GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

UPDATES

OCTOBER - DECEMBER 2022

EXECUTIVE SUMMARY

This Global Data Alliance Update provides information on recent cross-border data policy developments from around the world.

Africa

- Several economies are advancing data protection frameworks with cross-border data provisions, including Namibia, Nigeria, and Tanzania. New rules are also expected to go into effect in 2023 in Botswana and Rwanda.

Asia-Pacific

- Countries such as Australia, Singapore, and Japan are advancing advance international norms favoring data transfers – in the World Trade Organization (WTO), in regional settings like the Indo-Pacific Economic Framework (IPEF), and in digital economy agreements.
- As it looks to advance its *Data Free Flow with Trust* initiative in its G7 Host Year, Japan will aim to support an environment conducive to data transfers and digital trust.
- Some regional economies – including Korea – continue to demand data localization particularly in connection with services procured by government entities.
- China continues to elaborate on its complex framework of cross-border data restrictions and data localization requirements. This augurs both increasing isolation for China and increasing difficulty in doing business in China. To the extent that Chinese data measures are emulated by other regional economies – for example, in Pakistan or Bangladesh, which is contemplating a restrictive draft Data Protection Bill covering both personal and non-personal data – there will be continued spillover effects.
- Vietnam is another economy that has embraced stringent cross-border data provisions, as reflected in the GDA's half-dozen submissions over a short period of time.
- As India embarks on its 2023 G20 Host Year, it remains to be seen how new Indian cross-border data policy proposals will unfold. It will be important to monitor exactly how India will advance its draft Digital Personal Data Protection Bill – with its as yet undefined "White List" approach to data transfers.
- At the WTO, Indonesia, India, and several other economies are advocating for a new system of customs duties and restrictions applicable to electronic transmissions – including media, software, and data – that move across transnational digital networks.

European Union

- It is hoped that the recent draft EU Adequacy Decision regarding the United States will ameliorate conditions for trans-Atlantic data transfers and business operations, once that decision goes into effect.
- Until that time and perhaps beyond, there may be further national Data Protection Authority rulings regarding data transfers under the *Schrems II* decision. Even after the EU Adequacy Decision goes into effect, a further legal challenge to the new EU-US Data Privacy Framework may be possible.
- Cross-border data policies also appear in the European Cybersecurity Certification Scheme for Cloud Services (EUCS), the EU Data Act, and the Proposal for a European Health Data Space, among others.
- EU authorities continue to work with counterparts in other countries on both data protection laws and free trade agreements. Working closely with the EU and trading partners on these important issues should be a priority.

United Kingdom

- The United Kingdom (UK) has begun issuing adequacy decisions that reflect a different treatment of cross-border data transfers (see e.g., the UK-Korea Data Bridge) than that reflected in EU adequacy decisions.
- The UK also continues to advance a robust trade negotiating agenda. UK trade agreements – with Australia, Singapore, Japan, and others – contain provisions safeguarding the ability to transfer data across transnational digital networks.

Middle East

- Saudi Arabia's draft Personal Data Protection Bill has become less restrictive of data transfers over successive draft iterations. However, continued engagement remains important.
- Outreach on cross-border data policy from the US and the UK to the United Arab Emirates and other countries may help set a new direction.

Western Hemisphere

- Western Hemisphere economies, including Argentina, Brazil, Canada, Chile, Mexico, and Peru have not historically favored an overly restrictive approach to data transfers. Some of these countries have also been leading voices in the WTO digital trade negotiations. Ongoing engagement should be a priority.
- The United States deserves particular attention, as concerns regarding China – including the treatment of personal data by Chinese authorities – continue to grow. Likewise, it remains to be seen whether the United States will maintain its past approach to data transfers and data localization in its ongoing trade negotiations, such as the IPEF negotiations or the Americas Partnership for Prosperity (APEP) negotiations.

TABLE OF CONTENTS

AFRICA

A. Kenya

Kenya – Strategic Trade and Investment Partnership with the US: On December 12, Kenya and the United States met to discuss plans relating to the US-Kenya Strategic Trade & Investment Partnership, which was launched in July 2022. The Partnership includes a pillar focused on digital trade. Negotiations are expected to accelerate in 2023. The GDA submitted comments in September 2022 regarding US-Kenya cross-border data negotiating priorities.

B. Namibia

Namibia – Draft Data Protection Bill: On November 25, Namibia's Ministry of Information and Communication Technology (MICT) reportedly commenced stakeholder engagement on the draft Data Protection Bill, which contains a chapter on "Transborder Flows of Personal Information." Article 53 of the Bill prohibits data transfers to another country unless:

- The transferee is subject to a law that provides an "adequate level of protection" that is substantially similar to Namibian law;
- The data subject consents to the transfer;
- The transfer is necessary to the performance of a contract or pre-contractual measures agreed to by the data subject; or
- The transfer is for the benefit of the data subject (where it is not reasonably practicable to obtain the consent of the data subject to that transfer; and the data subject would likely grant such consent).

The bill establishes a default rule that personal data may not be transferred from Namibia to any other country absent either an adequacy determination or the existence of other specified circumstances.

C. Nigeria

Nigeria – National Data Strategy: On November 10, the National Information Technology Development Agency released the draft National Data Strategy (NDS) of Nigeria. The NDS is organized around seven pillars, including a pillar devoted to Digital Sovereignty, which states as follows (emphasis added):

> The objective of this pillar is to address data ownership, classification, control and access as related to residency and data localization according to the national laws and regulations of Nigeria. This implies that data collected in Nigeria and from Nigerians within or outside the country is subject to all relevant laws, rules and regulations governing the use of data in Nigeria. Data Sovereignty ensures that any data generated is subjected to the laws and governance of the geographic location in which the data is collected and processed. Data Sovereignty is a key aspect of international data privacy that enables a country or any entity to regulate entities that can access sensitive data. Data Sovereignty is an important requirement that supports and strengthens data residency and compliance with national laws and regulations.

This pillar contains metrics, including "develop[ing] guidelines to monitor cross-border data flows and ensure the protection of Nigerian data while in motion, in use and at rest."

Nigeria – Draft Data Protection Bill: On October 5, Nigeria published a draft Data Protection Bill, which contains a section on the "Cross-Border Transfers of Personal Data." Article 43-45 of the Bill prohibits transfers of personal data unless:

- The recipient of the personal data is "subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal data" that is "substantially similar" to the standards in Nigerian law, including in relation to: (1) enforceable subject rights; (2) availability of judicial/administrative redress to data subjects; (3) binding agreements with other countries; (4) access of a public authority to personal data; and (5) the existence of a data protection law, and an independent data protection authority.

The Nigerian draft law also provides that Nigeria may:

- Make rules "requiring data controllers and data processors … explain [the] adequacy" of measures;
- Designate "categories of personal data that are subject to additional specified restrictions on transfer to another country based on the nature of such personal data and risks to data subjects";
- Issue "guidelines as to adequacy assessments and may list out which countries afford adequate or inadequate levels of protection";
- Approve binding corporate rules, codes of conduct or certification mechanisms; and
- Make adequacy determinations for other jurisdictions

The Global Data Alliance filed comments with Nigeria's Data Protection Bureau regarding the draft Nigerian Data Protection Bill. The GDA recommended as follows:

- Clarify that – in the absence of an adequacy determination – transfers are legally permitted on the basis of appropriate safeguards, such as standard contractual clauses (SCCs);
- Revise Article 44 to ensure that all internationally accepted data transfer mechanisms are available under the Bill and to include provisions that would accommodate other future data transfer interoperability mechanisms;
- Revise Article 45 to permit transfers in situations in which: (a) the transfer is necessary for important reasons of public interest; (b) the transfer is necessary for the establishment, exercise or defense of legal claims; (c) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, among other circumstances;
- Specify a grace period for enforcement the Bill's data transfer provisions that is 24 months from the date of enactment of any implementing regulations.

Nigeria – Interest in Cross-Border Privacy Rules Forum: Nigerian authorities met with counterparts from the United States to learn more about potential participation in the Global Cross-Border Privacy Rules (CBPR) Forum, which Australia, Canada, Japan, Korea, the Philippines, Singapore, Taiwan, and the United States established in the first half of 2022. The idea of converting CBPR from a regional to a global framework is rooted in a simple theory, foundational to the CBPR system: Baseline data protection standards across jurisdictions can be interoperable without being equivalent. In addition to Nigeria, countries that have expressed interested in the Global CBPR Forum include the UK, Bermuda, and others.

D. Tanzania

Tanzania – Personal Data Protection Bill: On November 1, the Parliament unanimously passed the Personal Data Protection Bill 2022. The was gazetted in December 2022. Part Five of the Bill contains two articles on data transfers, namely Article 31 ("Exporting personal information to a country with adequate protection of personal information") and Article 32 ("Exporting to a country without adequate protection of personal information"). Article 32 stipulates that data transfers may be permitted on the basis of: (a) consent; (b) necessity for fulfillment of certain legal contracts; (c) the public interest; (d) defense of legal claims; (e) to protect the interests of the data subject; and (f) a range of other objectives. For more information, *see* Round up of data protection Africa (licdn.com)

E. Other

Other Economies: On December 14, the National Assembly of Niger adopted a revised draft Personal Data Protection Law. Furthermore, several revised data protection laws are expected to go into effect in 2023, including in Botswana in September 2023 (additional details here) and in Rwanda in October 2023.

