GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

October 28, 2022

Mr. William Shpiece
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 on Significant Foreign Trade Barriers for the National Trade Estimate Report, 87 Fed. Reg. 56741 (Sept. 15, 2022): Docket Number USTR–2022–0013

Dear Mr. Shpiece,

The Global Data Alliance[1] provides the following information in response to your request[2] for written submissions to the Trade Policy Staff Committee (TPSC) regarding significant trade barriers for inclusion in the National Trade Estimate on Foreign Trade Barriers (NTE Report). The Global Data Alliance strongly endorses the efforts of the Office of the US Trade Representative (USTR) to facilitate digital trade and cross-border data transfers and to remove data localization mandates.

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

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

[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), at: https://www.globaldataalliance.org/downloads/aboutgda.pdf

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

The global economy faces an increasingly challenging environment, which includes the ongoing effects of the COVID-19 pandemic and the war in Ukraine. Among like-minded countries, cross-border digital trade and data transfers hold the potential to ameliorate these effects. Unfortunately, some governments continue to advance policies of data mercantilism and digital protectionism that undermine this potential. Proponents of such policies have cited to broad concepts of "digital sovereignty" or "Internet sovereignty" to justify blocking the cross-border transfer of information, mandating data localization, closing digital markets, interfering with the free flow of information and ideas, and undermining online economic opportunities to the detriment of domestic and foreign citizens, consumers, and companies alike. These trends underscore the critical importance of USTR and counterpart trade authorities sustaining and increasing their collaboration to reduce barriers to cross-border data transfers and digital trade.

Sincerely yours,

Joseph Whitlock

Joseph Whitlock
Executive Director
Global Data Alliance

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

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

I. Executive Summary
- A. Cross-Border Data Policy and Emerging Global Challenges
- B. Cross-Border Data Policy — Statistical Overview
- C. NTE Statutory Criteria Relevant to Cross-Border Data Policy
- D. Economic Benefits of Cross-Border Data Transfers
- E. Economic Costs of Data Transfer Restrictions and Data Localization Mandates
- F. Policy Arguments Relating to Data Transfer Restrictions and Data Localization Mandates
- G. Cross-Border Data Policies in International Agreements
- H. The GDA Cross-Border Data Policy Principles

II. Country-by-Country Analysis
- A. Bangladesh
- B. Brazil
- C. China
- D. European Union
- E. India
- F. Indonesia
- G. Republic of Korea
- H. Saudi Arabia
- I. South Africa
- J. Vietnam

I. Executive Summary

The seamless and responsible movement of information and data across borders has come to play an increasingly important role in attenuating the impacts recent crises, from the war in Ukraine to the COVID-19 pandemic.

A. Cross-Border Data Transfers and Emerging Global Challenges

Enterprises and workers depend upon forward-looking cross-border data policies to address the emerging global challenges noted above. 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.[3]

B. Cross-Border Data Transfers — Statistical Overview

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

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,[4] 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.[5] Furthermore, 75 percent of the value of data transfers reportedly accrued to traditional industries like agriculture, logistics, and manufacturing. [6]

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. During the pandemic, roughly 50% of US employees, or more, began to work in a remote or hybrid environment, with many relying on cross-border access to cloud-based remote work software solutions.[7] 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.[8]

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.[9] In Section II below, we highlight measures and policy trends of concern in several countries, including Bangladesh, Brazil, China, India, Indonesia, Saudi Arabia, South Africa, South Korea, 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.

1. Data Transfers Support US National Policy Objectives

The ability to transfer data in a trusted and secure manner across transnational digital networks is of central importance to the national policy objectives of the United States. Data transfers support COVID-19 recovery,[10] cybersecurity,[11] fraud prevention,[12] anti-money laundering, anti-corruption, and other activities relating to the protection of health, privacy, security, safety, consumers, and the environment. They also support shared economic prosperity.[13]

---

[4] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), at https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.
[5] *Ibid.*
[6] *Ibid.*
[7] *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf
[8] *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (Sept. 2020) https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf
[9] 19 USC 2411 *et seq.*
[10] Global Data Alliance, *Cross Border Data Transfers & Remote Work* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/10052020cbdtremotework.pdf
[11] Global Data Alliance, *Cross-Border Data Transfers & Data Localization Measures* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/02112020GDAcrossborderdata.pdf
[12] Global Data Alliance, *GDA Website – Finance* (2022), https://globaldataalliance.org/sectors/finance/
[13] Global Data Alliance, *Cross-Border Data Transfers & Economic Development: Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/05062021econdevelopments1.pdf

2. Data Transfers Support US Industries Across all Sectors

75 percent of the value of data transfers accrues to companies in sectors such as manufacturing, agriculture, and logistics.[14] Indeed, cross-border data transfers are critical to economic and supply chain resilience across many sectors, including:

- Agriculture,[15]
- Automotive,[16]
- Clean energy,[17]
- Finance,[18]
- Healthcare and medical technology,[19]
- Logistics,[20]
- Media,[21]
- Pharmaceuticals,[22]
- Telecommunications,[23] and
- Many other sectors.[24]

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

3. Data Transfers Support US Innovation

Scientific and technological progress require the exchange of information and ideas across borders.[25] Many international organizations recognize the close nexus between cross-border data transfers and innovation. The G20 has underscored that the "[c]ross-border flow of data, information, ideas and knowledge generates … greater innovation,"[26] and the WTO has similarly emphasized that, "for data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies."[27] Likewise, UNCTAD has warned that barriers driven by "data nationalism" reduce "opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation."[28]

By their nature, data localization mandates and data transfer restrictions tend to impede the cross-border exchange of knowledge, technical know-how, laboratory analysis, scientific research, and

[14] Global Data Alliance, *Cross-Border Data Transfer Facts and Figures* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf
[15] Global Data Alliance, *GDA Website – Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/
[16] Global Data Alliance, *GDA Website – Automotive* (2022), at: https://globaldataalliance.org/sectors/automotive/
[17] Global Data Alliance, *GDA Website – Energy* (2022), at: https://globaldataalliance.org/sectors/energy/
[18] Global Data Alliance, *GDA Website – Finance* (2022), https://globaldataalliance.org/sectors/finance/
[19] Global Data Alliance, *GDA Website – Healthcare* (2022), https://globaldataalliance.org/sectors/healthcare/
[20] Global Data Alliance, *GDA Website – Supply Chain Logistics* (2022), https://globaldataalliance.org/sectors/supply-chain-logistics/
[21] Global Data Alliance, *GDA Website – Media and Publishing* (2022), https://globaldataalliance.org/sectors/media-publishing/
[22] Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/
[23] Global Data Alliance, *GDA Website – Telecommunications* (2022), https://globaldataalliance.org/sectors/telecommunications/
[24] Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf
[25] Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf
[26] G20, *Ministerial Statement on Trade and Digital Economy* (2019), http://www.g20.utoronto.ca/2019/2019-g20-trade.html
[27] *See Trade Policy Review of India*, Secretariat Report.
[28] UNCTAD Digital Economy Report 2021.

other information. Data localization mandates and unnecessary data transfer restrictions hurt local innovation because a country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are integral to innovation and the dissemination of technology. These include: (a) scientific, research, and other publications; (b) manufacturing data, blueprints, and other operational information; and (c) digital tools for remote work, laboratory research, and other innovation-related applications.[29] Faced with higher costs to access or exchange information and an unpredictable environment for R&D investments, local industries face increasing innovation challenges. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for R&D.

4. Data Transfers Support the US Workforce and US Small Businesses

Data transfers support the US workforce's ability to remain productive through hybrid work arrangements that involve teleworking, virtual collaboration, and online training. Data transfers also facilitate job creation by US Small and Medium-sized Enterprises (SMEs). As detailed in Box 1 below, with greater foreign market access, US SMEs estimate that they could increase sales by 15-40% and hire between 10-50 new employees each. Furthermore, access to digital tools and cross-border data transfers help small businesses reduce export costs by 82 percent and transaction times by 29 percent. As detailed in Box 2 below, US jobs that depend on data transfers are growing rapidly.

Unfortunately, many such US jobs are under increasing threat as countries erect barriers to US digitally enabled goods and services, and the workers that design, produce, and deliver them. SMEs have identified data localization mandates and divergent privacy rules as the primary barriers to their ability to export and access foreign markets. Such digital barriers hurt US workers and impede foreign market access for US exports of aircraft, vehicles and other connected devices, as well as services, that depend upon Internet-, wireless-, and satellite-based communications and other IoT functionality for their sales, operation and support.

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

Data transfers are critical at all stages of the economic value chain.[30] More specifically, the ability to move data across borders responsibly contributes to the ability of companies of all sizes to access key technologies in the cloud and across national borders to innovate, invest, create jobs, and promote productivity, workplace safety, and environmental efficiency, at every stage of the production life cycle, as summarized below.

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

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

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

[29] See Global Data Alliance, Cross-Border Data Transfers and Remote Work (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf; See Global Data Alliance, Cross-Border Data Transfers and Remote Health Services (Sept. 2020) https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf
[30] Global Data Alliance, *Global Data Alliance Infographic: Jobs in All Sectors Depend Upon Data Flows* (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf

- Regulatory Compliance: Legal compliance teams gather data from global operations to demonstrate that products and services meet regulatory requirements for transparency, safety, and effectiveness.

