GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

Global Data Alliance Statement of Support for
Japan's Leadership of WTO and G7 Initiatives on Cross Border Data and Digital Trust

The Global Data Alliance (GDA) welcomes Japan's cross-border data policy agenda for 2023. The GDA is a multi-industry coalition of over 75 companies[1] that depend upon the ability to transfer data across borders and that are committed to high standards of digital trust. Alliance members — which include companies based in Australia, Brazil, Denmark, Germany, Hungary, Ireland, Japan, Korea, Sweden, Switzerland, South Africa, the UK, and the US — are active across sectors including the aerospace, agriculture,[2] automotive,[3] clean energy,[4] finance,[5] healthcare,[6] logistics,[7] media,[8] pharmaceutical,[9] telecommunications,[10] and travel sectors. As part of our engagement with government policy makers, the GDA produces legal analysis, and sector- and issue-focused studies on cross-border data and digital trust.

The GDA supports Japan's cross-border data policy agenda, including in the World Trade Organization (WTO) plurilateral digital trade negotiations and in Japan's G7 Host Year. The GDA also applauds Minister Kono's January 11 speech on DFFT in Washington DC. More specifically,

- We support Japan's call for greater international cooperation to ensure interoperability among national systems affecting data across borders.

- We welcome Japan's proposed "Institutional Arrangement for Partnership" involving policy experts, companies, universities, and other relevant entities.

- We endorse Japan's recommended international base registry of regulations on data transfers and data localization. To this end, we also share a list of selected data transfer restrictions and data localization requirements that impact GDA members (Appendix).

Finally, the GDA supports the reaffirmation of core tenets of international law in the context of DFFT, 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 through interoperable legal frameworks.[11]

We urge Japan to recognize these tenets as four "pillars of trust"[12] supporting the proposed *Institutional Arrangement for Partnership* on DFFT.

Appendix

Selected Cross-Border Data Measures of Concern

The Global Data Alliance (GDA) offers the following country-by-country summary of measures that impact the ability to responsibly transfer data across borders.

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 navigate digital transformation. 75 percent of the value of data transfers accrues to companies in sectors such as manufacturing, agriculture, and logistics.[13] Cross-border data transfers are important to economic and supply chain resilience in sectors including the agriculture,[14] automotive,[15] clean energy,[16] finance,[17] healthcare,[18] logistics,[19] media,[20] pharmaceutical,[21] and telecommunications sectors, [22] among others.[23]

Data transfers factor in every stage of the business value chain,[24] including:

- R&D: Multinational R&D teams collaborate across borders to develop new products, cures, and other advances using cloud-based software solutions and research data produced globally.
- Market Forecasting: AI tools analyze data from around the world to identify patterns that can help predict market demand, customer design preferences, and risk factors relevant to global investment decisions.
- Safety and Productivity: Real-time analytics of data gathered from sensors embedded in global production facilities, machinery, and other assets can alert operators before hazards or breakdowns can occur – allowing for predictive maintenance and safe, productive working conditions.
- Regulatory Compliance: Legal compliance teams gather data from global operations to demonstrate that products and services meet regulatory requirements for transparency, safety, and effectiveness.
- Sales: From order fulfillment, to invoicing, to responding to customer feedbacks – businesses can meet global customer needs only if they can receive and respond to customer queries transmitted across borders.
- Inventory Control: Data analytics and AI can be used to adjust global inventories –avoiding shortages and freeing up resources for more productive uses.
- Supply Chain Management: Real-time electronic data exchange allows companies to authenticate documents seamlessly, optimize shipping routes, and manage transportation assets for purposes of time, cost, and energy efficiency.
- Post-Sale Service: Cross-border data transfer allow manufacturers to trace and recall products, and address service requests, transparently, safely, and quickly.