APAC

A. Australia

Australia – Economic Cooperation and Trade Agreement with India: On December 29, the Australia-India Economic Cooperation and Trade Agreement (**ECTA**) came into force. The ECTA offers "greater certainty and transparency regarding the rules that will apply when providing services" on a cross-border basis. ECTA is a described as stepping-stone towards a full Australia-India Comprehensive Economic Cooperation Agreement.

Australia – Ministerial Consultations with the US: On December 7, Australia and the United States held the 32nd annual Australia-US Ministerial (AUSMIN) consultations. Among other things, both sides discussed the following:

- *IPEF:* The principals are committed to ensuring that IPEF delivers for everyone, especially workers, consumers, and under-represented groups such as Indigenous Peoples and women.
- *Digital Connectivity:* The principals identified additional areas for collaboration and financing opportunities to support trusted ICT infrastructure, including promoting supplier diversity and innovation to build more resilient supply chains in the Indo-Pacific region and globally. They also discussed how additional public-private partnerships on topics such as 5G/Open RAN, standards, and supply chains could augment our work to support critical and emerging technology among Quad governments.
- *Emerging Technology:* They highlighted how the bilateral partnership in critical and emerging technologies helps to provide a model for the entire Indo-Pacific region. This includes joint capacity building and outreach to Southeast Asia and other Indo-Pacific partners on responsible deployment of new technologies like artificial intelligence and facial recognition.

B. Bangladesh

Bangladesh – On December 6, the United States and Bangladesh convened the Sixth meeting of the US-Bangladesh Trade and Investment Cooperation Forum Agreement Council this week. The two sides discussed a number of topics, including digital trade. The United States reportedly "advocated for the development of digital trade policies that support MSME's participation in the digital economy, increase trust for consumers, businesses, and workers, and facilitate secure cross-border data flows. The United States emphasized that new digital policies should be developed in an open and transparent manner with opportunities for public stakeholder engagement. Participants discussed ways to ensure that digital policies do not disadvantage foreign and domestic suppliers, disclose proprietary data, or increase cybersecurity risks," according to the USTR statement. The GDA has previously submitted comments on cross-border data policies under Bangladesh' draft Cloud Computing Policy and Bangladesh' draft Data Protection Act of 2022.

C. China

China – Measures for Data Security Management in the Fields of Industry and Information Technology (Trial): 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 specified below (emphasis added).

- 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. The contents of filing shall include but not limited to the basic information of data such as sources, categories, levels, size, carriers, handling purposes and methods, use scope,

responsible subjects, outbound sharing, cross-border transfer, and security protection measures, exclusive of the data content itself.

- Article 21: The key data and core data generated and collected by the data handlers in the fields of industry and information technology within the territory of the People's Republic of China shall be stored within the territory of the People's Republic of China if laws or administrative regulations have such requirements. *Should the data need to be provided abroad, a data cross-border transfer security assessment shall be carried out* according to laws and regulations. ... Without the approval of the Ministry of Industry and Information Technology, the data handlers in the fields of industry and information technology shall not provide foreign industrial, telecommunication and radio law enforcement agencies with data in the fields of industry and information technology that is stored within the territory of the People's Republic of China.

- Article 24: In case of cross-entity provision, transfer or entrusted handling of core data, the data handler in the fields of industry and information technology shall assess security risks, and take necessary security protection measures; the case shall be reviewed by the sector-specific regulatory department in the region and reported to the Ministry of Industry and Information Technology. The Ministry of Industry and Information Technology shall conduct review according to the relevant regulations.

- Article 31: The Ministry of Industry and Information Technology shall develop a sector-specific data security assessment management system to manage the assessment institutions; develop a specification for assessment of sector-specific data security, to guide the assessment institutions to carry out data security risk assessment, cross-border transfer security assessment and other work. The local sector-specific regulatory departments shall be responsible for carrying out the data security assessment work in their own regions respectively. 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 on their own or by entrusting a third-party assessment institution, make timely rectifications over risk issues, and send a risk assessment report to the sector-specific regulatory department in their own regions.

China – Technical Specification for Cross-Border Processing of Personal Information: On December 16, 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. It states in relevant part as follows (emphasis added):

> In carrying out cross-border processing activities, personal information handlers applying for personal information protection certification shall comply with the requirements of *GB/T 35273 Information security technology – Personal information security specification* and this document. This document … provides a basis for certification bodies to conduct an assessment over personal information cross-border processing activities of personal information handlers, and providing reference for personal information handlers to lawfully carry out personal information cross-border processing activities as well.
> …
> Personal information handlers who apply for certification shall obtain a lawfully issued legal person certificate, operate normally and have a good reputation and goodwill. Where a personal information cross-border processing activity takes place between subsidiaries or

affiliates of a multinational or an economic or noneconomic entity, the party located in China may apply for certification, and assumes legal liability. For an overseas personal information processor specified in the second paragraph of Article 3 of the Personal Information Protection Law of the People's Republic of China, its China-based office or its designated representative may apply for certification, and assumes legal liability.

A legally binding and enforceable document shall be entered into between the personal information handler and the overseas recipient in a personal information cross-border processing activity, to ensure the rights and interests of personal information subjects are fully protected. The document shall at least specify the following contents:

a) Basic information of the personal information handler and the overseas recipient, including but not limited to name, address, contact person's name, contact information, etc.;
b) Purpose of the cross-border processing of personal information, and the scope, types, sensitivity, volume, processing method, retention period, storage location and the like of personal information;
c) Responsibilities and obligations of the personal information handler and the overseas recipient for personal information protection, technical and management measures taken to prevent possible security risks caused by the cross-border processing of personal information, etc.;
d) Rights of personal information subjects, and the ways and methods to protect the rights of the personal information subjects;
e) Remedy, cancellation of contract, liability for breach of contract, dispute settlement, etc.;
f) The overseas recipient undertakes to honor the same personal information cross-border processing rules, and ensures that the protection of personal information is not lower than the standard specified in the laws and administrative regulations of the People's Republic of China on personal information protection;
g) The overseas recipient undertakes to subject itself/himself to the continuous supervision of the personal information cross-border processing activities by the certification body;
h) The overseas recipient undertakes to accept the jurisdiction of the laws and administrative regulations of the People's Republic of China on personal information protection;
i) Clarifying the organization assuming legal liability within the territory of the People's Republic of China, and undertaking to fulfill the obligation of personal information protection;
j) Both the personal information handler and the overseas recipient undertake to assume civil legal liability for the infringement of the personal information rights and interests, and explicitly agree on the civil legal liability to be borne by both parties;
k) Other obligations that are specified by laws and administrative regulations and shall be fulfilled.

China – National Technical Standard re Cybersecurity Requirements for Critical Information Infrastructure Protection: On November 7, 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). This is reportedly China's first national standard for critical information infrastructure ("CII") security protection. It establishes cybersecurity requirements for CII protection in areas such as analysis and identification, security protection, testing and evaluation, monitoring and early warning, active defense, incident disposal, etc., aiming to take necessary measures to protect the continuous operation of CII business and its important data from damage. The technical standard includes the following "data security" requirements (emphasis added):

Requirements for data security protection include:

a) Shall establish data security management responsibilities and appraisal and assessment system, prepare data cybersecurity plan, implement data security technology protection,

carry out data security risk assessment, develop data security incident emergency plans, dispose of security incidents in a timely manner, and organize data security education and training.

b) Shall establish data cybersecurity policies based on data categorization and classification, and specify the corresponding measures for the protection of important data and personal information.

c) Personal information and important data collected and generated during operations in China will be stored within the territory of China. If, due to business needs, it is necessary to provide data abroad, security assessment shall be conducted in accordance with the relevant national regulations and standards. Where there are other provisions in laws or administrative regulations, such provisions shall prevail.

d) Shall strictly control the use, processing, transmission, provision and disclosure and other key aspects of important data, and adopt encryption, desensitization, de-identification and other technical means to protect the security of sensitive data.

e) Business continuity management and disaster recovery backup mechanisms shall be established, and important systems and databases shall be backed up off-site.

f) If the data availability requirement is high, the database remote real-time backup measures shall be taken, and if the business continuity requirement is high, the system remote real-time backup measures shall be taken to ensure that once the critical information infrastructure is damaged, it can be restored and remedied in a timely manner.

g) When the critical information infrastructure is decommissioned, the stored data shall be processed in accordance with the data security protection policies.

h) The security capability of the whole process of data processing activities shall be established, which shall comply with the requirements of relevant national standards on data cybersecurity protection

China – 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 procedural matter, the rules provide for a Certification Implementation Process, which includes: (1) a certification application process, (2) a technical verification of the application by the technical verification body, (3) an on-site audit, (4) the certification body's certification decision (based on an assessment and approval of certification results), and (5) post-certification supervision. 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. Additional coverage here: Reed Smith, ODP, Han Kun, Bird & Bird.

China – Beijing Municipal Regulations on the Promotion of Digital Economy: On November 25, the City of Beijing published Municipal Regulations on the Promotion of Digital Economy in order to "turn Beijing into a global benchmark city in practicing digital economy." Relevant provisions include:

- Article 29: The commerce department shall, in conjunction with relevant departments, promote the high-quality development of digital trade, ...support the development of cross-border trade, cross-border logistics and cross-border payments, boost the international mutual recognition of digital certificates and electronic signatures, construct international Internet data dedicated channels, international data and information dedicated channels and application support platforms based on advanced technologies such as blockchain so as to provide facilitation for the product delivery and settlement in digital trade.