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

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

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

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

Box 1: Cross-Border Data Policy and US Small- and Medium-Sized Businesses[31]

Box 1

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

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

Cross-Border Data Transfers Benefit SMEs

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

Cross-Border Data Transfers Matter to SMEs

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

[31] Underlying sources for the data in Box 1 follow: OECD, SME Digitalisation to "Build Back Better", Digital for SMEs (D4SME) Policy Paper (2021), at: https://www.oecd-ilibrary.org/economics/sme-digitalisation-to-build-back-better_50193089-en; OECD, Enhancing SMEs' Resilience through Digitalisation (2021), at: https://www.oecd-ilibrary.org/economics/enhancing-smes-resilience-through-digitalisation_23bd7a26-en; US Census Bureau, Preliminary Profile of US Exporting Companies, 2022 (Nov. 4, 2021), at: https://www.census.gov/foreign-trade/Press-Release/edb/2019/2019prelimprofile.pdf; US Chamber of Commerce, Growing Small Business Exports (2021) at https://www.uschamber.com/assets/archived/images/ctec_googlereport_v7-digital-opt.pdf Other reports also bear out this critical opportunity for small businesses. See e.g., CSIS, Filling in the Indo-Pacific Economic Framework (2022) at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220126_Goodman_Indo_Pacific_Framework.pdf?eeGvHW0ue_Kn118U5mhopSjLs7DfJMaN ; ("In the Indo-Pacific region, SMEs account for 60–70 percent of employment but only 35 percent or less of direct exports, meaning there is ample room for growth.") citing: https://development.asia/explainer/how-can-asia-reignite-its-sme-growth-engine-through-trade ; https://www.apec.org/groups/som-steering-committee-on-economic-and-technical-cooperation/working-groups/small-and-

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.[32] 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.

medium-enterprises ; AlphaBeta, MicroRevolution: The New Stakeholders of Trade in APAC (2019), at: https://alphabeta.com/our-research/micro-revolution-the-new-stakeholders-of-trade-in-apac/ ; Federal Reserve Banks, Small Business Credit Survey: 2021 report on employer firms (2021), at: https://www.fedsmallbusiness.org/medialibrary/FedSmallBusiness/files/2021/2021-sbcs-employer-firms-report ; IDC, Small Business Digital Transformation: A Snapshot of Eight of the World's Leading Markets (2020) https://www.cisco.com/c/dam/en_us/solutions/small-business/resource-center/small-business-digital-transformation.pdf ; US International Trade Commission, Digital Trade in the US and Global Economies (Part II) (2014), at: https://www.usitc.gov/publications/332/pub4485.pdf A 2019 survey of US-based SMEs shows that 96% of eBay-enabled SMEs exported to an average of 16 different markets, whereas 0.9% (less than one percent) of other businesses exported to an average of 4 markets. Furthermore, eBay-enable SMEs across the United States averaged 16 different export markets. eBay, United States Small Online Business Report (May 2021), at: https://www.ebaymainstreet.com/sites/default/files/policy-papers/2021%20Small%20Online%20Business%20Report.pdf ; Center for Strategic and International Studies, What Do CPTPP Member Country Businesses Think about the CPTPP (2021), at: https://www.csis.org/analysis/what-do-cptpp-member-country-businesses-think-about-cptpp For SMEs engaged in online sales, the most important digital economy provisions were those that: (1) ensured that companies can move customer data across borders; (2) permitted companies to choose where to store their data; (3) prohibited digital customs duties; and (4) protected consumers from harmful practices, such as spam.

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

Box 2: Cross-Border Data Policy and the US Workforce[33]

Box 2

Cross-border data policy is a core aspect of US international competitiveness. In contrast to economies such as China, India, and Russia, the US economy and US workforce are not encumbered with numerous unnecessary cross-border data restrictions and data localization mandates. An agile US workforce benefits from cross-border access to knowledge, information, and technology, and from an absence of data localization mandates and unnecessary data transfer restrictions. US jobs that depend on data transfers are growing rapidly, with:

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

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

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

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

Second, data localization mandates and unreasonable data transfer restrictions **raise the costs of international trade**. Data transfers are critical to reducing the costs to local firms of exporting to other markets. One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.[34] 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%.[35] 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,

[33] Underlying sources for the data in Box 2 follow: Congressional Research Service, Digital Trade and US Trade Policy (2021) at: https://sgp.fas.org/crs/misc/R44565.pdf; BSA | The Software Alliance, Advancing a Jobs-Centric Digital Trade Policy (2021), at: https://www.bsa.org/files/policy-filings/11132021jobscentricdigitrade.pdf ; Software.org, Supporting US Through COVID (2021), at: https://software.org/wp-content/uploads/2021SoftwareJobs.pdf ; BSA | The Software Alliance, BSA Workforce Agenda (2019), at: https://www.bsa.org/policy-filings/innovation-competitiveness-opportunity-a-policy-agenda-to-build-tomorrows-workforce ; Software.org, Every Sector is a Software Sector – Manufacturing (2019), at https://software.org/wp-content/uploads/Every_Sector_Software_Manufacturing.pdf ; ransform Your Trade Website (2022) at: https://transformyourtrade.org/ ; International Trade Administration, COVID-19 Economic Recovery: An Important Moment Arrives for U.S. Exporters (May 2021), at: https://blog.trade.gov/2021/05/19/covid-19-economic-recovery-an-important-moment-arrives-for-u-s-exporters/#:~:text=Additionally%2C%20export-intensive%20industries%20pay%20more%2C%20on%20average%2C%20than,who%20work%20in%20manufacturing%20industries%20that%20don%E2%80%99t%20export.

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

[35] 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

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**. As discussed in Box 3 below, *how* data is protected is much more important to security than *where* it is stored. Companies may choose to store data at geographically diverse locations to reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.

Some also argue that data localization and data transfer restrictions are necessary for **privacy** reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. This is not the case. Data localization mandates and data transfer restrictions do not increase personal data protection. To the contrary, for a variety of reasons including, organizations that transfer data globally typically implement procedures to ensure that the data is protected even when transferred outside of the country. Different organization types and business models require the use of different transfer mechanisms that are not interchangeable. It is important that businesses be able to rely on a range of data transfer mechanisms, which may include, where relevant, adequacy decisions, certifications, codes of conduct, Binding Corporate Rules (BCRs), and Standard Contractual Clauses (SCCs). These mechanisms can help support global data transfers and can be designed with strong safeguards. These mechanisms are integrated into national laws including those of the EU,[36] Japan,[37] New Zealand,[38] and Singapore.[39] Broadly speaking, these types of mechanisms are consistent with the so-called "accountability principle," which allows personal data to be transferred across borders while maintaining standards of data protection found in the jurisdiction in which the personal data was first collected. This principle is described in the OECD Privacy Framework;[40] the APEC Privacy Framework,[41]

[36] Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj
[37] Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/
[38] Privacy Act 2020, https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
[39] Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act
[40] OECD Privacy Framework (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[41] APEC Privacy Framework (2015), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

the APEC Privacy Recognition for Processors (PRP) system,[42] the APEC Cross Border Privacy Rules (CBPR) system,[43] the Global Cross-Border Privacy Rules Forum,[44] and the ASEAN Model Contractual Clauses.[45] 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.[46] In fact, economic growth benefits from an increase — not a decrease — in connectivity. By some estimates, just over 50% of the world's population was connected to the Internet in mid-2017, and cross-border data restrictions or localization mandates (whether premised on "data sovereignty" or other grounds) serve only to limit the economic opportunities for those who are connected. Countries that unreasonably limit cross-border data transfers and impose data localization mandates isolate themselves from the global digital economy. Such self-imposed restrictions hinder economic development, reduce productivity, limits public policy options, and depress export competitiveness.

[42] APEC Privacy Recognition for Processors (2021)
[43] APEC Cross Border Privacy Rules system, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System
[44] Global Cross-Border Privacy Rules Forum (2022), https://www.commerce.gov/global-cross-border-privacy-rules-declaration
[45] ASEAN Model Contractual Clauses (2021), at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf; *See also,* Singapore Personal Data Protection Commission, Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore (2022), at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en#:~:text=The%20ASEAN%20Model%20Contractual%20Clauses%20%28ASEAN%20MCCs%29%20are,parties%20that%20protects%20the%20data%20of%20data%20subjects.

[46] *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).

Box 3: Cross-Border Data Policy and Cybersecurity

Box 3

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

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

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

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

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

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

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

G. Cross-Border Data Policies in International Agreements

The United States and its allies play an important role in ensuring that global cross-border data policies are supportive of open markets. Consistent with prior regional and bilateral agreements among WTO members,[47] we recommend that the United States continue to include cross-border data commitments in its trade negotiations relating to:

- Cross-Border Transfer of Information by Electronic Means: Across all sectors, Parties shall not prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of a business.

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

- Location of Computing Facilities: Across all sectors, Parties shall not impose requirements to use or locate computing facilities in their own territory as a condition for conducting business.
- Custom Duties: Parties shall not impose customs duties on electronic transmissions.

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

To address the cross-border impacts of any data regulations that involve incidental restrictions on data transfers,[48] we urge the United States to continue to clarify that such data regulations should:

- Be necessary to achieve a legitimate public policy objective;[49]
- Not be applied in a manner that would result in arbitrary or unjustifiable discrimination or a disguised restriction on trade;[50]
- Not impose restrictions on transfers that are greater than necessary;[51]
- Not improperly discriminate among different economic sectors;[52]
- Not discriminate against other WTO member entities by modifying conditions of competition through the imposition of less favorable treatment on cross-border data transfers relative to domestic ones;[53]
- Be designed to be interoperable with other WTO members' legal frameworks to the greatest extent possible;[54] and
- Be developed in a transparent and accountable manner.

The bulleted list above reflects longstanding tenets of international law and practice, namely: (1) the freedom to pursue necessary public policy objectives; (2) the renunciation of discrimination against non-national persons, products, services, or technologies; (3) the commitment to minimize trade-restrictive effects; and (4) due consideration for trading partner laws.[55]

H. GDA's Cross-Border Data Policy Principles

The GDA has published a set of Cross-Border Data Policy Principles to help inform domestic and international policymaking in relation to measures that have an impact on cross-border data transfers.[56] The GDA respectfully submits that that US government may wish to reference these principles when evaluating the design, impact, and trade effects of relevant trading partner policies. The principles are as follows:

---

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

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

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

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

[52] Cross-border and data localization provisions should apply to all services and financial services sectors with no exclusions, including for electronic payment services. *See e.g.,* UK-Singapore DEA Art. 8.54.1; US-Japan DTA Art. 12-13; USMCA Chapter 17.

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

[54] *See e.g.,* UK-Singapore DEA Art. 8.61.E(6); US-Japan DTA Art. 15.3; USMCA Art. 19.8.4, 19.8.6.

[55] In the WTO context, these tenets – which trace back to the 1947 General Agreement on Tariffs and Trade – now apply to all multilateral trade rules, including those relating to goods, services, investment, technical regulations, and customs procedures. In the same spirit, WTO digital trade negotiators should explicitly extend these core tenets to trade rules relating to the cross-border movement of data.

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

- Principle 1: Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders
- Principle 2: Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices
- Principle 3: Any rules impacting cross-border data transfers should be non-discriminatory
- Principle 4: Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary
- Principle 5: Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices
- Principle 6: Countries should work together to create compatible trust-based frameworks support the seamless and responsible movement of information across borders

We have reproduced the Principles in more detail in the Annex to this submission for additional reference.

I. Conclusion

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

II. Country-by-Country Analysis

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

National policies on cross-border data transfers and data localization are – alongside economic profile, level of Internet and broadband access, and level of computer literacy – important determinants of the ability of economies to sustain economic 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.[57] South Korea's Cloud Security Assurance Program (CSAP) requires use of local data centers for a broad range of cloud services.[58] 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[59] and draft 2022 implementing regulations impose improper data localization requirements. These guidelines raise significant market access concerns for companies offering software, IT, and data services overseas.