Data transfers are important to countries and economies of all sizes, but they are particularly critical for smaller economies that lack the large internal markets (e.g., China, India, the EU, and the US). Similarly, while data transfers help companies of all sizes, they are especially important for micro, small, and medium-sized enterprises (MSMEs) that benefit disproportionately from cross-border market opportunities yet lack the resources of multi-national corporations (MNCs) to navigate diverse data barriers in different markets.

Data transfers are also a catalyst for today's innovation-driven economy because 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.[26] By their nature, data restrictions impede the cross-border exchange of knowledge, technical know-how, laboratory analysis, scientific research, and other information.[27]

Unfortunately, governments are increasingly advancing policies of data mercantilism and digital protectionism that undermine this potential.[28] 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 workers, consumers, citizens, and enterprises alike.

There are many types of measures that undermine the ability to responsibly transfer data across borders. Sometimes these measures expressly require data to stay in-country. Sometimes, they impose unreasonable conditions on sending data abroad or prohibit such transfers outright. Oftentimes, they require the use of domestic data centers or other equipment, or the need for such data centers to be operated by local vendors. They sometimes impose nationality-, domicile-, or shareholding-based requirements and thresholds to disfavor foreign enterprises, services, or technologies.

Sometimes these measures cite privacy or security as their underlying purpose, but they are often 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 a disguised restriction on trade; a means of arbitrary or unjustifiable discrimination; or impose more restrictions on data transfers than necessary; or
- Treat cross-border data transfers less favorably than domestic data transfers in a way that discriminates against non-national enterprises.

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

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.[29] In September 2022, the GDA submitted comments regarding the draft Data Protection Act.[30] 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.[31] In May 2021, the GDA submitted comments on this draft policy.[32] 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.[33]

(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.[34]

(d) Absence of any mechanisms that permit data transfers.[35]

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. 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). The GDA has requested that, until relevant implementing 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.[36]

ANPD Regulations on International Data Transfers: In June 2022, the GDA filed comments[37] 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 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.

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,[38] the Digital Service Trade Five Year Plan,[39] and its Digital Economy Five Year Plan.[40] 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[41] and the Security Assessment Measures for Cross-border Data Transfers[42] *(Translation here.*[43]*).* China will also continue to work on implementation and enforcement of the Data Security Law (DSL),[44] the Personal Information Protection Law (PIPL),[45] the Data Management Rules for Automotive Applications,[46] and the Internet Medical and Health Information Security Management Specifications[47]- all of which came into effect in the 2020-2021 timeframe. In this same timeframe, China issued the Platform Economy Opinions[48]; 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*. Since June 2022, China has issued another half-dozen measures and technical standards relating to restrictions on cross-border data transfers.

The GDA has coordinated four different global industry letters and statements on the foregoing measures: July 2022,[49] December 2021,[50] June 2021,[51] and November 2020.[52] Additional details follow:

Measures for Data Security Management in the Fields of Industry and Information Technology: On January 1, 2023, China's Measures for Data Security Management in the Fields of Industry and Information Technology went into effect. This final version of the Measures was released on December 13, 2022, and includes data localization mandates and cross-border data transfer restrictions of varying degrees of severity for "general data," "key data," and "core data," which are defined in Articles 9-11, respectively. Potentially with scope are: (1) Industrial data generated and collected in the process of R&D and design, production and manufacturing, operation management, maintenance, etc.; (2) Telecommunications data; (3) Radio data, including radio frequency, station, other radio wave parameter data generated and collected during radio business activities. Affected entities include: (1) industrial enterprises; (2) Software and IT service enterprises; (3) Telecommunication business operations; (4) Station operators holding a telecommunication business license. Relevant cross-border data provisions are summarized below.

- Article 12: Data handlers in the fields of industry and information technology shall file their own catalogs of key data and core data with the sector-specific regulatory department in their own regions. Including information on outbound sharing and cross-border transfers.

- Article 21: The key data and core data generated and collected within China shall be stored within China wherever required by law. Cross-border transfer security assessments must be performed before requesting to transfer data. Without the approval of the Ministry of Industry and Information Technology, the data handlers … shall not provide foreign law enforcement agencies with data stored within the territory of the People's Republic of China.