- Article 48: In carrying out data processing activities, an entity shall establish a data governance and compliance operation system, fulfill data security protection obligations, strictly implement relevant systems such as those regarding legal use of personal information, the commitment to the safe use

of data and the security management over cross-border transfer of key data, and based on application scenarios, conduct a security assessment over anonymization and de-identification technologies, and take necessary technical measures to strengthen the protection of personal information security, to prevent illegal abuse.

- Article 56: Work to encourage the expansion of international cooperation in the field of digital economy, support participation in the development of international rules, standards and agreements, set up cooperation platforms such as international exhibitions, forums, commerce & trade fairs, competitions and training, and achieve mutual benefit and win-win cooperation in the fields of cross-border flow of data, opening up of the digital service market, and digital product security certification.

China – Technology Import Prohibition/Restriction Catalogue: On November 5, China's Ministry of Commerce (MOFCOM) released the finalized *Technologies Import Prohibition/Restriction Catalogue* with immediate effect. The Catalogue imposes significant cross-border restrictions on import and export of certain key technologies, especially encryption technologies, predictive algorithms for push services, and artificial intelligence services.

D. India

India – Trade Policy Forum with the United States: The next US-India Trade Policy Forum (TPF) is scheduled for January 11, 2023. GDA staff has communicated with both US and Indian negotiators over the last several years to underscore the importance to both economies of ensuring that US-India cross-border data transfers and technology access is not unduly interrupted. Along with other industry groups, the GDA has also supported the establishment of a US-India bilateral focus group dedicated to trade-related digital governance issues. Such a focus group could supplement the existing five TPF focus groups covering: (1) Services, (2) Agriculture, (3) Investment, (4) Innovation and Creativity, and (5) Tariff and Non-Tariff Barriers. The TPF meeting will be co-chaired by Commerce and Industry Minister Piyush Goyal and US Trade Representative Katherine Tai. The previous TPF meeting was held on November 23, 2021, after a gap of four years here. *See* BSA Nov. 2021 letter.

India – Trade Negotiations with the EU: On December 2, India and the EU concluded their third round of negotiations towards an EU-India trade agreement. This round was also the first formal negotiation over digital trade and cross-border data transfer matters. The EU has proposed cross-border data transfer and data localization provisions reportedly in line with its negotiating positions at the WTO and with New Zealand, Chile and other trading partners.

India – Digital Personal Data Protection Bill: On December 16, the GDA filed comments in response to the November 18 publication by the Ministry of Electronics and Information Technology (MeitY) of the Digital Personal Data Protection Bill, 2022. 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. GDA recommended that the Bill be revised:

- 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.
- 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.
- 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.

India – 2023 G20 Host Year: *See entry under G20.*

E. Indonesia

Indonesia – 2022 G20 Host Year: *See entry under G20.*

F. Japan

Japan – Meetings with the US on Digital Issues: On January 5, 2023, Commerce Secretary Gina Raimondo met with Japan's Minister of Economy Trade and Industry, Yasutoshi Nishimura, to discuss shared US-Japan technology priorities – some with cross-border data implications. Among other things, both sides discussed the US-Japan collaboration relating to critical and emerging technologies, such as quantum computing, including through R&D and export controls.

Japan – Digital Partnership with the UK: On December 7, Japan and the UK agreed to establish a digital partnership aiming to elevate bilateral cooperation on digital and data policies. The initial focus of this Partnership focuses on four pillars: (1) digital infrastructure and technologies; (2) data; (3) digital regulation and standards; and (4) digital transformation. Under the Data Pillar, the two sides have committed to address the following:

> a. Championing Data Flows: Maintain, expand and promote the safe international flow of data and operationalise Data Free Flow with Trust initiatives.
>
> b. Regulatory Cooperation: Support collaboration between both Participants' data protection regulators to provide regulatory certainty for UK and Japanese businesses and citizens, and explore further opportunities for both Participants to promote regulatory cooperation both bilaterally and within multilateral fora.
>
> c. Data Innovation: Explore opportunities for joint collaboration on data innovation (for example on Privacy Enhancing Technologies (PETs), sharing information on distributed data managing systems such as Japan's Trusted Web initiative, and compare approaches on improving data sharing and international standards).

Under this partnership, the two sides are also planning to coordinate digital policy development aimed at fostering competition, promoting human-centric application of artificial intelligence, and ensuring a reliable supply of semiconductors and a diversity of vendors in the 5G telecom supply chain.

Japan – Economic Partnership Negotiations with the EU: On October 24, the EU and Japan launched negotiations relating to rules on cross-border data flows under the EU-Japan Economic Partnership Agreement. According to DG Trade, the negotiations demonstrated that Japan and the EU have the same goals in balancing the importance of data transfers and ensuring data security and data privacy, although both countries have adopted different approaches to achieve that outcome.

Japan – Supplementary Rules re EU-Japan and UK-Japan Data Transfers: Japan's Personal Information Protection Commission has launched a public consultation (Japanese link) on the draft partial amendment of Supplementary Rules under the Act on the Protection of Personal Information ("APPI") for the Handling of Personal Data Transferred from the EU and the United Kingdom based on an Adequacy Decision (Japanese link).

- Following the Japan-EU mutual adequacy decision which came into force in January 2019, with Supplementary Rules to APPI adopted to bridge differences to ensure high level of protection, and the adequacy decision remaining in effect with the UK after UK's exit from the EU in 2020, this mechanism has been under review since 2021.

- The discussion has proceeded with the only issue remaining on the "pseudonymously processed information" which was introduced in the 2020 amendment of APPI.* To resolve the difference, following has been added to the Supplementary Rules: *"Pseudonymously processed Information*

*obtained by processing personal information provided from within the EU or the UK based on adequacy decision shall be handled in accordance with Article 41 of the Act.** In addition, such pseudonymously processed information shall be handled only for statistical purposes. In this case, statistical purposes mean the purposes of statistical surveys or any other processing to produce statistical results, and the statistical results produced by such processing are aggregate data and shall not be used to support any action or decision with respect to a specific individual."*

Japan – 2023 G7 Host Year / DFFT: *See entry under G7.*

G. Korea

Korea – Digital Partnership Agreement with Singapore: On December 21, 2022, the Korea-Singapore Digital Partnership Agreement (KSDPA) entered into force. The KSDPA contains several important provisions on data transfers. While the KSDPA contains helpful language on financial data transfers, consistent with GDA's prior submission on the same topic, the final agreement regrettably does not prohibit data localization mandates relating to financial services data, in contrast to several other regional agreements. *Cf,* AU-SG DEA (Art. 25), AU-HK FTA (Art. 11.15), SG-UK DEA (Art. 8.54), AU-UK FTA, and UK-JP CEPA. Relevant provisions include the following:

- Article 14.14: Neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of business of a covered person. However, a Party may - to achieve a legitimate public policy objective - adopt measures inconsistent with this obligation, provided that such measures are not discriminatory or more restrictive of data transfers than required.

- Article 14.15: Neither Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. However, a Party may derogate from this obligation on the same terms as outlined in Art. 14.14.

- Article 14.16: Location of Computing Facilities for Financial Services: The Parties recognise that the ability of covered financial persons to aggregate, store, process and transmit data across borders is critical to the development of the Parties' financial sectors. The Parties further recognise that the ability of covered financial persons to use data and technology comprehensively across borders to supply financial services offers a range of benefits, including enhanced risk management capabilities, increased efficiency and operational effectiveness, insights that support innovation, improved consumer welfare, and others. … [T]he Parties shall endeavour to share information regarding: (a) cross-border access to financial information by financial regulatory authorities on an "immediate, direct, complete and ongoing" basis; (b) joint initiatives to facilitate covered financial persons to use or locate computing facilities outside of a Party's territory… provided that financial regulatory authorities have necessary access to financial regulatory information.

- Article 14.17: Personal Information Protection: Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of persons who conduct or engage in electronic transactions... [E]ach Party shall take into account [inter alia] principles reflected in the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, [including]: limitation on collection; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability… Each Party shall encourage the development of mechanisms to promote compatibility and interoperability between these different approaches.

- Article 14.25: Data Innovation: … To support the cross-border transfer of information by electronic means and promote data-driven innovation in the digital economy, the Parties … recognise the need to create an environment that enables and supports, and is conducive to, experimentation and innovation [including through] collaborating on data-sharing projects, including projects involving researchers, academics and industry…

Korea – UK-Korea Data Bridge: On November 23, 2022, the United Kingdom issued an adequacy decision vis-à-vis the Republic of Korea, its first independent adequacy decision since its department from the EU. This final decision follows a July 2022 agreement in principle. Notably, the UK's adequacy decision is broader than the EU's adequacy for South Korea. For example, UK organizations will be able to share personal data related to credit information with Korea to help identify customers and verify payments – credit information is excluded from EU adequacy. The UK estimates that its adequacy decision will generate an estimated £14.8 million in annual business savings and increased exports. The UK is working on several other adequacy decisions, including the adequacy between the UK and the US, which is expected soon.