Finally, the GDA 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 dramatically restrict cross-border data flows with third countries.

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

[57] *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.
[58] *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.
[59] *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.

A. Bangladesh

Since 2020, Bangladesh has proposed several measures that contain unnecessary cross-border data restrictions and data localization mandates. We discuss two of these measures below.

Data Protection Act: Bangladesh's 2022 draft Data Protection Act contains unnecessary cross-border data restrictions and data localization mandates – covering both personal data and non-personal data.[60] In September 2022, the GDA submitted comments regarding the draft Data Protection Act.[61] The GDA made the following specific suggestions:

(a) Revise Article 42 to eliminate the requirements for exclusive storage of data in Bangladesh.

(b) Revise Article 42 to permit storage outside of Bangladesh, provided that the data is stored in a way that mitigates the risk of cybersecurity threats and consistent with Bangladesh legal standards.

(c) Amend the outright prohibition in Article 42 on "[any] other state's court, law enforcing agency or authority" having jurisdiction over, or access to, data generated in Bangladesh, so as to permit mutual legal assistance and cross-border access to evidence by Bangladeshi and foreign authorities, consistent with international law and practice.

(d) Amend the provisions in Article 43 that only recognize consent or *ad hoc* governmental approvals as a basis for transferring certain types of data, and instead recognize additional bases for international data transfers, including binding corporate rules, international trustmarks, regional certifications, and contractual arrangements.

(e) Add provisions to Article 43 to highlight the obligations of companies (both data transferor and recipient) to protect data regardless of its location of storage and recognize that the commitments reflected in these provisions are independent bases for transferring data.

(f) Focus the Act's application on personal data, rather than broad categories of non-personal data.

Draft Cloud Computing Policy: Bangladesh's 2021 Draft Cloud Computing Policy also contains unnecessary cross-border data restrictions and data localization mandates.[62] In May 2021, the GDA

[60] Under the heading, "Data Storage and Transfer Related Provisions," Chapter X of the Act states as follows:

> **42. Storage of sensitive data, user generated data and classified data.** (1) Sensitive data, user generated data and classified data shall only be stored in Bangladesh and no other state's court, law enforcing agency or authority other than the courts, law enforcing agencies or authorities of Bangladesh shall have jurisdiction over such data.
> **43**. **Provision regarding data transfer mentioned in section 42**. (1) Any data under section 42 that is specified, from time to time by general or special order, by the Government as classified data, shall not be transferred to a place or system outside Bangladesh without prior authorisation of the Government.
> (2) Notwithstanding anything contained in sub-section (1) or any other provisions of this Act-
> (a) the sensitive data of a data-subject and any other data, including user-generated data, with his consent,
> (b) for the purpose of maintaining international relations, cross-border business, immigration or any other data as specified, from time to time, by the Government, may be transferred to any state or organisation outside Bangladesh or any international organisation.
> (3) The Director General shall be notified in a manner, as may be prescribed by the rules, regarding any data transfer under this section to any other state or international organisation outside of Bangladesh

[61] GDA Comments on Draft Data Protection Act of Bangladesh, https://globaldataalliance.org/wp-content/uploads/2022/09/09072022gdabgdpa.pdf

[62] Under the heading, "Data Storage Location," the draft Cloud Computing Policy states as follows: "The primary location of cloud service provider's data storage must be in Bangladesh. Information may be allowed to be taken outside Bangladesh for back-up and retrieval purposes where the such (*sic.*) information do not have any personal, sensitive or any such information and information which is not harmful to the security and critical information infrastructure of Bangladesh. All that information should be hosted in those countries where the Government of Bangladesh has multilateral or bilateral relations for unconditional and instantaneous laws can prevail."

submitted comments on this draft policy.[63] The GDA observed that these restrictions would likely produce unintended consequences and would undermine the stated goals of the draft Cloud Computing Policy for the following reasons:

(a) Lack of definition for restricted data categories ("personal information", "sensitive information", "information that is harmful to the security and critical information infrastructure…"), with the likely result that companies will need to overclassify information into these categories.[64]

(b) Impracticability of segregating broadly construed data types from other data types, with the result that other data types (e.g., non-personal or non-sensitive data) would also need to be localized.

(c) Untested safe harbors to transfer data to foreign countries that offer "unconditional and instantaneous" data access. The draft Policy does not identify any countries that have established relations for such "unconditional and instantaneous" access.[65]

(d) Absence of any mechanisms that permit data transfers.[66]

[63] GDA Comments on Bangladesh Draft Cloud Computing Policy, https://globaldataalliance.org/wp-content/uploads/2021/07/05122021gdabdcloudpol.pdf
[64] While the processing and transfer of sensitive information across borders may require enhanced data protection measures, a broad-brush approach to restrict the data transfers of sensitive information would disrupt services and manufacturing operations in Bangladesh, including for local enterprises seeking to reach overseas markets.
[65] Please see the GDA background paper, *Cross-Border Data Transfers and Data Localization,* for a discussion of legal mechanisms that apply to cross-border governmental access to data, at: https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf
[66] Many companies that operate internationally adhere to robust and secure data transfer mechanisms, which may include, where relevant, adequacy decisions, certifications, codes of conduct, binding corporate rules (BCRs), and standard contractual clauses (SCCs). Assuming that such working mechanisms have not already been established in Bangladesh law, we would recommend eliminating the data localization mandates and data transfer restrictions from the draft Policy.

B. 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 2020, the GDA 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.[67] 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.

ANPD Regulations on International Data Transfers. In June 2022, the GDA filed comments[68] to the Brazilian Data Protection Authority (ANPD) in connection with its development of regulations on international transfers of personal data. The consultation is the first step in the ANPD's development of regulations on international data transfers under Brazil's national data protection law, the LGPD. The 20 questions on which the ANPD seeks input focus on contractual transfer mechanisms including SCCs and BCRs and on promoting convergence and interoperability. GDA's responses focuses on three main topics:

(1) Recognizing the benefits of international data transfers

(2) Promoting convergence and interoperability among contractual transfer mechanisms

(3) Practical approaches to implementing new transfer mechanisms.

The ANPD should recognize that existing contractual transfer mechanisms can satisfy the LGPD's transfer obligations, if those contracts contain sufficiently similar substantive protections as those required by the LGPD. This would allow companies to use existing contracts (i.e., EU SCCs, bespoke agreements) to support transfers from Brazil, so long as those existing contracts embody the same substantive protections required by the LGPD.

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

[67] 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

[68] GDA Response to ANPD Consultation on Data Transfers (June 2022), https://globaldataalliance.org/wp-content/uploads/2022/06/20220617BrazilBSACommentsDataTransfersEN.pdf

requirements that negatively impact the procurement of cloud computing services by all federal agencies. The subsequently issued final Guidelines also included these localization requirements.

C. China

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

China has set ambitious goals to restrict the export of data out of China, while also promoting its restrictive data policies among aligned countries. This includes initiatives such as the MIIT 14th Five-Year Big Data Industry Development Plan,[70] the Digital Service Trade Five Year Plan,[71] and its Digital Economy Five Year Plan.[72] These plans focus on issues such as "monitoring of sensitive data leakage, illegal cross-border data flow" and promoting China-style data transfer restrictions via pilot programs in other countries. China will also continue work on its draft Network Data Security Administrative Regulation[73] and the Security Assessment Measures for Cross-border Data Transfers[74] *(Translation here.*[75]*).* China will also continue to work on implementation and enforcement of the Data Security Law (DSL),[76] the Personal Information Protection Law (PIPL),[77] the Data Management Rules for Automotive Applications,[78] and the Internet Medical and Health Information Security Management Specifications[79]- all of which came into effect in the last 12-18 months. In this same timeframe, China issued the Platform Economy Opinions[80]; the June 24, 2022 *Cybersecurity Standard Practice Guideline — Specification for Security Certification of Personal Information Cross-Border Processing Activities by the National Information Security Standardization Technical Committee*; and the June 30, 2022 draft *Provisions on the Standard Contract for Personal Information Cross-Border Transfer*.

The GDA has coordinated four different global industry letters and statements on the foregoing measures: July 2022,[81] December 2021,[82] June 2021,[83] and November 2020.[84]

The GDA 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.

---

[69] 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

[70] https://wap.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2021/art_c4a16fae377f47519036b26b474123cb.html
[71] https://www.scmp.com/tech/policy/article/3153196/china-pursue-digital-trade-expansion-under-new-five-year-plan-cross
[72] https://english.www.gov.cn/policies/latestreleases/202201/12/content_WS61de9a35c6d09c94e48a385f.html
[73] http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm
[74] http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm
[75] https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/
[76] https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/
[77] https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/
[78] http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm
[79] https://mp.weixin.qq.com/s/dc7gd8ElPJzT9OD4Wp91pw
[80] https://www.chinamoneynetwork.com/2022/01/21/china-issues-new-rules-regulating-internet-giants-and-platform-economy
[81] https://globaldataalliance.org/wp-content/uploads/2022/08/en07282022gdachdftcontractprov.pdf
[82] https://globaldataalliance.org/wp-content/uploads/2021/12/12012021gdachmultiassltr.pdf
[83] https://globaldataalliance.org/wp-content/uploads/2021/07/en06022021gdachinadslpip.pdf
[84] https://globaldataalliance.org/wp-content/uploads/2021/07/en11242020chinamultiassocltr.pdf

***Data Security Law*:** The Data Security Law ("DSL"), enacted on June 1, went into effect on September 1, 2021. The DSL (a) requires the State Internet Information Department to draft rules for all "other data handlers" (i.e., not just CII operators) to restrict those other handlers' exportation of "important data"; (b) applies to "[any person] handling important data"; (c) requires the State to create a "categorical and hierarchical system for data protection" as well as "catalog of" for "important data", and to assess the "importance" of data based on broad criteria relating to: economic development, social development, national security, the public interest, and the lawful rights and interests of citizens or organizations; (d) authorizes each region and department to set a "catalog of important data" within that region and in corresponding industries and sectors; and (e) requires the State to create a "monitoring and early warning system" for important data, which will apparently help it prevent the exportation of "important data". Following the swift enactment of the DSL, the Cyberspace Administration of China and sectoral regulators such as the Ministry of Industry and Information Technology have developed 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.