- Article 31: The Ministry of Industry and Information Technology shall develop a sector-specific data security assessment management system. The key data and core data handlers in the fields of industry and information technology shall conduct risk assessment on the data handling activities at least once a year and send a risk assessment report to the sector-specific regulatory department in their own regions.

Technical Specification for Cross-Border Processing of Personal Information: On December 16, 2022, China released the Specification for Security Certification of Personal Information Cross-Border Processing (V2.0-202212). The Specification is a "standards-related technical document developed and issued by the

Secretariat of the National Information Security Standardization Technical Committee (TC260)." The Specification applies to personal information handlers carrying out cross-border handling activities of personal information, and it serves as the certification basis for certification bodies to conduct personal information protection certification for cross-border handling activities of personal information (Art. 1). It defines "personal information handler" as an organization or individual who independently decides the purpose and method of handling in the handling of personal information, and it defines "overseas recipient" as an organization or individual located outside China and receiving personal information from personal information handlers.

National Technical Standard re Cybersecurity Requirements for Critical Information Infrastructure Protection: On November 7, 2022, the TC260 National Information Security Standardization Technical Committee announced that the State Administration for Market Regulation and National Standardization Administration had issued (on October 28), a technical standard entitled Information security technology - Cybersecurity Requirements for Critical Information Infrastructure Protection (GB/T 39204-2022). The standards "data security" requirements include requirements that, "[p]ersonal information and important data collected and generated during operations in China will be stored within the territory of China." If it is necessary to provide data abroad, a security assessment shall be conducted and governmental approval obtained, in accordance with the relevant national regulations and standards.

Implementation Rules for Personal Information Protection Certification (PI Certification Rules): On November 18, 2022, the Cyberspace Administration of China (CAC) and the State Administration of Market Regulation (SAMR) announced the publication (with immediate effect) of the Personal Information Certification Rules. These rules are intended to support the Personal Information Protection Law (PIPL), outlining requirements for the certification of personal information processors to carry out personal information collection, storage, use, processing, transmission, provision, disclosure, deletion, cross-border, and other processing activities. As a substantive matter, the Rules mandate compliance with the GB/T 35273 Information Security Technology Personal Information Security Specification, for personal information processors conducting cross-border processing activities, they should also comply with the requirements of TC260-PG-20222A Specification for Security Certification of Personal Information Cross-Border Processing Activities.

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.[53]

CAC Draft Standard Contracts for Outbound Data Transfers: On July 28, 2022, the GDA submitted comments[54] in response to the Cyberspace Administration of China's draft Measures on Standard Contracts for the Export of Personal Information.[55] 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 "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.

Personal Information Protection Law: On November 1, 2021, the Personal Information Protection Law ("PIPL") went into effect. 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); and
(6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established. (PIPL, Art. 39).
(7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43)

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. On October 1, 2021, the *Data Management Rules for Automotive Applications* became effective. These rules 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.

Data Security Law: The Data Security Law ("DSL") 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."

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.

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[56] The Cyberspace Administration of China (CAC) and other authorities continue to issue measures and standards to implement the CSL. Many of these measures leave important issues vague and unclear (e.g., the definition of critical information infrastructure (CII) or "important information"), or appear to expand the scope of the law — exacerbating the negative impact of these rules on the software industry. Broadly speaking, the impact of the CSL and related data regulations is to require that important information and personal information collected in China (by CII operators and others) must be held in-country. 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.

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 new cross-border data restrictions.

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 fora. There are some calls for data localization in Europe especially in the wake of the CJEU *Schrems II* decision, such as Council declarations on the need to create an EU Cloud Federation, contributing to the emergence of projects such as GAIA-X.