Korea – Digital Partnership with the EU: On November 29, the Republic of Korea signed a Digital Partnership with the European Union. The EU-ROK Digital Partnership sets out a framework for cooperation across various issues including infrastructures, skills, digital transformation of businesses, and digitalisation of public services, as well as digital economy and trade. The Digital Partnership is not a binding agreement, but sets out an agreed initial set of joint activities both parties will collaborate on. Notable collaborations include the following:

- **Data related Laws and Systems:** Both sides recognise that ensuring the free and trusted flow of data across borders in compliance with data protection rules and other public policy objectives, including public security and public order, is fundamental to unlock the benefits of digitalisation. Both sides agree to cooperate on supporting international data flows with trust including for instance by promoting the convergence of data protection rules, building upon the existing adequacy decision for the transfer of personal data, and to explore ways to develop and implement data policies aiming to foster the data economy.
- **Digital Trade:** Both sides should deepen their understanding of digital trade to be reflected in a set of digital trade principles building on the ROK-EU FTA and covering issues relevant for digital trade such as, inter alia, paperless trading, electronic invoicing, electronic transactions framework and digital identities, online consumer protection, the protection of source code, and cryptography. Both sides intend to discuss and, when relevant, share information, with a view to coordinating their approaches regarding digital protectionist measures adopted by third countries

H. Singapore

Singapore – Digital Partnership with EU: On December 15, the EU and Singapore announced the conclusion of a new EU-Singapore Digital Partnership Agreement. A joint statement by European Commission's President von der Leyen and Singapore's Prime Minister Lee states: "Partnership will advance cooperation on the full range of digital issues, including trade facilitation, trusted data flows and data innovation, digital trust, standards, digital skills for workers, and the digital transformation of businesses and public services." The EU and Singapore have also agreed on a set of Digital Trade Principles, as a first deliverable of their Digital Partnership. These principles reflect joint commitment to an open digital economy and provide a common framework to boost digital trade between the two parties and globally. "We aim to build on these principles to enact a set of bilateral digital trade rules. We believe that the forward-looking digital trade engagements between the EU and Singapore will complement and support ongoing WTO negotiations to put in place global rules on electronic commerce," – reads the statement.

Singapore – International Cyber Week: From October 18-20, Singapore held its annual International Cyber Week. The Cybersecurity Agency of Singapore (CSA) made announcements including the appointment of a Global Forum on Cyber Expertise (GFCE) Southeast Asia liaison position to grow existing cyber capacity building efforts in ASEAN and launch of an Internet Hygiene portal (IHP) to serve as a one-stop platform, providing SMEs with easy access to resources and self-assessment tools for enterprises to adopt internet security best practices. CSA has plans to expand the IHP to sectors prone to cyber attacks, including banking, finance and healthcare. Also announced was ASEAN Regional Computer Emergency Response Team (CERT), which will operate as a virtual center comprising incident responders from across member states, each sharing information during security incidents that occur in any of the respective nation.

Singapore – Revised PDPA Financial Penalty Limits: On October 1, the Personal Data Protection Act's revised financial penalty caps came into effect. Penalties are now set at up to SG$1 million or 10% of an

entity's annual turnover in Singapore (whichever is higher). More information here and here. These penalties would potentially apply to breaches of PDPA provisions relating to data transfers, including Article 26 relating to the "Transfers of personal data outside of Singapore."

I. Taiwan

Taiwan – Initiative on 21st Century Trade: January 14-17, 2023 will are the dates for the next negotiating round of the US-Taiwan Initiative on 21st-Century Trade. Office of Trade Negotiations Chief of Staff Hsiao Chen-Jung has said that the trade office "expects to sign some of the 11 components of the U.S.-Taiwan Initiative on 21st-Century Trade over the next two and a half months after talks began in mid-August," and that Taiwan hopes for the initiative to be finalized by the end of next year, according to the South China Morning Post. The GDA's negotiating recommendations are linked here.

Taiwan – Economic Prosperity Partnership Dialogue: On December 14, the US and Taiwan held discussions under the US-Taiwan Economic Prosperity Partnership Dialogue (EPPD) - an economic initiative being led by the State Department. This initiative complements ongoing negotiations under the US-Taiwan 21st Century Trade Initiative, which are being led by USTR. The GDA continues to highlight the importance of ambitious cross-border data commitments by both sides in those negotiations, following GDA comments to Taiwan and the United States earlier this year.

J. Thailand

Thailand – Draft Notification of Appropriate Personal Data Protection for International Transfer under the Personal Data Protection Act 2019: On October 24, the GDA submitted comments to Thailand's Personal Data Protection Committee Office (PDPC Office) on its draft notification on international transfers. The GDA asked Thailand to adopt approaches that are interoperable with prevailing international norms in relation to standard contractual clauses, binding corporate rules, and other data transfer mechanisms in Thailand. The draft notification includes two Appendices with standard contractual clauses. Our comments are based on the unofficial English translation of the draft notification provided by PDPC Office.

K. Vietnam

Vietnam – On December 23, the GDA filed comments with Vietnam's Ministry of Information and Communication (MIC) regarding a proposal to update the 2009 Law on Telecommunications. Within the draft law is the inclusion of a new Chapter X that governs data center and cloud computing services. Among other requirements, such services must register with the MIC and comply with Vietnam-specific standards and technical regulations. Within Article 75.1 of the draft law is a possible requirement for data localization: "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. 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.

Vietnam – Multi-Industry Statement on Vietnam's Data Localization Mandates and Data Transfer Restrictions: The GDA continues to engage with Vietnam on the continuing proliferation of cross-border data restrictions and data localization requirements in Vietnamese law and practice. In the past 16 months, the GDA has submitted comments on data localization and related data restrictions in Vietnam in April 2021, September 2021, November 2021, December 2021, September 2022, and December 2022.

EUROPE

A. European Union

EU – European Commission released draft adequacy decision for the EU-US Data Privacy Framework. On December 13, the European Commission released its draft adequacy decision on EU-US data transfers,

paving the way for the adoption of the EU-US Data Privacy Framework. This framework will be built similarly to the EU-US Privacy Shield, whereby US entities will be able to benefit from the Framework by committing to comply with a detailed set of privacy obligations. EU citizens will benefit from several redress avenues if their personal data is handled in violation of the Framework, including free of charge independent data protection review court.

The formal approval will involve obtaining a non-binding opinion from the European Data Protection Board (EDPB) and the approval from a committee composed of representatives of the EU Member States. Once this procedure is completed, the Commission will adopt the adequacy decision for the US. The formal approval is expected to happen before the summer of 2023. The EDPB is expected to release a draft opinion on the US adequacy decision in February and adopt their final opinion in April. The Commission is expected to socialize the draft adequacy decision with the "article 93 Committee" of the Council in the coming weeks and hold periodic talks with the Member States to ensure a swift adoption of the decision by mid-2023.

Bruno Gencarelli (Head of "International data flows and protection" Unit at DG Justice) has explained that before the final adoption of the adequacy decision, the European Commission expects the US government to take a number of steps to fully operationalize the new agreement, including:

- The adoption of new policies and procedures by intelligence agencies to ensure that their activities are: (1) meeting specified legislative objectives; (2) proportionate to address a specific risk; (3) subject to a process to validate collection priorities; (4) subject to oversight re how data is collected; and (5) subject to processes for reporting non-compliance with the foregoing requirements;
- The setting up of the new redress process, centered on a new data protection review court.

The functioning of the EU-U.S. Data Privacy Framework will be subject to **periodic reviews**, which will be carried out by the European Commission, together with European data protection authorities, and the competent US authorities. The first review will take place within one year after the entry into force of the adequacy decision, to verify whether all relevant elements of the US legal framework have been fully implemented and are functioning effectively in practice.

The GDA has actively advocated on this issue since mid-2019, including through an EU Industry Report on Transatlantic Data Transfers; a US Industry Position Paper; a Letter to Presidents Biden and von der Leyen, a GDA White Paper, a Report on Strengthening Transatlantic Data Flows, a Privacy Shield Report, and numerous press statements and other materials. The GDA also hosted a panel event in October 2022 to build support for the new framework.

For more information on US Executive Order and related procedures, please see entry under United States

EU – Schrems II Enforcement by DPAs: On December 15, the Spanish Data Protection Agency ("AEPD") issued the latest in a long line of decisions by European DPAs regarding the transfer of data to the United States via the Google Analytics tool from the European Economic Area (EEA). In contrast to earlier DPA decisions, the AEPD concluded that the use of the Google Analytics tool by the Royal Spanish Academy (RAE), a government organization, did not breach the GDPR. Specifically, RAE ensured that only aggregated information was processed – not information that could be used to identify persons. AEPD also noted that RAE stopped using Google Analytics after the Schrems II decision. This decision follows decisions or statements by DPAs in:

- Denmark (September 21 decision; September 8 Aarhus decision; August 8 Helsingør decision; July 2022 statement, Jan. 2022 statement)
- Austria (Oct. 2021, April 2022),
- Germany (Berlin DPA)
- France (CNIL ruling)
- Guernsey (DPA ruling)
- Italy (Garante June 23 ruling), and
- The Netherlands (Dutch DPA statement).

EU – Hamburg DPA Statement on EU-US Data Transfers. On November 29, a Hamburg Commissioner for Data Protection and Freedom of Information has published an analysis of the US President Joseph Biden's Executive Order on Enhancing safeguards for US signals intelligence activities**.** The analysis identifies certain challenges, such as "it is not clear from the text of the Executive Order to what extent the new proportionality requirement specifically influences the bulk surveillance," or regarding judicial review that it lacks the provisions on "information in the [court's] judgments about whether and what measures have been taken". However, it seems that the analysis is overall rather positive regarding the proportionality criteria applied to national surveillance and a new Data Protection Review Court. At the same time, the conclusion of the Hamburg Commissioner is clear – "the Executive Order deserves a reasoned, open-ended review" and the European Commission in its adequacy decision has to "thoroughly examine the legal guarantees" and "keep an eye on future developments".