***Personal Information Protection Law*:** The Personal Information Protection Law ("**PIPL**") went into effect on November 1, 2021. The PIPL raises the following concerns:

(1) data localization requirements for "personal information" (PIPL Art. 40) and highly restrictive data transfer provisions for "personal information" (PIPL Arts. 38-40);
(2) lack of definition or overbroad scope for key concepts that implicate data localization requirements and data transfer restrictions, including what constitutes a "justified need," or a "large volume [of data]" (PIPL Art 40);
(3) mandates for data assessments requiring governmental notification and/or approval in conjunction with the data localization and data transfer provisions noted above (PIPL Art. 38(1), 40);
(4) proposed data transfer "standard contracts" that, while encouraging, may not be interoperable with standard contractual clauses under the EU General Data Protection Regulation (GDPR) or other established personal data protection frameworks (PIPL, Art. 38(3));
(5) the absence from the PIPL of other internationally recognized data transfer mechanisms, such as intra-corporate binding rules, trustmarks and regional certifications (PIPL, Art. 38);
(6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established (PIPL, Art. 39); and
(7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43).

***Measures for Security Assessment of Cross-Border Data Transfers*:** On September 1, 2022, the Measures for Security Assessment of Cross-Border Data Transfers of the Cyberspace Administration of China (CAC) took effect. These security assessment measures are required only for a limited subset of companies engaging cross-border data transfers – specifically:

- A critical information infrastructure operator or a personal information processor based in China (akin to a "data controller" under the GDPR) that processes personal information for 1 million or more persons;
- A transferor of "important data";
- A processor of the personal data of more than 1 million individuals; a transferor of personal information of more than 100,000 individuals; or a transferor of sensitive personal information of more than 10,000 individuals. The latter criteria apply to the period beginning on January 1 of the preceding calendar year.

CAC also issued the Guidelines on Application of Security Assessment of Cross-border Data Transfers (First Version) on August 31, 2022.[85]

***CAC Draft Standard Contracts for Outbound Data Transfers*:** On July 28, 2022, the GDA submitted comments[86] in response to the Cyberspace Administration of China's draft Measures on Standard Contracts for the Export of Personal Information.[87] GDA recommended that the Measures should: (1) not impose greater restrictions on data transfers than necessary; (2) afford equal treatment to Chinese and foreign enterprises, services, and technologies; and (3) be administered in a uniform, impartial, and reasonable manner with a view to ensuring non-discriminatory and streamlined approvals. The GDA also recommended that the CAC seek to:

(a) Improve alignment with international best practices: China's Standard Contract Provisions should reflect international best practices, and should be revised for greater alignment and interoperability with standard contractual clauses (SCCs) under the EU General Data Protection Regulation (GDPR), such as by aligning definitions and transfer scenarios with the EU GDPR SCCs.

(b) Adopt Document Retention Requirements: Article 3 requires filing of standard contracts with CAC. To align with the international practice, we would propose that CAC instead require data controllers to retain the original agreement and produce a copy to CAC regulators upon request.

(c) Reevaluate disqualifying conditions: Article 4 conditions for disqualifying companies from using Standard Contract Provisions do not align with any known international practice, including those relating to critical information infrastructure, as well as volume limits for personal and sensitive personal data. Accordingly, we recommend that CAC (1) revise disqualifying thresholds (thresholds required for CAC security assessments are very low (representing transfers covering 0.07% [seven hundredths of 1 percent] and 0.0007% [seven 10,000ths of 1 percent] of China's population over a 12-24 month period); and (2) revise overbroad exclusions (given that China's TC260 definition of

[85] The Guidelines on Application of Security Assessment of Cross-border Data Transfers require a person making a security assessment application to prepare:

- a certified copy of its unified social credit code certificate;
- a certified copy of its legal representative's ID card;
- a Power of Attorney appointing an agent handling the application related matters – a template of this is included in the Guidelines;
- a certified copy of the appointed agent's ID card;
- a completed Application Form for Security Assessment of Cross-border Data Transfers – a template of this is included in the Guidelines;
- a certified copy of the agreements or other legal documents with the overseas data recipients. (In practice, it may be preferable to fulfill this requirement by submitting a copy of a China-approved standard contract (if and when they are published. However, the viability of this approach remains to be seen);
- a Report of Self-assessment of Risks in Cross-border Data Transfers – a template of this is included in the Guidelines (including an explanation, and risk/compliance/mitigation analyses for each transfer); and
- other supporting documents and materials

[86] GDA, Global Industry Statement on Draft China Standard Contract Provisions, https://globaldataalliance.org/wp-content/uploads/2022/08/en07282022gdachdftcontractprov.pdf

[87] Article 38 of the Personal Information Protection Law (PIPL) introduces standard contracts as a cross-border data transfer mechanism, noting that such contracts may be used only by processors that:

1. are not critical information infrastructure operators;
2. handle personal information for fewer than 1 million persons;
3. have transferred personal information for fewer than 100,000 persons since January 1 of the prior calendar year; and
4. have transferred sensitive personal information for fewer than 10,000 persons since January 1 of the prior calendar year.

Processors must file standard contracts (and Data Protection Impact Assessments) with provincial CAC authorities within 10 business days of the effective date of the contract.

Standard contracts must contain, among other things: (1) basic information on the parties, (2) the purpose, scope, category, sensitivity and volume of data transfers, (3) the respective obligations and liabilities of the transferor and transferee, (4) information on the laws of the destination country, (5) protections afforded to data subjects, and (6) provisions regarding termination, liability and dispute resolution.

Data Protection Impact Assessments must evaluate: (1) the purpose, scope, and method of processing by the processor and overseas recipient; (2) risks of leakage of personal information and whether data subjects have legal means to safeguard their rights and interests; (3) the impact of personal information protection policies and laws in the overseas country on the performance of the contract (Art 5).

"critical information infrastructure" sweep in a wide array of computing equipment typically used for ordinary and non-sensitive international business transactions)

(d) Refine transfer impact assessment procedures: Article 5 of the Standard Contract Provisions contains prescriptive review requirements relating to – among other things – the volumes, scope, sensitivity, and categories of information (categories that have not yet been clearly defined in Chinese law), as well as the laws and practices of the recipient's home country; regional or global organizations to which the country or region is a member; and binding international commitments made. It would be helpful for CAC to look for ways to streamline and rationalize these requirements, including by citing to neutral and factual legal summaries, and by developing a list of categories of low-risk data transfers for which no formal, or a less detailed assessments would be required.

(e) Clarify that parties may tailor the language of contracts to specific circumstances

***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.[88] 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

[88] CSL, *op.cit.*

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.

In September 2022, the CAC proposed several amendments to the CSL, which may create further enforcement challenges from a cross-border data policy perspective. The proposed amendments are summarized below.

- The CSL Amendments would expand the scope of regulatory enforcement actions against companies that fail to fulfill network protection obligations. Financial penalties would increase from the current RMB 1 million to RMB 50 million or 5% of the prior year's revenues.
- Critical information infrastructure operators (CIIOs) would be subject to heightened compliance obligations. If a CIIO fails to comply with data localization requirements and transfers data outside China in violation of applicable rules, it will be subject to a maximum penalty of RMB 50 million or 5% of the prior year's revenues. Its executives can be subject to a fine of up to RMB 1 million plus disqualification from senior roles.
- The CSL would require that a CIIO must only utilize network products and services that have passed the security review. If a CIIO uses network products or services that have not passed the required review, the CIIO can be penalized up to 5% of prior year revenues.

D. 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. These updates have included an intense focus on cross-border data transfers, and (regrettably) new restrictions on data transfers or new data localization mandates. Measures that impede the transfer of data across borders impose substantial burdens on EU and non-EU enterprises alike, and have a particularly negative impact on US service providers and US jobs. European authorities and civil society have historically focused on data transfers to the United States, the top destination for third-country personal data transfers from the EU, while paying less attention to personal data transfers to other jurisdictions that lack data protection safeguards or respect for personal privacy as a constitutional or human right.

GDA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, and in harnessing the value of data 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 Commission develops and puts forward new policy proposals, the GDA 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 unnecessarily impede cross-border data transfers.

EU Digital Sovereignty: The 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 for a. 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.

Schrems II Decision and Subsequent DPA Decisions: 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 *Schrems II* case led to an increase in the incidence of EU cross-border data restrictions, including through the actions of EU member state or regional Data Protection Authorities (DPAs). For example, in a September 2022 decision, the Danish DPA ordered the Aarhus municipality to cease transferring data to the United States pending certain internal changes. This decision followed the same DPA's August 2022 Helsingør decision, which imposed similar cross-border data transfer restrictions. In a separate September 2022 decision, the Danish DPA also declared that certain US-based data analytics software solutions "cannot be used legally without additional safeguards." These rulings follow other DPA rulings on the use of digital tools that implicate US-EU data transfers in: (1) Austria (Oct. 2021, April 2022), (2) Germany (Berlin DPA) (3) Denmark (July 2022, Jan. 2022) (5) France (CNIL ruling), (6) Guernsey (DPA ruling), Italy (Garante June 23 ruling), and the Netherlands (Dutch DPA statement).

A New US-EU Data Privacy Framework: In October 2022, the United States the Biden Administration issued an Executive Order (EO) on Enhancing Safeguards For United States Signals Intelligence

Activities,[89] which was first announced in March 2022.[90] The EO creates new safeguards on US signals intelligence activities, establishes a new redress mechanism, and enhances US oversight of signals intelligence. The EO will form the basis of an adequacy decision by the European Commission, which would create a successor agreement to the Privacy Shield and facilitate data transfers across the Atlantic.

EU Standard Contractual Clauses for Data Transfers: 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. The final SCCs require an assessment of both the laws and "practices" of the transfer destination country. In June 2022, the European Commission released its long-awaited Q&A document on the practical use of SCCs (both on the "Article 28 SCCs" and the "transfer SCCs").[91] Concerns remain regarding a lack of predictability in the design and administration of SCCs, including in the standards application to third country transfer impact assessments.

Cybersecurity Certification Scheme for Cloud Services (EUCS): In September 2022, three German Federal Ministries (Interior; Economics and Technology; and Transport, Building and Urban Affairs) sent a joint letter to the European Commission urging that the discussions on so-called "immunity requirements" under the EUCS should not be conducted in the standardization bodies of the European Union Agency for Cybersecurity (ENISA), but in a Council working group, as these are political and not technical issues. This is a positive development that may help address concerns regarding the ENISA's EUCS drafting process. Among those implications are the requirements on immunity of Cloud Service Providers with regard to non-EU law and sovereignty requirements (including data localisation requirement restricted to EU territory). German Ministries letter, which is also supported by Sweden, Ireland, and the Netherlands, follows extensive engagement by BSA/GDA and governments across the EU and third countries. This would have an impact on all sectors relying on cloud computing.