EU – European Health Data Space: On May 3, 2022, the Commission published the European Health Data Space (EHDS),[57] sectoral legislation that will complement the EU Data Act. The EHDS proposed Regulation contains extensive provisions on the third country transfer of health data and non-personal electronic data. Those provisions would, among other things, (1) deem pseudonymized or anonymized health data to be "highly sensitive" if their transfer to third countries presents a risk of re-identification; and (2) require digital health authorities, health data access bodies, the authorized participants to "take all reasonable technical, legal and organizational measures… to prevent international transfer or governmental access to non-personal electronic health data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State."

On July 28, the GDA published a White Paper regarding Cross-Border Data Transfers & the EU Health Data Space (EHDS).[58] The 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).[59]

EU Data Act: On February 23, 2022, the European Commission proposed the draft Data Act, which is part of the European Data Strategy together with the Data Governance Act (DGA).[60] Among other things, the Data Act seeks to prevent unlawful transfers and access to nonpersonal data held in the EU, to the extent such transfer or access would create a conflict with EU law or the relevant national law.

On June 30, the Global Data Alliance published its position paper on the EU Data Act. 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."[61]

EU DPA Data Transfer Decisions: The decision of the European Court of Justice in the *Schrems II* case, which invalided the EU-US Privacy Shield agreement, also 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).[62]

E. India

Overview/Business Environment

The commercial environment for GDA members remains challenging in India,[63] 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,[64] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[65] and payment processing regulations.[66] 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 Personal Data Protection Bill: On November 18, 2022, the Ministry of Electronics and Information Technology (MeitY) published a draft Digital Personal Data Protection Bill, 2022.[67] The Bill allows transfer personal data outside India but only to a so-called "White List" of jurisdictions identified by the central government. The Bill does not address other grounds for transfers, such as contractual mechanisms or certifications.

On December 16, the GDA filed comments in response to the Bill. GDA recommended that the Bill be revised: (1) to support cross-border data transfers while ensuring organizations remain accountable for protecting the privacy and security of personal data after transfer, and more specifically, that Section 17 be revised to reflect the accountability model under which entities that collect personal data remain responsible for its protection, regardless of where the data is processed; (2) to state that international transfers are permitted when a Data Fiduciary or Data Processor uses a data transfer mechanism that is able to provide a comparable level of protection, regardless of where the data is processed; and (3) to recognize other transfer mechanisms, in addition to any white-list, so that the Bill would permit transfers made with consent of the data principal and transfers based on interoperable mechanisms such as model contracts, intra-group schemes, and certifications like the APEC-CBPR & PRP systems.

Digital India Act: In August 2022, India announced that it was considering developing a comprehensive set of laws that would purportedly be in "sync with today's digital economy"[68] and "make the online world more accountable"[69] 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.[70] 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.

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).[71] 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,[72] as highlighted in prior industry comments.[73]

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).[74] In comments dated February 2022[75], 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.

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[76] and September 2020.[77]

Directive on Storage of Payment System Data: In April 2018, the RBI issued the Directive on Storage of Payment System Data (Directive)[78], requiring payments firms to store data solely in India and ensure that any data processed abroad be deleted within 24 hours. (Directive), imposing data and infrastructure localization requirements that required payment system operators to "ensure that the entire data relating to payment systems operated by them (system providers) are stored in a system only in India."[79] "Data" is defined broadly, and the Directive is likely to affect both payment processors and their service providers.[80] 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.[81] 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.[82] The recommendations have still not been published by MeitY.

F. Indonesia

The commercial environment in Indonesia is challenging for GDA member companies[83] as Indonesia advances policies that impede market access for digitally-enabled products and services.

Personal Data Protection: In September 2022, Indonesia's Personal Data Protection (PDP) Bill went into effect. Chapter 8 of the PDP Bill focuses on International Transfers. Notably, the PDP Bill stipulates personal data transfer requirements which are like the EU GDPR. The requirements include: (i) a data controller can only transfer the personal data to a country that has adequate protection to Indonesia, (ii) assurance from the data controller to the data subject that a legally binding and appropriate personal data protection is available, or (iii) data controller has obtained consent from data subject to transfer their personal data abroad. These requirements apply alternatively, and further provisions on this will be stipulated under Government Regulations.

