA | The Software Alliance, *Comments on Korea Cloud Security Assurance Program*, https://www.bsa.org/files/policy filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.

[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/