EU Health Data Space: In July 2022, the GDA published a White Paper regarding Cross-Border Data Transfers & the EU Health Data Space (EHDS).[92] The GDA White Paper underscores the importance of the cross-border exchange of non-personal health data to developing new biopharmaceutical treatments and improving medical outcomes for patients within the EU and beyond. The comments urged the Commission to avoid imposing in the EHDS restrictive cross-border data policies that would have far-reaching and unintended consequences. Using data localization mandates and unnecessary data transfer restrictions to isolate the EU from the global transnational biopharmaceutical and medical innovation ecosystem would not only undermine the availability of new treatments within the EU, but also EU-based biopharmaceutical research and development (R&D). Incorporating such restrictions into the EHDS could significantly curtail the capacity and readiness of EU-based biopharmaceutical enterprises to respond to emergent health risks or to participate in critical R&D related to Alzheimer's disease, cancer and other longstanding medical challenges. Similarly, such restrictions would likely directly impact the healthcare availability in the EU to

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

[90] White House, Announcement of Transatlantic Data Privacy Framework (March 2022), at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[91] On the specific aspect of use of SCCs for international data transfers, the Q&A document does not provide more information on how companies should conduct "transfer impact assessments" than the one already contained in the SCCs themselves. Moreover and unhelpfully, for the additional safeguards that should be included in the SCCs in case the parties allocate a "negative assessment" to the Third country to which the data will be transferred, the document refers to the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data as the source for practical information for additional safeguards to be included in the SCCs. On a more positive note, the Q&A document stresses that the data importer IS NOT contractually required to challenge each request for disclosure it receives from a public authority in a Third country. However, the data importer has to review whether the requests it receives are lawful under the applicable domestic legal framework. If the importer considers that there are reasonable grounds to consider the request unlawful, it should make use of the procedures available under its domestic law to challenge the request. If the data importer has challenged a request and considers that there are sufficient grounds to appeal the outcome of the procedure in first instance, such appeal should be pursued.

[92] GDA White Paper on Data Transfer Provisions of the EU Proposal for a European Health Data Space (2022), https://globaldataalliance.org/wp-content/uploads/2022/08/07282022gdaeuhealthdataspace.pdf

the extent that they would impede cross-border digital access to medical experts and professionals based in other parts of the world, and would undermine the ability to receive the benefits of data analytics and artificial intelligence (AI) technologies applied to broader transnational datasets that include EU-based data. The White Paper also includes detailed evidence and case studies regarding the importance of data transfers to cross-border: (1) biopharmaceutical R&D, (2) clinical trial processes, (3) demographic representativeness in R&D, (4) regulatory collaboration, (5) good pharmacovigilance practice, (6) healthcare diagnosis, (7) deployment of medical technologies in healthcare delivery, (8) responsible AI-based health applications, and (9) remote health services.

EU Data Act: In June 2022, the GDA published its position paper on the EU Data Act.[93] The GDA position paper recommended as follows: "To mitigate interpretative challenges for EU judicial and administrative authorities, we would recommend to clarify that Article 27.1 refers to conflicts with EU laws or EU member state laws that expressly prohibit data transfer or access. Such legislative clarification could help forestall alternative interpretations that data transfer or access must be blocked on the basis of a much wider and less defined scope of potential "conflicts" with EU law or member state law. Indeed, if data transfer or access were halted in this unpredictable and broad manner, it could raise questions regarding the EU's compliance with its international obligations and impede the future ability of EU and foreign entities to engage in cross-border commerce, R&D, and other activities."

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.

[93] GDA Position Paper on the EU Data Act Proposal (2022), https://globaldataalliance.org/wp-content/uploads/2022/07/06302022gdadataactprop.pdf

E. India

Overview/Business Environment

The commercial environment for GDA members remains challenging in India,[94] 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,[95] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[96] and payment processing regulations.[97] 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.

Digital India Act: In August 2022, the Government of India announced that it was considering developing a comprehensive set of laws that would purportedly be in "sync with today's digital economy"[98] and "make the online world more accountable".[99] To achieve these objectives, the Government of India is considering substantial revisions to the two decades old Information Technology Act, 2000, last amended in 2008.[100] This is an important opportunity to update a rapidly aging law and create a new, modern legislative framework for India. Accordingly, GDA recommends that the Government avoid the types of data localization mandates and data transfer restrictions that have been reflected in recent Indian digital policy proposals, bearing in mind that such restrictions undermine cyber- and data security, innovation, economic growth, and a wide range of other national policy priorities.

Personal Data Protection Bill: In August 2022, the Ministry of Electronics and Information Technology (MeitY) withdrew the Personal Data Bill 2019 (PDP 2019)[101] from the Indian Parliament. MeitY is expected to present a new personal data protection bill for public consultation in December 2022. Concerns with the PDP Bill 2019 include requirements to localize critical data and to maintain copies of sensitive data in India (definitions of what type of data would constitute critical or sensitive data are not provided). It is uncertain whether the new privacy bill will continue to include requirements to localize data and cross-border data transfer restrictions. In comments (dated January 2022[102] and February 2020[103]) on an earlier version of

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

[95] *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

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

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

[98] Comprehensive legal framework is in the works: Ashwini Vaishnaw accessible at: https://www.livemint.com/news/india/comprehensive-legal-framework-is-in-the-works-ashwini-vaishnaw-11659552785859.html

[99] Govt working on new Data Protection Bill, Digital India Act: IT Minister Ashwini Vaishnaw, accessible at: https://www.financialexpress.com/industry/technology/govt-working-on-new-data-protection-bill-digital-india-act-it-minister-ashwini-vaishnaw/2657315/

[100] Information Technology Act 2000, https://www.meity.gov.in/content/information-technology-act-2000

[101] *Personal Data Protection Bill, 2019,* http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[102] GDA Comments on the Joint Parliamentary Committee Report on the Personal Data Protection Bill 2019, https://globaldataalliance.org/wp-content/uploads/2022/01/01262022gdajocreport.pdf

[103] GDA Comments on Personal Data Protection Bill 2019, https://globaldataalliance.org/wp-content/uploads/2021/07/02252020IndiaGDAcmtsPDP2019.pdf

the Bill,[104] the GDA described its concerns that the Bill lacked the conceptual clarity and consistency that is crucial for the Indian digital economy to effectively integrate with the global data economy. These challenges, coupled with serious concerns about data localization, disproportionate criminal penalties, and overly rigid data classification requirements, are broken down in greater detail in those comments.

CERT-In Directions: In April 2022, the Indian Computer Emergency Response Team (CERT-In) released *'Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*' (Directions).[105] The Directions mandated many onerous obligations on cyber incident reporting including the localization of relevant data within India. CERT-In subsequently released FAQs which provided additional clarifications on some of the onerous provisions, but the Directions continue to remain a challenge to implement for companies,[106] as highlighted in prior industry comments.[107]

TRAI Data Centre Consultation: In December 2021, the Telecom Regulatory Authority of India issued a draft consultation paper entitled "Regulatory Framework for Promoting Data Economy through Establishment of Data Centres, Content Delivery Networks and Interconnect Exchanges in India" (Consultation Paper).[108] In comments dated February 2022[109], the GDA noted that the Consultation Paper endorsed a misplaced assumption around privacy and data localization — and adopted the view that localization would create more demand for data centres in India (refer to section 2.35 and 2.36 in the Consultation Paper). The GDA supports the development of data centres within India, but the economic benefits of new data centres are best realized when those centres can be used by a wide array of individuals and companies within India to access data and services worldwide.

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 GDA 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. The GDA submitted comments on the NPD Framework in January 2021[110] and September 2020.[111]

Directive on Storage of Payment System Data: In April 2018, the RBI issued the Directive on Storage of Payment System Data (Directive)[112], requiring payments firms to store data solely in India and

[104] BSA Submission to the Joint Parliamentary Committee on India's Personal Data Proteciton Bill, 2019, https://www.bsa.org/policy-filings/india-bsa-submission-to-the-joint-parliamentary-committee-on-indias-personal-data-protection-bill-2019
[105] Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet by CERT-In, MeitY accessible at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[106] Frequently Asked Questions (FAQs) on Cyber Security Directions of 28.04.2022 accessible at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf
[107] BSA concerns on the CERT-In Directions on Information Security Practices accessible at: https://www.bsa.org/files/policy-filings/05302022meitycertin.pdf
[108] TRAI consultation paper No. 10/2021, December 16, 2021, https://www.trai.gov.in/sites/default/files/CP_16122021.pdf
[109] GDA Submission on TRAI Consultation Paper on Regulatory Framework for Promoting Data Economy, https://globaldataalliance.org/wp-content/uploads/2022/02/02022022traicp.pdf
[110] GDA Comments on revised Non-Personal Data Governance Framework, https://globaldataalliance.org/wp-content/uploads/2021/07/01292021gdanpd.pdf
[111] GDA Comments on Non-Personal Data Governance Framework, https://globaldataalliance.org/wp-content/uploads/2021/07/09112020GDACommentsonNPDFramework.pdf

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."[113] "Data" is defined broadly, and the Directive is likely to affect both payment processors and their service providers.[114] 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.[115] 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.[116] The recommendations have still not been published by MeitY.

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

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

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

[115] 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

[116] 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

F. Indonesia

The commercial environment in Indonesia is challenging for GDA member companies,[117] as Indonesia has developed or is developing policies that make it increasingly difficult to access the Indonesian market with digitally-enabled products and services.

Personal Data Protection: Indonesia has been developing a draft Personal Data Protection (PDP) Bill since 2014 and successfully enacted the PDP Act on October 17, 2022. The law draws from several principles and aspects of the European Union's General Data Protection Regulation (GDPR), focusing on five main areas: data collection, data processing, data security, data breach, and the right for individuals to have their personal data erased. In terms of data transfers, 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. There is a two-year grace period for data controller and data processors to adjust their practices to comply with the law. A data protection authority that reports to the President will be set up within this period.

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, it provided 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 GDA 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 GDA 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).

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.

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

This requirement is overly restrictive, as it does not appear to account for other internationally recognized transfer mechanisms, including transfer pursuant to the APEC CBPR System, 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 new PDP Act.

Duties on Electronic Transmissions: In February 2018, the Ministry of Finance (MOF) issued Regulation 17, which amended Indonesia's Harmonized Tariff Schedule (HTS) to add Chapter 99 "[s]oftware and other digital products transmitted electronically."[118] Although Chapter 99 is currently duty free, Chapter 99 effectively treats electronic transmissions as imports, to which customs requirements apply, including requirements to comply with all customs laws that attach to imports, prepare and file import declarations, and pay 10 percent value-added tax (VAT) and 2.5 percent income tax.