Regulation 71 on the Operation of Electronic Systems and Transactions: In October 2019, the Government of Indonesia issued Government Regulation 71 on the Operation of Electronic Systems and Transactions (GR71), which replaced Government Regulation 82 – an earlier cross-border data restriction.[84] GR71 explicitly states that public sector data must be managed, stored, and processed in Indonesia. While localization is not expressly required for private sector data, GR71 gives regulators discretion to define sector-specific requirements. For example, 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.

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

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."[85] 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) as well as other taxes. On December 13, 2022, Indonesia again formally reiterated its interest in unilaterally imposing customs restrictions on the cross-border movement of data.[86] Indonesia issued this formal statement despite a June 2022 WTO agreement to renew the Moratorium on Customs Duties on Electronic Transmissions,[87] and despite support for that Moratorium from Indonesian and other industry groups.[88]

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.[89] Korea has a strong IT market and a mature legal system. Although the Cloud Computing Promotion Act[90] 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 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.[91] Furthermore, we understand that certain non-government entities in the healthcare and education sector are now encouraged to adopt the CSAP, which has proven impossible for foreign CSPs to become certified. Thus, significant barriers to providing cloud computing and related services in Korea remain.

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.[92] Since 2016, the CSAP has contained problematic physical network separation requirements.[93] As described in our August 2019 comments,[94] these requirements will have a negative impact on Korea's digital ecosystem and curtail its ability to participate effectively in the global digital economy — raising the cost of providing services and inhibiting the choice of technology available to end-users and procuring entities. Similarly, the Financial Services Commission (FSC) recently approved the use of personal credit information by public cloud services and may be considering additional measures to expand the ability to manage financial data on the public cloud. However, the FSC specifically requires that such data be maintained on servers located in Korea.[95]

Personal Information Protection Regime: 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 Korean market. In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[96] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[97] and the Credit Information and Protection Act.[98] 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 Korea's personal information protection regime closer to that of EU's General Data Protection Regulation and may aid Korea's efforts in attaining an "adequacy" recognition from the European Commission. However, more work is required to reform 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. 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.

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,[99] Article 28 of which contains strict data localization mandates and unnecessary data transfer restrictions. The GDA filed comments[100] 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 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[101] - the *Draft Executive Regulation of the Personal Data Protection Law* (Draft Personal Data Regulation).[102] The Draft Executive Regulation contains strict data localization mandates and unnecessary data transfer restrictions.[103] 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:

- 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.[104]

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.[105]

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.[106]

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.[107]

In April 2021, the GDA provided comments on the draft Cloud Computing Policy,[108] 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.

J. Vietnam

Over the past several years, Vietnam has enacted, implemented, and proposed a wide array of cross-border data restrictions and data localization mandates, as reflected in over a half dozen GDA submissions over an 18-month period. GDA provided comments on data localization and related data restrictions in Vietnam in April 2021[109] (translation),[110] September 2021[111] (translation),[112] November 2021[113] (translation),[114] December 2021[115] (translation),[116] September 2022[117] (translation),[118] and December 2022.[119] The GDA has also joined a broad group of global industries in expressing concerns regarding Vietnam's cross-border data restrictions and data localization requirements.[120] We elaborate below.