EU – Cybersecurity Certification Requirements. On November 29, at the American Chamber of Commerce Conference on Transatlantic Digital Economy a former European Commissioner, Andrus Ansip, who is now a Member of European Parliament's center-right Renew Europe political group, warned the EU about its plans on data localization and protectionist technology standards and cybersecurity schemes. He said that data localization "would be a mistake because Europe won't be able to boost its artificial intelligence sector if it doesn't have access to non-EU data" and protectionist technology standards "are creating a mess", stressing that a free-market economy is of key importance.

Relatedly, a group of eight EU governments – Denmark, Estonia, Greece, Ireland, Lithuania, Poland, Sweden and the Netherlands – have expressed concerns regarding the EU's proposed cloud certification requirements, warning that the cloud certification rules proposed by the EU cybersecurity agency, ENISA, could breach the EU's international trade commitments. The draft rules suggest that non-EU cloud providing companies have to move their headquarters to the bloc, limit the non-EU stakes to less than 39 percent and demonstrate they are out of reach of data-access rules in non-EU countries. "Any possible measures should not breach existing or hamper future (bilateral, plurilateral or multilateral) trade agreements between the EU and third countries," states the position paper issued at the end of September. Similar concerns are expressed by digital industry associations from central and eastern European countries – Lithuania, Czech Republic, Slovakia and Poland, which have warned that the certification process as proposed could "override" WTO rules and be "considered protectionist" by trade partners.

EU – EDPB Recommendations on BCRs: On November 16, the European Data Protection Board (EDPB) has issued its draft Recommendations 1/2022 on Controller Binding Corporate Rules under Art. 47 GDPR (C-BCR). The draft Recommendations 1/2022 apply to C-BCR, which can be used as legal mechanism for transfers of personal data from controllers subject to the GDPR to other entities of the same company group established outside the EEA also acting in the role of controllers or "group-internal" processors. Amendments include the following:

- Amendments to transparency obligations regarding the appointment of processors (Sec. 5.3) and to obligation to list all applicable legal basis of processing (including local laws) and applicable exemptions for processing special categories of personal data (Sec. 5.1.2);

- Introduction of additional mandatory content for the C-BCR text, which was formerly only required to be provided in the application form, such as details on the audit programme covering the C-BCR (Sec. 3.3).

- Expansion of data subject rights, including provisions on legal remedies, compensation (Sec. 1.3.2) and new rights concerning government access requests (Sec. 1.3.1).

- Strict requirements on the publication of the C-BCR, similar to a privacy notice (Sec. 1.7), as well as the obligation to notify all data subjects of any changes of the C-BCR text and its member list (Sec. 1.3.1), although it is not specified how such update notices shall be provided.

- New safeguards to avoid conflict of interests of the data protection officer competent for the C-BCR, e.g., the prohibition for the DPO to conduct data protection impact assessments or audits related to the C-BCR (Sec. 3.4).

EU – Sweden's Government Reveals Trade Priorities For 2023 Council Chairmanship: After a general election in September 2022, a new government was formed in Sweden with Ulf Kristersson as the Prime Minister, leading a right-wing minority three-party coalition government with his Moderate party (liberal-conservatives) joined by the Christian Democrats and Liberals. Johan Forssell (Moderate party) was appointed as the country's trade minister. The new trade minister revealed Sweden's priorities for the European Council Presidency as the country prepares to take over the chairmanship of the European Council for six months in January 2023. Sweden will aim "to do what they can to improve the relationships between the EU and the US." Sweden will also aim to bring progress in the digital trade chapters in free trade agreement negotiations with Australia, New Zealand, India and Indonesia.

EU – Stronger emphasis on trade negotiations: In the conclusions published on October 17, the European Foreign Affairs ministers (Trade) put a stronger emphasis on concluding trade deals in order to support a green and just economic growth. "The Council considers that new policy orientations for sustainable trade agreements, coupled with the new drive for engagement with partners, against the backdrop of a new geopolitical situation caused by Russia's war of aggression against Ukraine, are necessary to build broad support for the advancement of the proactive and balanced EU's trade agenda based on sustainability, fairness and open market. … "The Council looks forward to the new approach ensuring the EU's capability to negotiate, conclude and implement new trade agreements swiftly."

EU – Digital Partnership with Singapore: *See entry under Singapore*.

EU – Digital Partnership with Korea: *See entry under Korea*.

B. France

France – CNIL Announcement re Standard Contractual Clauses: On December 21, France's data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), issued an issued an announcement noting that "[d]ata exporters and importers will no longer be able to use the old European Commission standard contractual clauses and will either have to use the clauses updated in 2021 or use another transfer tool."

C. Ukraine

Ukraine – Digital Economy Agreement with the United Kingdom: On November 30, the UK and Ukraine announced the conclusion of digital economy agreement negotiations. The agreement includes outcomes on data transfers and personal data protection, described as follows by the UK:

> Guaranteed cross-border data flows: The agreement will enable the free flow of trusted data between the UK and Ukraine for business purposes by preventing unjustified restrictions to cross-border data transfer. This means that trade can flourish between both countries. This does not prevent the UK or Ukraine placing restrictions on cross-border data transfers if these are introduced to achieve a legitimate public policy objective; for example, the protection of personal data. This exemption requires that any restrictions are no more restrictive than required to achieve the stated public policy objective. Such restrictions also cannot be applied in a way that would represent an arbitrary or unjustifiable discrimination or a disguised restriction on trade.
>
> Personal data protection: The deal safeguards the UK's high standards on personal data protection and locks in a requirement for personal data to be protected in both countries. The

deal ensures that both the UK and Ukraine maintain domestic data protection regimes and draw on world-leading international principles and guidelines in their design.

D. United Kingdom

United Kingdom – Free Trade Agreement / Digital Economy Agreement Negotiations: On November 4, the GDA engaged with the UK and its trading partners re cross-border data policies in ongoing UK trade negotiations with Canada, India, Israel, Mexico, Switzerland, Ukraine, as well as the CPTPP Parties and the Gulf Cooperation Council. The GDA made submissions to the UK government and UK trading partners including Israel, Mexico, Switzerland, and the Gulf Cooperation Council.

United Kingdom – Data Protection Reforms: On October 3, the UK government announced a goal of reforming *inter alia* the cross-border aspects of UK data protection laws, given the "disproportionate burden to small businesses" from a "one-size-fits-all" approach reflected in the GDPR. Relatedly, on November 2-4, Members of the European Parliament Civil Liberties, Justice, and Home Affairs Committee visited the UK to "to better understand the direction the UK's data protection reform is heading and whether these changes impact the UK's adequacy status under the GDPR."

United Kingdom - US-UK Data Agreement: On October 3 the US-UK Data Access Agreement entered into force. According to a US-UK Joint Statement, the Agreement reflects a renewed bilateral commitment to tackling the threat of serious crime, and is "the first agreement of its kind, allowing each country's investigators to gain better access to vital data to combat serious crime in a way that is consistent with our shared values and mission of protecting our citizens and safeguarding our national security." Such agreements can help address one of the purported policy rationales for data localization measures.

United Kingdom – Transfer Risk Assessment Tool: The UK Information Commissioners' Office (ICO) has published a new Transfer Risk Assessment tool (TRA). The TRA enables organizations to make a restricted transfer when they plan to rely on one of article 46 transfer tools, such as the International Data Transfer Agreement (#IDTA). The TRA helps organizations to ensure that the article 46 transfer tool provides appropriate safeguards in the particular circumstances of your restricted transfer. The tool also contains: (a) a list of UK GDPR special categories of data; (b) a list of typical categories of PD with an initial risk score; and (c) examples of extra steps and protection to consider for transfers.

United Kingdom – UK-Korea Data Bridge: *See entry under Korea*.
United Kingdom – UK-Ukraine Digital Economy Agreement: *See entry under Ukraine.*
United Kingdom – UK-Japan Digital Partnership: *See entry under Japan.*

MIDDLE EAST

A. Israel

Israel – Proposed Regulations re Data Transfers from the European Economic Area (EEA): On November 29, in conjunction with the EU's review under GDPR Art. 45 of the adequacy of Israel's system of personal data protection, Israel has proposed new regulations re certain data transfers from the EEA. According to the Israeli authorities, maintaining adequacy "has broad economic significance for the Israeli economy, as well as great importance in terms of the foreign relations of the State of Israel." The proposed regulations establish four obligations that will apply to database owners in Israel, in relation to information transferred to Israel from EEA: the obligation to delete information, the restriction on the possession of unnecessary information, the obligation to accurately provide information, and the obligation to inform.

Israel – Trade Negotiations with the United Kingdom: *See entry under United Kingdom.*

B. Saudi Arabia

Saudi Arabia – Personal Data Protection Law: On December 15, the GDA filed comments in response to a public solicitation for input from the Saudi Authority for Data and Artificial Intelligence regarding proposed amendments to the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 9/2/1443 AH. The GDA's recommended that Saudi Arabia:

- Adopt the so-called "Accountability Principle," and remove the presumption in draft Article 28.1.a that personal data transfers are to be prohibited to all or most other countries;
- Replace the requirement for "no less" standards of protection with a requirement for "broadly equivalent" standards of protection;
- Explore approaches in Article 28 to ensure that appropriate transfer mechanisms are available under Saudi law and interoperable with other global frameworks, including through cross-border data transfer mechanisms such as 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;
- Revise and clarify the statutory exceptions in Article 28.2 relating to the public interest, international commitments, and contract obligations to ensure that they can operate as intended.