These compliance obligations are already burdensome for physical goods and require companies to have compliance departments composed of specialized trade professionals that can determine proper customs valuation, country of origin, HTS classification, and other requirements. Complying with Chapter 99 would not only prove very costly for companies, but in most cases these obligations simply cannot be applied to electronic transmissions.

In June 2022, the WTO Membership renewed the WTO Moratorium on Customs Duties on Electronic Transmissions. On June 16, the WTO membership unanimously agreed to renew the Moratorium on Customs Duties on Electronic Transmissions, thus forestalling the imposition of a new class of cross-border data transfer restrictions by major WTO trading partners. This outcome accompanies other WTO agreements on intellectual property, fisheries, agriculture, and WTO reform. The draft Ministerial Decision regarding the E-Commerce Moratorium provides for the Moratorium to remain in place until the next Ministerial (scheduled for December 2023), stating as follows:

> We agree to reinvigorate the work under the Work Programme on Electronic Commerce, based on the mandate as set out in WT/L/274 and particularly in line with its development dimension. We shall intensify discussions on the moratorium and instruct the General Council to hold periodic reviews based on the reports that may be submitted by relevant WTO bodies, including on scope, definition, and impact of the moratorium on customs duties on electronic transmissions. We agree to maintain the current practice of not imposing customs duties on electronic transmissions until MC13, which should ordinarily be held by 31 December 2023. Should MC13 be delayed beyond 31 March 2024, the moratorium will expire on that date unless Ministers or the General Council take a decision to extend.

An important factor in the renewal was the support from 110 global associations (including Indian, Indonesian, and South African associations) that signed onto a Global Industry Statement on the same subject matter.[119]

[118] *Regulation No. 17/PMK.010/2018 (Regulation 17)* (Indonesian) at: https://jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf.
[119] Global Industry Statement on WTO Moratorium on Customs Duties on Electronic Transmissions (2022), https://globaldataalliance.org/wp-content/uploads/2022/05/051322glwtomoratorium.pdf

G. Republic of Korea

Overview/Business Environment

The overall commercial environment in the Republic of Korea (Korea) for GDA members is mixed on the subject of cross-border data transfers and data localization.[120] Korea has a strong IT market and a mature legal system. Although the Cloud Computing Promotion Act[121] 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.[122] 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.[123] Since 2016, the CSAP has contained problematic physical network separation requirements.[124] As described in our August 2019 comments,[125] 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 the use of cloud services in the financial services sector has improved somewhat of late. The Financial Services Commission (FSC) recently approved the use of personal credit information by public cloud services and may be considering additional measures to

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

[121] *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

[122] 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").

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

[124] 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."

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

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.[126]

Personal Information Protection Regime: South Korea's personal information protection regime is one of the most stringent in the region and has significantly decreased the ability for certain GDA members to serve the South Korean market.

In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[127] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[128] and the Credit Information and Protection Act.[129] 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.

[126] 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.
[127] *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.
[128] *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.
[129] *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.

H. Saudi Arabia

Since 2018, the Kingdom of Saudi Arabia has steadily introduced a number of regulatory frameworks which contain data localization requirements or unnecessary data transfer restrictions. This includes the following:

Personal Data Protection Law (PDPL). In August 2022, Saudi Arabia issued its most recent draft of the PDPL,[130] Article 28 of which contains strict data localization mandates and unnecessary data transfer restrictions. The GDA filed comments[131] regarding the draft Personal Data Protection Law, urging Saudi Arabia to explore revisions to Article 28: (1) to better promote data protection and data security; (2) to eliminate data transfer restrictions that are greater than necessary; (3) to eliminate aspects that discriminate against non-national persons or technologies, or against particular economic sectors; and (4) to allow enterprises and citizens (including workers and consumers) in Saudi Arabia to benefit from cross-border access to best-in-class technology from across the globe. More specifically, the GDA urged Saudi Arabia:

(a) To revise Article 28.1.A to avoid unintended legal conflicts with other countries' legal frameworks and difficulties in administration. This includes removal of the clause that conditions the ability to transfer data to another country on that country having "standards for the protection of Personal Data [that] … are no less than those contained in the [Saudi] Law and Regulations."

(b) To explore approaches in Article 28 to ensure that appropriate transfer mechanisms are available under Saudi law and interoperable with other global frameworks. Among other things, we recommend that Saudi Arabia allow, consistent with prevailing international norms and best practices, for a framework of cross-border data transfer mechanisms (including contractual arrangements, binding corporate rules, codes of conduct, certification mechanisms, mutual recognition frameworks, adequacy arrangements, or other means of protecting data that is being transferred);

(c) To refrain from requiring case-by-case advance governmental approval for the use of data transfer mechanisms. Such ad hoc approval requirements would reduce legal predictability and would be

---

[130] Article 28 states as follows:

1. The Controller may transfer Personal Data outside the Kingdom or disclose it to an entity outside the Kingdom as follows:
   A. The State to which Personal Data will be transferred shall have in place laws that ensure the necessary protection of personal data and safeguard the rights of Data Subjects, and has a supervisory authority that imposes appropriate procedures and measures for the protection of Personal Data on Controllers, provided that the standards for the protection of Personal Data in that State are no less than those contained in the Law and Regulations.
   B. The Competent Entity shall adopt the evaluation criteria set out in Paragraph 1(a) of this Article.
2. Notwithstanding Paragraph (1) of this Article, the Controller may transfer Personal Data outside the Kingdom or disclose it to an entity outside the Kingdom other than that specified in Paragraph 1(b) of this Article in the following cases:
   A. Where it is extremely necessary to protect the Data Subject's life outside the Kingdom.
   B. Where it is extremely necessary to protect the Data Subject's vital interests.
   C. Where it is extremely necessary to prevent, examine or treat an infection.
   D. If transfer is necessary in order to protect the public interest.
   E. If transfer is related to fulfilling an obligation under an international convention to which the Kingdom is a party.
   F. If transfer is related to fulfilling an obligation to which the Data Subject is a party, in accordance with the provisions set out in the Regulations.
3. When transferring Personal Data outside the Kingdom or disclosing it to an entity outside the Kingdom, the Controller shall take into account the following:
   A. The transfer shall not prejudice the national security or the vital interests of the Kingdom.
   B. Transfer or Disclosure is limited to the minimum amount of the required Personal Data.

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

[131] https://globaldataalliance.org/wp-content/uploads/2022/09/09082022gdaksapdp.pdf

unnecessary in light the government's existing authority to set transfer conditions under such transfer mechanisms.

(d) To amend the permissible bases for data transfers as follows:

(i) Article 28.2.D: Include an illustrative list of examples of the "public interest," such as "to protect Saudi Arabia's cybersecurity or other security interests; to promote compliance with Saudi Arabia's regulatory requirements; to promote Saudi Arabia's international relations; to promote economic opportunity for Saudi Arabia; and to achieve other outcomes in the public interest of Saudi Arabia."

(ii) Article 28.2.E: Revise this provision to add the following underlined text: "…an international convention to which the Kingdom is a party or seeks to become a party." This change would allow Saudi Arabia to continue to permit data transfers under agreements that it is actively negotiating, such as the WTO Joint Statement Initiative on e-commerce or other similar agreements that specifically address data transfers.

(iii) Article 28.2.F: Revise this provision to add the following underlined text: "…obligation to which the Data Subject, Controller, or Processor is a party." This change would recognize that the data controller or processor may also be subject to contractual obligations that require the transfer of data, and that such obligations should be respected.

Draft Executive Regulation of the Personal Data Protection Law. In March 2022, Saudi Arabia issued – and then postponed implementation until March 2023 of[132] - the *Draft Executive Regulation of the Personal Data Protection Law* (Draft Personal Data Regulation).[133] The Draft Executive Regulation contains strict data localization mandates and unnecessary data transfer restrictions.[134] The GDA submitted comments urging Saudi Arabia:

(a) To revise and/or implement Art. 28.1 so as to eliminate or relax its localization requirements and restrictions on cross-border storage, transfers, and other processing. Such requirements and restrictions undermine data security and various policy and economic goals (as discussed below). We respectfully recommend that Saudi Arabia eliminate these elements, or develop approaches to mitigate their impact to the greatest possible extent.

(b) To eliminate and revise advance *ad hoc* government approval requirements. The requirements in Art. 28.1 and 28.3 for advance, case-by-case government approvals for all personal data transfers represents the most onerous personal data transfer requirement anywhere in the world, including China. We recommend that this advance government approval requirement be revised and/or implemented as follows:

---

[132] Saudi Data and AI Authority, Notification of Postponement of Draft Implementing Regulation on Data Protection (March 22, 2022), at: https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=2339791

[133] Draft Executive Regulation on Data Protection (March 2022), https://istitlaa.ncc.gov.sa/en/transportation/ndmo/pdpl/Documents/Draft%20of%20the%20Executive%20Regulation%20of%20Personal%20Data%20Protection%20Law%20-%20MARCH%209.pdf

[134] Chapter VII of the *Draft Executive Regulation* deals with the "Transfer or Disclosure of Personal Data to Parties outside the Kingdom." We summarize key provisions below.

(a) Article 28 – Transfer of Personal Data to Outside the Kingdom. Article 28.1 requires data localization within Saudi Arabia, and prohibits storage or processing outside of Saudi Arabia "before conducting an impact assessment and obtaining the written approval of the Regulatory Authority after the Regulatory Authority has liaised with the Competent Authority on a base-by-case basis". Article 28.2 permits data transfers on the basis of consent or for purposes relating to the public interest.

(b) Article 29 - Criteria and Guarantees for Personal Data Transfer to a Country not on the Approval List. This Article addresses risk and impact assessments for countries not on the "approved" list. This Article outlines several governmentally approved transfer mechanisms, including standard contractual clauses (Art. 29.b.2.a), binding corporate rules (Art. 29.b.2.b), codes of conduct (Art. 29.b.2.c), certification (Art. 29.b.2.d), or other government-approved mechanisms.

(c) Article 30 - Adequacy List. This Article requires the Competent Authority to prepare a list of the countries that provide adequate level of protection for Personal Data and the rights of Data Subjects.

- Clarify that advance written government approval of transfers is not required in cases in which conditions of consent / public interest are satisfied.
- Clarify that advance written government approval of transfers is not required in cases in which governmentally-approved transfer mechanisms (Arts. 29.b.2.a – d) are employed.
- Clarify that advance government approvals are required only in relation to data transfers that may be subject to export-controlled transactions (e.g., those that implicate military or national security-related imperatives.

(c) To ensure that the governmentally-approved data transfer mechanisms identified in Article 29.b.2 are designed to be interoperable with other global frameworks, including the APEC Cross-Border Privacy Rules and the transfer mechanisms outlined in GDPR Article 46.