Cybersecurity Law and Implementing Decrees: On October 1, 2022, On August 15, 2022, the Ministry of Public Security (MPS) published the final Decree No. 53/2022/ND-CP (Decree 53) to implement *inter alia* the restrictive cross-border data elements of 2019 Vietnam's Cybersecurity Law.[121] Decree 53 is concerning because it requires storage of data within Vietnam by "domestic enterprises," a term that has been broadly construed to include various foreign-invested enterprises and/or their subsidiaries.[122] On September 30, the GDA submitted comments on Decree 53.[123]

Telecommunications Law: On December 23, 2022 the GDA filed comments with Vietnam's Ministry of Information and Communication (MIC) regarding a proposal to update the 2009 Law on Telecommunications. Article 75.1 of the draft law states as follows: "Enterprises engaged in data center service and cloud computing service business are responsible for storing data in Vietnam in accordance with relevant laws." The GDA urges Vietnam to remove Article 75(1), which reaffirms Vietnam's data localization requirements, from the draft Law.[124]

Personal Data Protection (PDP) Decree: As of January 2023, the draft PDP Decree is reportedly still pending at the National Assembly Standing Committee while lawmakers await the Central Politburo's comments. Based on previous iterations, the PDP Decree will likely impose restrictive data transfer and data localization requirements. In addition, there are 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.

Cybersecurity Administrative Penalties: On September 23, 2021, the MPS released a draft Decree on Administrative Penalties in the field of Cybersecurity. The draft details various infractions to the draft PDPD, which include the transfer of data across borders.

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 appear to create a preferential framework for domestic cloud service providers, and measures currently characterized as "voluntary" will be treated as *de facto* requirements.

[1] The Global Data Alliance 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. BSA | The Software Alliance administers the Global Data Alliance. BSA is the leading advocate for the global software industry before governments and in the international marketplace.

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

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

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

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

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

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

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

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

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

[11] In the WTO context, these tenets apply to multilateral disciplines relating to goods, services, investment, intellectual property, technical regulations, and domestic regulations relating to protect human, animal or plant life or health (e.g., environmental rules); consumer protection; privacy and personal data protection; and safety. *See e.g., WTO Secretariat, General Agreement on Trade in Services - An Introduction (2013), at: https://www.wto.org/english/tratop_e/serv_e/gsintr_e.pdf; see also*, *WTO Analytical Index – GATS Art. XIV* at: https://www.wto.org/english/res_e/publications_e/ai17_e/gats_art14_jur.pdf; *WTO Analytical Index – GATS Art. XVII*, at: https://www.wto.org/english/res_e/publications_e/ai17_e/gats_art17_jur.pdf

[12] Global Data Alliance, *Cross-Border Data Policy Principles* (2020), at: https://globaldataalliance.org/wp-content/uploads/2021/07/03022021gdacrossborderdatapolicyprinciples.pdf

[13] Global Data Alliance, *Cross-Border Data Transfer Facts and Figures* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf
[14] Global Data Alliance, *GDA Website – Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/
[15] Global Data Alliance, *GDA Website – Automotive* (2022), at: https://globaldataalliance.org/sectors/automotive/
[16] Global Data Alliance, *GDA Website – Energy* (2022), at: https://globaldataalliance.org/sectors/energy/
[17] Global Data Alliance, *GDA Website – Finance* (2022), https://globaldataalliance.org/sectors/finance/
[18] Global Data Alliance, *GDA Website – Healthcare* (2022), https://globaldataalliance.org/sectors/healthcare/
[19] Global Data Alliance, *GDA Website – Supply Chain Logistics* (2022), https://globaldataalliance.org/sectors/supply-chain-logistics/
[20] Global Data Alliance, *GDA Website – Media and Publishing* (2022), https://globaldataalliance.org/sectors/media-publishing/
[21] Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/
[22] Global Data Alliance, *GDA Website – Telecommunications* (2022), https://globaldataalliance.org/sectors/telecommunications/
[23] 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
[24] 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
[25] Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf
[26] The G20 has underscored that the "[c]ross-border flow of data, information, ideas and knowledge generates … greater innovation," 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." 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." *See* G20,

Ministerial Statement on Trade and Digital Economy (2019), http://www.g20.utoronto.ca/2019/2019-g20-trade.html; *Trade Policy Review of India*, Secretariat Report, *supra* note 5; UNCTAD Digital Economy Report 2021.

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

[28] 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

[29] 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

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

[31] 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."