C. United Arab Emirates

UAE – DIFC Data Transfer Risk Matrix: On October 5, the Commissioner of Data Protection at the Dubai International Financial Centre (DIFC) issued an Ethical Data Management Risk Index (EDMRI) to:

> [P]rovide an exporting organization with a way of knowing quickly, efficiently, and with regulatory certainty, what may be expected of a company or other importing organization in any given jurisdiction. The EDMRI is akin to a regulatory compliance and risk assessment... [along with] … the EDMRI+ [which contains] … a set of questions that can be used as a
> - basis for a more detailed Transfer Impact Assessment (TIA);
> - way to determine whether additional contractual obligations should be factored into a services agreement or transaction;
> - general compliance management tool within an organization, as a part of a technical or organizational policy or procedure, to add to a compliance program arsenal of safeguards…
>
> Each country's risk index is hyperlinked to the research narrative, detailing the compliance indicators and responses as assessed by an independent third party.
>
> What is also interesting to note is that many of the countries on the index below have data protection laws, some of which are deemed "adequate", yet when it comes to risk of non-compliance by the importing organizations in that jurisdiction, it can still be quite high. This is what exporters need to ascertain and mitigate before transfers, direct or onward, occur. Please review the EDMRI FAQs, available here, for more details.

The DIFC's Index treats as "low risk" data transfers to Australia, Canada, Japan, Korea, Malaysia, Mexico, New Zealand, South Africa, the United Kingdom, and many EU jurisdictions. It treats as "medium risk" data transfers to Brazil, China, Germany, Indonesia, Kenya, Nigeria, Russia, and the United States (among others). It treats as "high risk" data transfers to Bangladesh, India, Pakistan, and Vietnam (among others).

UAE – Joint Statement on Cross-Border Data Flows with the US: On November 22, the United Arab Emirates and the United States issued a Joint Statement on Cross-Border Data Flows. USG Press Statement here. UAE Press Statement here. The Joint Statement provides as follows:

> The United States and the United Arab Emirates recognize that the ability to aggregate, store, process and safely transmit data across borders is critical to the development of the digital economy, digital trade and innovation.
>
> The accelerating digitization of the modern global economy and the increasing use of technology to supply services can offer a range of benefits, including empowering workers and consumers, enhancing risk management capabilities and increasing innovation and economic growth. These developments also pose new challenges for policymakers and regulators. The United States and the United Arab Emirates are committed to working together and with other countries to promote a digital economy that empowers individuals, including through strong and effective privacy protections, and fosters connectivity and development.
>
> The United States and the United Arab Emirates recognize the economic and social benefits of ensuring robust data protections, and enforcement of those protections, while promoting interoperable mechanisms that facilitate cross-border data transfers across economies with different regulatory regimes. Recognizing that our governments may take different regulatory approaches to protecting personal data, we intend to pursue innovative mechanisms to bridge our regulatory differences, promote compatibility and explore interoperability, including through mechanisms modeled after the Cross Border Privacy Rules system. We intend to continue to share information on international frameworks and mechanisms that facilitate the transfer of personal data, and data privacy best practices to promote interoperability between our two privacy regimes.
>
> Based on this shared understanding, the United States and the United Arab Emirates intend to promote adoption and implementation of policies and rules in our bilateral and multilateral economic relationships to help ensure that mechanisms such as certifications are available for cross-border data transfers when necessary or appropriate. The United States and the United Arab Emirates also intend to share information on developments related to these issues.

UAE – Joint Statement on Cross-Border Data Flows with the UK: On December 15, the UK government and the Dubai International Financial Centre Authority (DIFC) issued the following Joint Statement on deepening the UK-DIFC data partnership. The DIFC is a financial free zone which acts as a financial hub for the Middle East, Africa, and South Asia (MEASA) markets:

> We have made significant progress, including obtaining feedback from the UAE government, towards building a robust data bridge: a framework which will facilitate the free and secure flow of personal data following an assessment of the laws and practices that protect data to high standards. Since August 2021, there have been numerous positive, productive, and enlightening technical discussions on how our respective jurisdictions value, protect, and promote the protection of personal data, including when personal data is accessed by government authorities. We also note the issuance of the recent Public Authority Personal Data Sharing Presidential Directive, which lays down requirements for the provision of personal data by DIFC entities to public authorities. The DIFC has already recognised the UK's strong data protections and the UK is now in the advanced stages of its technical data protection assessment of the DIFC.

We agree that the protection of personal data and free flow of personal data across borders can be mutually reinforcing priorities. We are committed to working together to realise the benefits of the important role that the trustworthy use of data across borders plays in international commerce, responsible innovation, and research as well as in empowering, protecting, and delivering better outcomes for individuals, and in sustaining peaceful and prosperous societies.

WESTERN HEMISPHERE

A. Argentina

Argentina – Trade & Investment Framework with the US: On December 1, the US and Argentina held the US-Argentina Trade & Investment Framework Agreement negotiations. According to USTR's announcement, both sides "explored emerging investment opportunities and areas for engagement, including energy transition and digital economy, as well as development finance." The GDA previously highlighted the importance of data transfers in comments on Argentina's draft amendments to the Personal Data Protection bill.

B. Brazil

Brazil – ANPD Leadership: On November 23, Director Miriam Wimmer was reappointed to the National Data Protection Agency (ANPD) for a four-year term.

C. Canada

Canada – Privacy Law Reform: On November 4, the House of Commons raised Bill C-27, the Digital Charter Implementation Act, 2022, for a second reading. The bill would enact the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act (PIDPTA), and the Artificial Intelligence and Data Act (AIDA). Although C-27 does not contain many provisions on cross-border data transfers, it does include a requirement, at Article 62, for organizations to "make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations under this Act," including "(d) whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications." The organization must also make available information re: (a) types of personal information under its control; (b) how it uses that information; (c) circumstances in which it may not seek individual consent; (d) data retention periods; (e) contact information for complaints, and so forth.

Canada – Model Digital Trade Agreement: Following on the GDA comments provided to Global Affairs Canada on the subject of a new model Canadian Digital Trade Agreement, GDA staff will be participating in roundtable "workshops" hosted by Canada as it develops a new model text. Those workshops will focus on Artificial Intelligence, Barriers to Digital Trade (including localization mandates and data transfer restrictions), and Confidence and Trust in the Digital Economy (including trade provisions on cybersecurity, privacy, consumer protection, and so forth).

D. Chile

Chile – Interim Data Transfers Agreement with the EU: On December 21, the EU and Chile finalized an Interim Trade Agreement, which includes a new Digital Trade Chapter containing new provisions on cross-border data transfers and data localization. Article 19.4 provides as follows:

> A Party shall not restrict cross-border data flows taking place between the Parties in the context of activity that is within the scope of this Chapter, by:
>
> (a) requiring the use of computing facilities or network elements in its territory for data processing, including by requiring the use of computing facilities or network elements that are certified or approved in the territory of the Party;
> (b) requiring the localisation of data in its territory;
> (c) prohibiting storage or processing of data in the territory of the other Party; or
> (d) making the cross-border transfer of data contingent upon the use of computing facilities or network elements in its territory or upon localisation requirements in its territory.

Because this article contains a closed list, it does not place any limits on data transfer restrictions or localization measures beyond those specifically enumerated. Furthermore, the EU-Chile Interim Agreement

also contains broad exceptions for putative privacy-related measures. Specifically, Article 19.5 provides as follows: "Each Party may adopt and maintain the measures it deems appropriate to ensure the protection of personal data and privacy, including the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective measures."

E. Mexico

Mexico – Free Trade Agreement Negotiations with the UK: *Please see entry under WTO for more detail on GDA Comments to Mexico re UK-Mexico FTA Negotiations.*

Mexico – WTO JSI Negotiations on Cross-Border Data Policies: *Please see entry under WTO for more detail on GDA Comments to Mexico re WTO JSI Negotiations.*

F. United States

US – Transatlantic Data Privacy Framework: On October 7, 2022, the Biden Administration issued an Executive Order (EO) on the Transatlantic Data Privacy Framework, which was first announced in March 2022.

The EO creates new safeguards on US signals intelligence activities, establishes a new redress mechanism, and enhances US oversight of signals intelligence. The EO will form the basis of an adequacy decision by the European Commission, which would create a successor agreement to the Privacy Shield and facilitate data transfers across the Atlantic. The EO follows a political agreement announced in March by President Biden and European Commission President Ursula von der Leyen. Attorney General Merrick Garland also issued new regulations today establishing a data protection review court, which is central to the new redress process. The EO has two parts:

- First, the EO replaces most of PPD-28 and provides additional safeguards on the collection of signals intelligence. This part of the EO sets out principles pursuant to which US intelligence agencies will collect signals intelligence, including setting out objectives for which agencies may pursue signals intelligence collection and objectives for which intelligence collection is prohibited. It also requires intelligence agencies to draft new policies and procedures, and empowers the Privacy and Civil Liberties Oversight Board (PCLOB) to play an oversight role in those processes.
    - Among other requirements, US intelligence agencies' signals intelligence activities must: (1) meet specified legislative objectives; (2) be proportionate to address a specific risk; (3) be subject to a process to validate collection priorities; (4) be subject to oversight re how data is collected; and (5) be subject to processes for reporting non-compliance with the foregoing requirements.