(d) To ensure that adequacy determinations under Article 30 provide a standalone basis for data transfers – without requiring use of the transfer mechanisms under Article 29.b.2 or the advance governmental approval requirements of Articles 28.1 and 28.3. Additionally, we recommend that Saudi Arabia clarify that "appropriate international agreements and obligations" include the OECD Privacy Guidelines and the APEC Privacy Framework.[135]

Other recent measures containing data localization requirements or cross-border data restrictions follow:

National Data Governance Interim Regulations. On October 20, 2020, the Saudi Data and Artificial Intelligence Authority published the National Data Governance Interim Regulations. The Regulations require the storage and processing of personal data "in order to ensure preservation of the digital national sovereignty over such data". Personal data can only be transferred or processed outside of the Kingdom if organizations obtain the approval of the relevant regulatory authority and the National Data Management Office. These Regulations are concerning given its broad application to all companies which handle personal data and represents a step towards horizontal imposition of data localization requirements in the Kingdom.

Cloud Computing Regulatory Framework. In March 2018, the Communications and Information Technology Commission (CITC) published the Cloud Computing Regulatory Framework. While the original Framework did not contain a localization requirement, the Framework was updated in March 2019 and now requires cloud customers to ensure that no customer data that is generated or collected by private sector regulated industries is transferred outside the Kingdom. The prohibition extends to any permanent or temporary transfer or storage (e.g. for caching, or redundancy/backup) unless it is expressly allowed under law.[136]

IoT Regulatory Framework. In September 2019, and following on from the Cloud Computing Regulatory Framework, the Communications and Information Technology Commission (CITC) published the IoT Regulatory Framework which regulates the use of IoT services in the Kingdom. This Framework requires all IoT service providers to host all servers used in providing IoT services, and all data inside the Kingdom.[137]

[135] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (visited March 2022) at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; APEC Privacy Framework (visited March 2022), at: https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf#:~:text=The%20APEC%20Privacy%20Framework%20applies%20to%20persons%20or,economies%E2%80%99%20definitions%20of%20personal%20information%20controller%20may%20vary

[136] *See* https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

[137] *See* https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

I. South Africa

South Africa has published several proposed policies and measures that have cross-border data policy implications. We describe one such measure below.

Draft Cloud Computing Policy: Released in March 2021, this policy would appear to involve unnecessary data transfer restrictions and/or data localization mandates. Under the heading, "Policy Issues on Localisation and Cross Border Data Transfers," the draft Cloud Computing Policy states as follows:

> 10.4.1 All data classified/identified as critical Information Infrastructure shall be processed and stored within the borders of South Africa.
>
> 10.4.2 Cross-border transfer of citizen data shall only be carried out in adherence with South African privacy protection policies and legislation (POPIA), the provisions of the Constitution, and in compliance with international best practise.
>
> 10.4.3 Notwithstanding the policy intervention above, a copy of such data must be stored in South Africa for the purposes of law enforcement.
>
> 10.4.4 To ensure ownership and control:
>
> - Data generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled.
> - Government shall act as a trustee for all government data generated within the borders of South Africa.
> - All research data shall be governed by the Research Big Data Strategy of the Department of Science and Innovation (DSI).
> - All data generated from South African natural resources shall be co[1]owned by government and the private sector participant/s whose private funds were used to generate such, and a copy of such data shall be stored in the HPCDPC.
> - Ownership and control of personal information and data shall be in line with the POPIA.
> - The Department of Trade, Industry and Competition through the Companies and Intellectual Property Commission (CIPC) and the National Intellectual Property Management Office (NIPMO) shall develop a policy framework on data generated from intellectual activities including sharing and use of such data.[138]

In April 2021, the GDA provided comments on the draft Cloud Computing Policy,[139] noting that the cross-border data restrictive elements would have negative implications for: (1) South Africa's Position as Regional Center of Cloud Computing Services; (2) South Africa's Broader Economic Goals; (3) South African Manufacturing; (4) South African Services; (5) South Africa's Global Market Access; (6) South Africa's IoT Deployment; and (7) South African Enterprise Productivity.

[138] *South Africa Draft Cloud Computing Policy*, at p. 6.
[139] GDA Comments on Proposed Data and Cloud Policy (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/05122021gdasafrdatacloud.pdf

J. 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.[140]

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). The Law went into effect on January 1, 2019. The Law raises serious concerns and will likely significantly impact the ability of many GDA members to offer products and services on a cross-border basis in Vietnam. The breadth of the Law far exceeds cybersecurity protection and includes numerous unduly restrictive cross-border data elements. In sum, the Law is a significantly negative development in Vietnam's market access environment for the software sector.

On August 15, 2022, the Ministry of Public Security (MPS) published the final Decree No. 53/2022/ND-CP (Decree 53) that took effect from October 1, 2022. Decree 53 is concerning because it requires domestic enterprises to store data within Vietnam and it is not clear whether domestic enterprises include foreign-invested enterprises or subsidiaries of foreign or multinational corporations with head offices in Vietnam.[141] This leads to market access issues if domestic enterprises are unable to use cloud-based services that do not or cannot store data in Vietnam as part of their services. On September 30, the GDA submitted comments on Decree 53.[142]

***Personal Data Protection Decree*:** Following two rounds of public consultations on the draft PDP Decree, in September 2021, the MPS submitted their revised draft PDP Decree to the Ministry of Justice (MOJ) for internal appraisal. However, this version of the draft PDP Decree was kept strictly confidential. With the issuance of Resolution 27 in March 2022 approving the substantive content of the latest draft PDP Decree, the MPS was assigned to consult the National Assembly on the draft. The draft PDP Decree was expected to be passed in May 2022 following review by the National Assembly. However, this process has been delayed.

---

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

[141] Decree 53 provides guidance that will enable regulators to enforce the data localization and local office requirements under Article 26 of the Cybersecurity Law. Chapter V of Decree 53 set out key provisions relating to data storage in Vietnam. Notably, Decree 53 sets out:

a) Types of data subject to local storage (Article 26):
   - Personal data of service users in Vietnam
   - User-generated data in Vietnam (i.e., account name of service user, time of service use, credit card information, email address, network address (IP) of most recent login/log out, registered phone number associated with the account or data);
   - Data on the relationship of service users in Vietnam with onshore and offshore entities doing business in Vietnam (i.e., friends and groups with which users connect or interact).

b) Local storage and local office requirements:
   - Domestic enterprises: All domestic enterprises, no matter which services they provide, must store regulated data in Vietnam.
   - Foreign enterprises: There are 10 businesses/services of foreign enterprises subject to storage of regulated data in Vietnam and establishment of branches or representative offices in Vietnam ("regulated services"). These include (i) telecom services; (ii) services of data storage and sharing in cyberspace (cloud storage); (iii) supply of national or international domain names to service users in Vietnam; (iv) e-commerce; (v) online payment; (vi) intermediary payment; (vii) service of transport connection via cyberspace; (viii) social networking and social media; (ix) online electronic games; (x) services of providing, managing, or operating other information in cyberspace in the form of messages, phone calls, video calls, email, or online chat.
   - Conditions triggering data localization for foreign enterprises: Failure to comply/inadequately complied with written requests made by the Department of Cybersecurity and High-Tech Crime Prevention and Control under the Ministry of Public Security for Cybersecurity Law violations.

c) Data storage period (Article 27): The time period starts from the time an entity receives a request for local storage; the minimum period being 24 months.

[142] GDA Comments on Decree 53 to Implement the Vietnamese Law on Cybersecurity, https://globaldataalliance.org/wp-content/uploads/2022/09/en09302022gdavtde53.pdf

GDA understands that the draft PDP Decree is still pending at the National Assembly Standing Committee because the lawmakers are waiting on the Central Politburo's comments, which has delayed its passage till now (October 2022).

The MPS has also been assigned to take charge and coordinate with the MOJ to propose the formulation of a Personal Data Protection Law after the PDP Decree has been passed. Based on previous iterations of the draft PDP Decree, the PDP Decree will likely impose restrictive data transfer and data localization requirements. In addition, there are also burdensome requirements for personal data processors to store data transfer history for three years, register with the Personal Data Protection Commission (PDPC) for cross-border transfers of sensitive personal data with very detailed requirements for registration, and for the PDPC to carry out annual assessments or audit-like exercises on cross-border data transfers by personal data processors. These obligations are not only impractical, they may also create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

On September 23, 2021 the MPS also released a draft Decree on Administrative Penalties in the field of Cybersecurity, to be adopted on the basis of the Cybersecurity Law. Among others the draft details a number of infractions to the draft PDP Decree. The publication of this draft Decree, which is currently open for consultation, came as a surprise because the main PDP Decree is yet to be finalized. It does, however, provide insights in some of the key provisions under the PDP Decree such as data transfers, consent, data breach notification, etc.

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.

GDA Cross-Border Data Principles (excerpts)

Principle 1: Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders

A **presumption favoring the movement of data across digital networks** reflects the reality of international economic relations today: Data moves seamlessly and securely across globally or regionally distributed cloud-based digital networks that do not match up neatly with national boundaries.[143]

Digital networks lie at the heart of our interconnected global economy. They support millions of daily transactions occurring all over the world, across every sector and at every stage of the value chain, including at the R&D, product design, regulatory approval, manufacturing, finance, marketing, sales, and post-sale service stages. Countries should not disturb the longstanding practice and presumption that data can move seamlessly and responsibly across these networks.

Cross-border data transfers are already estimated to contribute trillions of dollars to global GDP.[144] Sixty percent of global GDP is expected to be digitized by 2022, and six billion consumers and 25 billion devices are expected to be digitally connected by 2025.[145] Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.[146] The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance.[147] Many Regional Trade Agreements (RTAs) reflect this presumption.[148]

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

The second pillar of an international policy consensus on data transfers involves **transparent, accountable, and evidence-driven regulatory practices**. Adhering to these practices helps ensure that any rules impacting cross-border data are well justified, enjoy the support and trust of the public, and do not unintentionally harm international commerce and innovation.

In the design, development, issuance, implementation, and review of measures that may impact cross-border data transfers, governments should:

- Be transparent;[149]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[150]

---

[143] *See e.g.,* Research Institute of Economy Trade and Industry of Japan, *The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies*, p. 4 (2019), at: https://t20japan.org/wp-content/uploads/2019/03/t20-japan-tf8-4-digital-economy-economic-development.pdf

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

[145] *Ibid*.

[146] *Ibid*.