[32] GDA Comments on Bangladesh Draft Cloud Computing Policy, https://globaldataalliance.org/wp-content/uploads/2021/07/05122021gdabdcloudpol.pdf

[33] 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.

[34] 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

[35] 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.

[36] 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

[37] GDA Response to ANPD Consultation on Data Transfers (June 2022), https://globaldataalliance.org/wp-content/uploads/2022/06/20220617BrazilBSACommentsDataTransfersEN.pdf
[38] https://wap.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2021/art_c4a16fae377f47519036b26b474123cb.html
[39] https://www.scmp.com/tech/policy/article/3153196/china-pursue-digital-trade-expansion-under-new-five-year-plan-cross
[40] https://english.www.gov.cn/policies/latestreleases/202201/12/content_WS61de9a35c6d09c94e48a385f.html
[41] http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm
[42] http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm
[43] https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/
[44] https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/
[45] https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/
[46] http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm
[47] https://mp.weixin.qq.com/s/dc7gd8EIPJzT9OD4Wp91pw
[48] https://www.chinamoneynetwork.com/2022/01/21/china-issues-new-rules-regulating-internet-giants-and-platform-economy
[49] https://globaldataalliance.org/wp-content/uploads/2022/08/en07282022gdachdftcontractprov.pdf
[50] https://globaldataalliance.org/wp-content/uploads/2021/12/12012021gdachmultiassltr.pdf
[51] https://globaldataalliance.org/wp-content/uploads/2021/07/en06022021gdachinadslpip.pdf
[52] https://globaldataalliance.org/wp-content/uploads/2021/07/en11242020chinamultiassocltr.pdf
[53] 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

[54] GDA, Global Industry Statement on Draft China Standard Contract Provisions, https://globaldataalliance.org/wp-content/uploads/2022/08/en07282022gdachdftcontractprov.pdf
[55] 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).

[56] CSL, *op.cit.*

[57] European Commission, *Proposal for a regulation - The European Health Data Space,* at: https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en

[58] GDA, *White Paper on Data Transfer Provisions of the EU Proposal for a European Health Data Space*, https://globaldataalliance.org/wp-content/uploads/2022/08/07282022gdaeuhealthdataspace.pdf
[59] 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 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.
[60] European Commission, *EU Data Act,* at: https://digital-strategy.ec.europa.eu/en/policies/data-act
[61] Global Data Alliance, *Comments on the EU Data Act,* at: https://globaldataalliance.org/wp-content/uploads/2022/07/06302022gdadataactprop.pdf
[62] 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).
[63] *See generally*, BSA Cloud Scorecard – 2018 India Country Report, at: https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

[64] *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

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

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

[67] MeitY, *Digital Personal Data Protection Bill*, at: https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022
[68] 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
[69] 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/
[70] Information Technology Act 2000, https://www.meity.gov.in/content/information-technology-act-2000
[71] 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
[72] 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
[73] BSA concerns on the CERT-In Directions on Information Security Practices accessible at: https://www.bsa.org/files/policy-filings/05302022meitycertin.pdf
[74] TRAI consultation paper No. 10/2021, December 16, 2021, https://www.trai.gov.in/sites/default/files/CP_16122021.pdf
[75] GDA Submission on TRAI Consultation Paper on Regulatory Framework for Promoting Data Economy, https://globaldataalliance.org/wp-content/uploads/2022/02/02022022traicp.pdf
[76] GDA Comments on revised Non-Personal Data Governance Framework, https://globaldataalliance.org/wp-content/uploads/2021/07/01292021gdanpd.pdf
[77] GDA Comments on Non-Personal Data Governance Framework, https://globaldataalliance.org/wp-content/uploads/2021/07/09112020GDACommentsonNPDFramework.pdf
[78] Storage of Payment System Data Directive, *op. cit.*

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

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

[81] 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

[82] 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

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

[84] Indonesia originally 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.