- Second, the EO creates a new redress process, centered on a new data protection review court. The redress process will begin when the ODNI's civil liberties protection office receives a complaint from a "qualifying state" (filed by the data protection authority in that state on behalf of an individual); the office then must determine if there is a "covered violation" and if so whether there was appropriate remediation of the violation. ODNI will then prepare an administrative record of that determination for review by a new Article II court, which will be established through regulations issued today by the Attorney General. The new court will consist of at least six individuals from outside government who will hear cases in panels; the court will also have the authority to appoint a special advocate to represent views of a complainant and will have binding authority to take corrective action. A few additional details follow.
    - Data Protection Review Court (DPRC): This new tribunal will be established by the Attorney General under Article II of the US Constitution. The DPRC will be staffed by at least six experts in national security law and privacy law who will serve on panels on a part time basis. To help guarantee its independence from the US Executive Branch, DPRC appointees must not be US government employees. Furthermore, DPRC appointees may only be removed from the court for misconduct or neglect of their duties.

- Special Advocate: The DPRC will also appoint a special advocate to represent the interests of the complainant. Special advocates will be drawn from a roster of individuals who have appropriate security clearances. Special advocates will have no legal relationship with the complainant, nor will they serve as attorneys for the complainant. However, they will advocate on behalf of the privacy interests presented by the complainant's position.
- Qualifying State: Claims to the DPRC can only be submitted by "Qualifying States." These may include countries and regional economic organizations, such as the European Union. The Attorney General will designate a country as a Qualifying State on the following grounds. A Qualifying State must: (1) have appropriate privacy protections in its laws for US persons relative to that country's own signals intelligence activities; and (2) allow the free flow of data to the United States (i.e., in the EU context, adequacy would be an important factor). Additionally, the Attorney General must determine that it is in the national security of the United States to designate a country as a Qualifying State. Countries that are designated as Qualifying States will be authorized to forward claims to the DPRC from a complainant in its jurisdiction.

On December 14, the US Office of the Director of National Intelligence released to the public Intelligence Community Directive 126: Implementation Procedures for the Signals Intelligence Redress Mechanism under Executive Order 14086. This Directive governs the handling of redress complaints regarding certain signals intelligence activities, as required by Sections 3(b) and 3(c)(i) of Executive Order 14086. It specifies the process by which qualifying complaints may be transmitted by an appropriate public authority in a qualifying state pursuant to Executive Order 14086. Additionally, and pursuant to the same Executive Order, this Directive authorizes and sets forth the process through which the ODNI Civil Liberties Protection Officer shall investigate, review, and, as necessary, order appropriate remediation for a covered violation regarding qualifying complaints; communicate the conclusion of such investigation to the complainant through the appropriate public authority in a qualifying state and in a manner that protects classified or otherwise privileged or protected information; and provide necessary support to the U.S. Data Protection Review Court.

The EO also renames the relevant agreements, as the EU-US Data Privacy Framework (formerly the Trans-Atlantic Data Privacy Framework) and the EU-US Data Privacy Framework Principles (formerly the Privacy Shield Principles). Program requirements for private sector participants are not expected to change in any material way, so as to ensure that current Privacy Shield participants can continue to benefit from the program on the basis of their original application.

On the EU side, the European Commission to begin its process for making an adequacy determination, now that the EO has been published. The process for approving an adequacy recommendation includes: (1) a proposal from the European Commission; (2) obtaining a non-binding opinion from the European Data Protection Board (EDPB); (3) approval from a committee composed of representatives of the EU Member States (in a comitology procedure, which requires 55% of EU countries that comprise 65% of the EU population approving). Once this procedure is completed, the Commission can adopt the adequacy decision.

US – USTR National Trade Estimate of Foreign Trade Barriers: The GDA submitted comments to the Office of the US Trade Representative (USTR) for the 2023 National Trade Estimate (NTE) report.
The GDA submission noted that "[t]he global economy faces an increasingly challenging environment, which includes the ongoing effects of the COVID-19 pandemic and the war in Ukraine. Among like-minded countries, cross-border digital trade and data transfers hold the potential to ameliorate these effects. Unfortunately, some governments continue to advance policies of data mercantilism and digital protectionism that undermine this potential. Proponents of such policies have cited to broad concepts of "digital sovereignty" or "Internet sovereignty" to justify blocking the cross-border transfer of information, mandating data localization, closing digital markets, interfering with the free flow of information and ideas, and undermining online economic opportunities to the detriment of domestic and foreign citizens, consumers, and companies alike. These trends underscore the critical importance of USTR and counterpart trade authorities sustaining and increasing their collaboration to reduce barriers to cross-border data transfers and digital trade." The GDA submission includes the following major sections:

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

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

US – Annual Special 301 Process on IP and Innovation: On December 15, USTR has announced the launch of the 2023 annual Special 301 cycle. USTR is soliciting input on *inter alia* "acts, policies, or practices of which deny adequate and effective protection for IP rights or deny fair and equitable market access to U.S. persons who rely on IP protection." The GDA filed responsive comments in January 2022, and intends to do so again in 2023.

G. Uruguay

Uruguay – Personal Data Protection Act: On November 3, Uruguay published an updated Personal Data Protection Act (Law No. 20075), which was enacted on October 20. Article 62 includes a new obligation, "[w]hen personal data is collected to inform the owners [of the data] in advance, accurately and unequivocally: of the [t]he existence or not of international data transfers."

Article 62 supplements existing Article 23, which prohibits "[t]he transfer of personal data of any kind with countries or international organizations that do not provide adequate levels of protection," and which allows for special exemptions in the case of (1) international judicial cooperation, (2) exchange of medical data, (3) bank or stock exchange transfers, (4) certain international treaties, and (5) international agreements relating to organized crime, terrorism and drug trafficking. Article 23 also permits data transfers on the basis of (1) consent, (2) performance of a contract requested by or in the interest of the data subject, (3) safeguarding the public interest, rights in a judicial proceeding, or the vital interests of the data subject, or (4) information found in a public registry. Additionally, Uruguayan authorities may authorize cross-border data transfers "to a third country which does not ensure an adequate level of protection, where the controller offers [adequate] guarantees," which "may be derived from appropriate contractual clauses.",

GLOBAL

A. AANZFTA

AANZFTA – Updated ASEAN-Australia-New Zealand Free Trade Agreement: On November 22, Australia, New Zealand and the ASEAN member states substantially concluded negotiations to upgrade the

ASEAN-Australia-New Zealand Free Trade Agreement (**AANZFTA**). The updated AANZFTA contains new chapters and provisions, including on micro, small, and medium sized enterprises, trade and sustainable development and education services. The upgraded agreement will also include enhanced provisions on electronic commerce, competition, customs procedures and trade facilitation, trade in goods, rules of origin, trade in services and investment. See media release here.

B. AfCFTA

AfCFTA – MOU on Trade Cooperation with the United States: On December 14, the Secretary General of the African Continental Free Trade Area (AfCFTA), Wamkele Mene, signed a Memorandum of Understanding on Trade and Investment Between the United States and the African Continental Free Trade Area (AfCFTA). Formal announcement here. Among other things, the MOU prioritizes cooperation on:

- The development of relevant AfCFTA instruments to facilitate responsible digital trade to ensure movement of vital goods and services to households;
- The promotion of the overall implementation of the AfCFTA Agreement, its annexes, and appendices, including its protocols on trade in goods and services, women and youth in trade, intellectual property, and digital trade; and
- The promotion of the overall implementation of the AfCFTA Agreement, its annexes, and appendices, including its protocols on trade in goods and services, women and youth in trade, intellectual property, and digital trade.

Related resources: Coalition for Healthcare Infrastructure, Partnership in Supporting Conservation, Climate Adaptation and a Just Energy Transition, Remarks by Deputy Secretary of the Treasury. US government engagement with AfCFTA is important as the AfCFTA continues in its efforts to create a continent-wide digital market to enable data transfers. *See e.g.,* AfCFTA Decision of Feb. 10, 2020; An AfCFTA Protocol on E-Commerce ; E-commerce in Preferential Trade Agreements; Digitalising Trade Finance under the African Continental Free Trade Agreement. Maintaining digital connectivity with countries outside of Africa, as well as the ability to transfer data transnational digital networks and cross-border access to technology, will continue to be important.

C. APEC

APEC – 2023 US Host Year: On December 13, the United States hosted an informal Senior Officials Meeting (SOM), identifying its broad goals for the 2023 US APEC Host Year. Under the theme "*Creating a Resilient and Sustainable Future for All,*" the United States emphasized its "commitment to drive forward work on key issues such supply chain resilience, digital trade, connectivity, opportunities for small and medium-sized enterprises, climate change and environmental sustainability. APEC Senior Officials will convene next in Palm Springs for their first meeting in February and again in Detroit, Michigan, in May for the Ministers Responsible for Trade Meeting and other related meetings. Their final preparatory meeting will take place in Seattle in September. Finally, APEC Economic Leaders' Week will be held in San Francisco in November 2023.

APEC – 2022 Thailand Host Year: On November 19, The APEC leaders' Summit concluded. APEC Leaders endorsed a consensus declaration that included commitments to "cooperate on facilitating the flow of data, and strengthening business and consumer trust." The relevant section of the statement is excerpted below.