[147] With COVID-19, these trends have become even more pronounced. *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf (showing that before COVID-19, 5–15 percent of US employees worked remotely; as of mid-2020, more than 50 percent of US employees do); Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (Sept. 2020), https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf (showing that remote health services are expected to grow by 700 percent by 2025, and some regions have seen even more rapid growth—up to 40-fold—for non-urgent telemedicine visits).

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

[149] For example, governments should adopt pre-publication and final publication processes that specify implementation timelines, how various substantive concerns are addressed, the evaluation of evidence and expert input, and alternatives or other steps taken to mitigate negative impacts of the measure. *See e.g.,* USMCA Arts. 28.9 and 28.11.

[150] For example, governments should seek out the best reasonably obtainable information relevant to the proposed policy, be transparent regarding information sources and any significant assumptions, and use sound statistical methodologies in analyzing that information. *See e.g.,* USMCA Art. 28.5.

- Analyze that evidence according to sound, objective, and verifiable methods (including regulatory impact assessments—as discussed further under Principle 4 below);
- Provide opportunity for input from the public, experts, and interested stakeholders;[151] and
- Include other procedural safeguards and due process.[152]

A robust and thorough set of regulatory good practices to evaluate the foregoing factors can help policymakers improve the quality and effectiveness of proposed measures, and eschew unintended consequences that may be particularly pronounced when such measures unnecessarily restrict cross-border data transfers.[153]

Principle 3: Any rules impacting cross-border data transfers should be non-discriminatory

The third pillar supporting an international policy consensus on data transfers requires a **commitment to principles of non-discrimination and national treatment in terms of the nationality of persons, products, services, or technologies**. Subject to legitimate public policy limitations, a rule impacting cross-border data transfers would raise concerns if it distorted the market or altered conditions of competition based on the national origin of the persons, the products or services, or the technologies involved. In some cases, concerns may also arise if data transfer rules are designed to provide economic advantages to transfers within a country's borders, and to domestic persons, their products or services, or their technologies, than are afforded to cross-border transfers and non-national persons, products, services, or technologies. Likewise, countries should refrain from discriminatory treatment among sectors, for example by blocking or impeding data transfers in particular sectors.

For the foregoing reasons, any rules relating to cross-border data transfers should not modify conditions of competition or serve protectionist ends by:

- Discriminating against foreign persons, products, or technologies;
- Treating data transfers into or out of the country less favorably than data transfers within the country; or
- Discriminating among different technologies.

---

[151] For example, governments should adopt procedural safeguards to ensure that any proposed measure that would impact cross-border data transfers is well-informed through input from experts, interested stakeholders, and the public. Such safeguards include:

- Advance publication, including an explanation of the measure's underlying objectives, the statutory or other legal basis underlying those objectives, and how the measure would achieve those objectives in light of available evidence;
- Opportunities for public comment; and
- Use of expert advisory groups, public-private consultative mechanisms, evaluation of best practices, and other means of protecting the public interest in thoughtful, deliberative policymaking.

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

[152] For example, governments should offer a retrospective review mechanism that allows for future enhancements or revisions of the measure, including from the perspective of cross-border data policy. The mechanism should permit the government to evaluate:

- How effective the measure has proven in achieving stated objectives;
- Whether changed circumstances or new information would justify a review of some aspects of the measure; and
- Whether there are any new opportunities to eliminate unnecessary regulatory burdens.

See e.g., USMCA Art. 28.13.

[153] Commentary on good regulatory practices in relation to cross-border data policy includes: OECD, *Trade in the Digital Era* (2019), http://www.oecd.org/going-digital/trade-in-the-digital-era.pdf; World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, White Paper (2020), p. 18 https://www.jmfrri.gr.jp/content/files/Open/Related%20Information%20/WEF_May2020.pdf ("[P]olicy-makers should ensure that domestic measures affecting data are enacted in a transparent manner that allows opportunities for broad stakeholder input; are evidence-based and consider the technical and economic feasibility of requirements; require the publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and are targeted and proportionate, and restrict trade as little as possible."); UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (2016), at: https://unctad.org/system/files/official-document/dtlstict2016d1_summary_en.pdf (recommending that the impact on smaller businesses be assessed with respect to proposed data protection legislation and data flow restrictions); Indian Council for Research on International Economic *Relations, Regulatory Burden on Micro, Small and Medium Businesses Due to Data Localisation Policies*, (Sept. 2019), at http://icrier.org/pdf/Regulatory-Burden.pdf; OECD, *Going Digital: Shaping Policies, Improving Lives* (2019), Molinuevo & Saez, Regulatory Impact Assessment Toolkit, The World Bank (2014), at: https://openknowledge.worldbank.org/bitstream/handle/10986/17255/9781464800573.pdf?sequence=1; ICTSD, Advancing Sustainable Development Through Services Regulation (2017)

Such measures should also not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade. As outlined above and in many RTAs negotiated to date, principles of non-discrimination and national treatment are critical to advancing an international policy consensus on data transfers.[154]

Principle 4: Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary

The fourth pillar underlying an international policy consensus on data transfers should embody a commitment to **specifically tailor any rules that would impact cross-border data transfers to legitimate and justified policy objectives and to refrain from imposing restrictions on data transfers that are greater than necessary**.

This standard is reflected in many RTAs negotiated to date[155] and in the administrative and regulatory processes adopted by many governments. As part of their administrative and regulatory practice, governments typically evaluate costs, benefits, and reasonably available alternatives as part of their assessment of whether proposed rules are necessary to achieve a specific public policy objective. Often referred to as regulatory impact assessments, these regulatory evaluations are particularly salient to data transfer restrictions, which can result in excessive economic costs and impacts. Such assessments should evaluate from a cross-border policy perspective:

- The particular public policy outcome that the proposed measure is intended to achieve;
- Whether the cross-border data restrictive features of the proposed measure are needed to achieve that outcome;
- Whether other regulatory or non-regulatory alternatives could feasibly address that need or achieve that outcome with fewer data transfer restrictions;
- The potential impacts of various alternatives over time (e.g., economic, social, environmental, public health, and safety effects) on the government, enterprises, and other persons who depend upon the ability to access technologies and transfer data across borders;
- The grounds for concluding that a particular policy alternative is preferable to others.

As a matter of international and domestic law, this type of assessment is critical to evaluate the disruptive potential of data transfer restrictions in an international commercial ecosystem. Regulatory impact assessments can help answer questions for policymakers in the process. For example, policymakers sometimes underestimate the costs of transfer restrictions, while overestimating their benefits. Policymakers also sometimes lack adequate information regarding non-regulatory solutions—e.g., evidence regarding internal controls that companies have adopted to keep data secure and private and to make it readily available in response to valid investigatory or regulatory requests. In some cases, there has been little substantiation or quantification of the risks that the measure purports to address, and little analysis of whether the proposed measure (and its most restrictive aspects) are necessary and proportionate to address any such risks.[156]

This analysis is important because **how** data is protected is typically more salient than **where** it is stored. As outlined above and in many RTAs negotiated to date, rules impacting cross-border data transfers should be necessary to achieve a legitimate and justified public policy objective and impose no more restrictions on data transfers than necessary.

Principle 5: Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices

[154] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[155] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[156] *See e.g.,* OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Art. 12 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf ("Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.")

The fifth pillar incorporates the accountability model, first established by the Organisation for Economic Co-operation and Development (OECD) and subsequently endorsed and integrated into other legal systems and privacy principles.[157] This model provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data transfers. Under legal frameworks that adopt the accountability model, organizations are required to implement procedures to ensure that data they transfer outside of the country continues to be protected, regardless of where it is stored.

Accountability models comport with a general view that the standards of protection applicable to data in the country of origin should continue to attach to the data as it is transferred across digital networks, including to data centers in other jurisdictions. When data subjects in the country of origin can be assured that the data protections they expect in the country of origin also apply in countries to which the data is subsequently transferred, it obviates one frequent claimed basis for data localization measures.

Wherever possible, countries developing rules that impact data transfers should support and rely upon international consensus-based standards, rather than advance unique, single-country standards that may be incompatible with international standards. Such an approach helps facilitate accountability by increasing alignment among countries and reducing the risks of regulatory inconsistency among countries.

Principle 6: Countries should work together to create compatible trust-based frameworks support the seamless and responsible movement of information across borders

The sixth pillar is for governments to take steps to build interoperable systems that facilitate an international consensus on data transfers.

Continuing to enjoy the transformative benefits enabled by the seamless and responsible movement of data requires a commitment to digital trust. Building digital trust requires both domestic and international action. That means domestic and international legal frameworks help economies realize the benefits of cross-border data transfers and cloud-based technology without sacrificing expectations of privacy,[158] security,[159] and safety.[160] In the international context, this may include:

- **Cross-Border Interoperability Mechanisms:** An important complement to international regulatory convergence efforts are mechanisms that ensure that different national legal regimes are "interoperable"—i.e., compatible—with one another. In the context of personal information protection, such mechanisms may include (among other things) private codes of conduct; contractual arrangements; certifications, seals, or marks; white-listing or mutual recognition arrangements; and participation in government programs. These coordination mechanisms help bridge current gaps in international privacy norms while facilitating the safe and secure transfer of personal information.

- **International Frameworks Regarding Regulation of Data Transfers and Localization:** Another trust-building mechanism involves negotiating agreements to prohibit unnecessary data transfer restrictions and data localization mandates. Thus, these agreements reaffirm the core principle that the seamless and responsible movement of information across digital networks is foundational to a healthy, integrated global economy. These agreements also can more precisely define the relationship between

[157] *See* OECD, *Guidelines governing the protection of privacy and transborder flows of personal data*, Arts. 14-18 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[158] Ensuring continued benefits from cross-border data transfers depends on users' faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of cloud-based technologies, providers must be free to move data across borders in an efficient and commercially viable manner.
[159] Users must be assured that governments and enterprises understand and properly manage the risks inherent in storing and running applications in the cloud. This requires implementing cutting-edge cybersecurity solutions without being required to use specific technologies.
[160] Laws online must provide meaningful deterrence and clear causes of action to deal with online threats and cybercrime. Legal systems should provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud.

rules impacting data transfers and specific policy objectives. Overall, these agreements support legal certainty, helping grow digital trust, economic development, and technological innovation.[161]

[161] To date, many countries have made, or are negotiating, such commitments under international agreements, including under the United States-Mexico-Canada Agreement (USMCA), the US-Japan Digital Trade Agreement, the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CP-TPP), the Digital Economy Partnership Agreement (DEPA), the Australia-Singapore Digital Economy Agreement (DEA), the UK-Japan Comprehensive Economic Partnership Agreement, the US-Japan Digital Trade Agreement, and the WTO Joint Statement Initiative digital trade negotiations. This positive trend should continue.