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

[86] Permanent Delegation of Indonesia to the World Trade Organization, *Communication - Indonesia's Perspective on Customs Duties on Electronic Transmissions*, WT/GC/W/859 (December 13, 2022).

[87] The WTO Decision 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.

[88] Global Industry Statement on WTO Moratorium on Customs Duties on Electronic Transmissions (2022), https://globaldataalliance.org/wp-content/uploads/2022/05/051322glwtomoratorium.pdf

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

[90] *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

[91] 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").

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

[93] 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."

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

[95] 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.

[96] *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.

[97] *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.

[98] *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.

[99] 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
[100] https://globaldataalliance.org/wp-content/uploads/2022/09/09082022gdaksapdp.pdf
[101] 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
[102] 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
[103] 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.

[104] 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
[105] *See* https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

[106] *See* https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf
[107] *South Africa Draft Cloud Computing Policy*, at p. 6.

[108] GDA Comments on Proposed Data and Cloud Policy (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/05122021gdasafrdatacloud.pdf
[109] Vietnam: Comments on Draft Viet Nam Personal Data Protection Decree (globaldataalliance.org)

[110] Góp ý về Dự thảo Nghị định về Bảo vệ Dữ liệu Cá nhân (globaldataalliance.org)

[111] Vietnam: Comments on Proposed Amendments to Draft Decree 72 (globaldataalliance.org)

[112] Ý kiến Đóng góp về các Sửa đổi được Đề xuất đối với Dự thảo Nghị định 72 (globaldataalliance.org)

[113] Vietnam: Comments On Proposed Amendments To Draft Decree On Sanctions Against Administrative Violations In the Field of Cybersecurity (globaldataalliance.org)

[114] Ý kiến Đóng góp về các Đề xuất Sửa đổi đối với Dự thảo Nghị định Quy định về Xử phạt Vi phạm Hành chính trong Lĩnh vực An ninh mạng (globaldataalliance.org)

[115] GDA Comments on Proposed Amendments to Draft Decree 72 (globaldataalliance.org)

[116] Ý kiến Đóng góp về các Sửa đổi được Đề xuất đối với Dự thảo Nghị định 72 (globaldataalliance.org)

[117] Vietnam: GDA Comments on Decree 53 to Implement the Law on Cybersecurity (globaldataalliance.org)
[118] Góp ý của Liên minh Dữ liệu Toàn cầu về Nghị định 53 hướng dẫn Luật An Ninh Mạng (globaldataalliance.org)
[119] Global Data Alliance, *Comments on Draft Vietnam Law on Telecommunications*, at: https://globaldataalliance.org/wp-content/uploads/2022/12/en12232022gdavtdfttelecom.pdf
[120] Vietnam: Multi-association Letter on Draft Decree on Personal Data Protection (globaldataalliance.org)

[121] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) at: https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/
[122] 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.

[123] GDA Comments on Decree 53 to Implement the Vietnamese Law on Cybersecurity, https://globaldataalliance.org/wp-content/uploads/2022/09/en09302022gdavtde53.pdf
[124] The GDA observes that Vietnam's various data localization requirements:

- Present challenges to Vietnam's efforts to harness digital transformation for the benefit of its economy and citizens;

- Restrict domestic enterprises, both small and medium-sized enterprises (SMEs) and larger organizations such as hospitals and banks, from using world leading information technology and cloud computing solutions from service providers that offer their services from outside of Vietnam;
- Expose domestic enterprises to greater data security risks, while noting that the GDA supports efforts to ensure data is protected commensurate with the risk its compromise poses;
- Increase legal uncertainty because Vietnam's various laws and draft regulations - including the Law on Cyber Security, the draft Personal Data Protection Bill, Decree 72, and Decree 53 - require local storage to different, and possibly contradictory, extents;
- Raise concerns regarding Vietnam’s compliance with its existing international commitments, including under the CPTPP and the WTO General Agreement on Trade in Services; and
- Complicate Vietnam’s ability to participate in and benefit from regional trade initiatives, such as the IPEF.