> Digital technology and innovation have a greater role to play in advancing inclusive and sustainable growth, improving access to services as well as opportunities to generate income and better the livelihoods of our people, including by encouraging the transition of economic actors from the informal to the formal economy. We will deepen cooperation to bridge digital divides between and within economies, including on facilitating access to digital infrastructure and supporting development of digital skills and digital literacy. We will cooperate on facilitating the flow of data, and strengthening business and consumer trust in digital transactions.
>
> We recognise the power of digital transformation in facilitating and reducing barriers to trade and unlocking exponential growth, including through nurturing the interoperability of digital

systems and tools across the region. We encourage APEC to incubate more cutting-edge and comprehensive cooperation initiatives on digital economy. We will, therefore, accelerate the implementation of the APEC Internet and Digital Economy Roadmap (AIDER) to harness new and emerging technologies and the full potential of our society as well as create an enabling, inclusive, open, fair and non-discriminatory digital ecosystem for businesses and consumers.

Vice President Harris held meetings with Vietnamese President Nguyen Phuc, Thai Prime Minister Prayut Chan-o-cha, and President Ferdinand Marcos, Jr. Katherine Tai met with Thailand's Minister of Commerce, Jurin Laksanawisit.

D. APEP

APEP: Following the Biden Administration's June 2022 announcement of the Americas Partnership for Economic Prosperity, the State and Commerce Departments were expected to issue a December 2022 Declaration identifying negotiating partners and providing additional detail on the five negotiating pillars: (1) investment, (2) supply chain resilience, (3) "updating the basic bargain," (4) decarbonization and (5) sustainable and inclusive trade. That Declaration is now expected in the first quarter of 2023.

E. ASEAN

ASEAN: At the East Asia Summit and US-ASEAN Summit, President Biden recommitted the United States to working with ASEAN to tackle issues like climate change and health security, protect a rules-based order and "build an Indo-Pacific that is free and open, stable and prosperous, resilient and secure." During the Summit, the U.S.-ASEAN partnership was elevated to a comprehensive strategic partnership and new initiatives were announced covering digital connectivity, among other issues. This included:

- *Digital Economy & Digital Trade Standards*: To strengthen ASEAN's digital trade ecosystem and enhance regional connectivity, the Commerce department will partner with the ASEAN Consultative Committee on Standards and Quality (ACCSQ) to co-develop programs on digital trust and cybersecurity standards. Commerce will convene U.S. industry leaders and the ASEAN Digital Trade Standards and Conformance Working Group to promote good regulatory practices, address cyber risks, and pursue best practices for regional harmonization and stronger interoperability.
- *U.S.-ASEAN Platform for Infrastructure and Connectivity*: the U.S.-ASEAN Platform for Infrastructure and Connectivity was launched, a demand-driven co-development mechanism through which the United States will support ASEAN initiatives that enhance connectivity across Southeast Asia and facilitate high-quality investment in regional infrastructure projects, under the auspices of the Partnership for Global Infrastructure and Investment (PGII).

F. CPTPP

CPTPP – Ratification and Accession Process: On December 22, Chile's Ministry of Foreign Affairs announced that Chile had deposited its instrument of ratification to join the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). With Chile's ratification, all eleven economies have now ratified the Agreement with the exception of Brunei. As has been widely reported, the UK, China, Taiwan, Costa Rica, and Ecuador have all formally applied to join the CPTPP. Additionally, Indonesia, the Philippines, South Korea, and Thailand have expressed an interest in joining the CPTPP. New Zealand and other CPTPP members continue to welcome input on prospective candidate members.

Relatedly, on November 14, Singapore Prime Minister Lee Hsien Loong and Chinese Premier Li Keqiang met on the sidelines of the 40th and 41st Asean summits in Phnom Penh, Cambodia. On China's application to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (**CPTPP**), Prime Minister Lee told reporters that the outcome of the country's application is "not known", and that while Singapore supports China's interest in joining, China "will have to meet the high standards which are expected of all the members". See Prime Minister Lee's remarks here.

Finally, the Asia Society has launched a process to assess what types of changes and enhancements to the CPTPP could facilitate the reentry of the United States into the Agreement. The Asia Society's Report can be found here. The 12 recommendations focus heavily on addressing concerns from a wide array of US stakeholders. They also include modernizing rules to reflect advancements in digital trade and promote digital inclusiveness.

G. G7

G7 – 2023 Japan Host Year / Data Free Flow with Trust (DFFT) Workstream: Japan will host the G7 in 2023, and it is planning to advance the Data Free Flow with Trust concept that Japan launched in 2019 during its G20 Host Year. In advance of the G7 summit 2023, Japan is planning to propose the establishment of an institutional arrangement for operationalization of DFFT, which will host joint public-private sector projects, dialogues, and other forms of partnerships to achieve outcomes such as regulatory cooperation, standardization, technology certification, etc. Though the proposal is still a 'work in progress', the current plan includes: Launching an 'international registry' to enhance regulatory transparency on data transfer restrictions; exploring the use of technology for privacy protection (Privacy Enhancing Technologies/PETs) and enhancing regulatory process (Regulatory Technology), and enhancing interoperability through regulatory and technical sandboxes. The initiative intends to provide an opportunity for private sector to advise governments on trade, privacy, security and technologies through members consisting of business, academia, and experts.

G7 – 2022 Germany Host Year: On October 5, the G7 issued a report (commissioned from the OECD Secretariat) entitled, Cross-Border Data Flows: Taking Stock of Key Policies and Initiatives – Background Report for the G7 Digital and Technology Track. This Report will likely also provide a foundation for Japan's 2023 DFFT Workstream. The Report's conclusions include the following:

> Data and their flow across borders is critical to realising the potential of digital technologies for thriving digital economies and societies, enabling the development of new and innovative business models and enhancing traditional ones that depend on moving and aggregating data around the world. In this context, maintaining a high degree of trust in cross-border data flows for businesses, citizens and societies is key to realising the benefits of digital transformation for our global economy while upholding high data protection standards. The stocktaking of key policies and initiatives seeking to promote trusted cross-border data flows provided in this report aims to offer a basis for G7 countries to continue advancing on this policy priority in a coordinated and coherent manner.
>
> This report identifies key efforts at the unilateral, inter-governmental and technological and organisational level that are underway to help advance the cross-border data flows agenda. These efforts have: supported a better understanding of the current policy landscape; started to develop an architecture for trusted cross-border data flows including through common standards, mechanisms and provisions where possible; and consistently called for governments to step up their cooperation efforts to promote cross-border data sharing in a trusted manner. In this sense, these efforts are largely complementary to one another.

H. G20

G20 – 2023 India Host Year: India's leadership of the 2023 G20 annual cycle officially commenced. Please see the official G20 website for more details on upcoming meetings of the development, financial inclusion, infrastructure, and health working groups. Additionally, the Confederation of Indian Industry (CII) has been appointed as the official secretariat for B20 India, which will include separate workstreams on Digital

Transformation, Workforce, R&D/Innovation, Financial Inclusion, Inclusive Global Value Chains, and Climate and Sustainability, among other topics. CII will host the **B20 India Inception Meeting** on January 22-24, 2023 at The Leela, Gandhinagar, Gujarat – with a public session scheduled for January 23. Registration link here: https://b20india2023.org/eventregistration/6

On December 25, Amitabh Kant, who will play a coordinating leadership role in India's G20 host year, published an op ed (reflecting his personal views) entitled, India Will Set New Data Standards in G20 Stint. The article described, "data [as] … the bedrock on which today's knowledge pyramid rises towards awareness, understanding and finally, wisdom, which is essential for nuanced and effective policymaking. For this wisdom to be democratically accessible, affordable, and available for nation-states across the world, the G20 presidency of India will be pivotal." The article also highlighted the importance of overcoming challenges to making government data to citizens across all G20 economies, and highlighted India as a relevant case study:

> As we enter India's techade, data must be accessible to all citizens. We must adopt a multisectoral approach to collecting, integrating and interpreting data. This will strengthen service delivery by governments at all levels. Even as terabytes of data flow through the government's data pipeline involving collection, cleaning, processing, analysis, modelling and visualisation, the pipeline is constrained with structural plaque. This plaque comes from databases being inaccessible and siloed, and data platforms being cluttered with complexity without any flexibility to innovate. [One model to address this challenge is to ensure that] … datasets are converted from PDFs into machine-readable formats, standardised into a common schema, given the optionality to merge and interoperate across datasets, which is a very efficient tool for users. [This can] … make government datasets accessible, interoperable and interactive, … [so] that developing nations need to tap into the power of data for development to leapfrog into an era of progress. … India's G20 Presidency is an opportune time to set a new gold standard for data. A gold standard which emphasises nations to invest in self-evaluation of their data governance architecture, calls for modernisation of national data systems to incorporate citizen voice and preferences regularly, advances principles of transparency for data governance and finally brings to the forefront the need for strategic leadership on data for sustainable development.

G20 – 2022 Indonesia Host Year: On November 15-16, Indonesia hosted the G20 Leaders' Summit. The G20 Bali Leaders' Declaration highlighted the importance of:

- [I]nclusive international cooperation on digital trade. We recognize the need to promote value addition through sustainable and inclusive investment in highly productive sectors such as downstream manufacturing, digital trade, and services, and to foster linkages between foreign investors and local enterprises particularly MSMEs. We note the initiative from the Indonesian Presidency to hold discussions on policy coherence between trade, investment and industry, and to continue addressing industry-related issues in the broader G20 process, as appropriate. …
- [P]olicies to create an enabling, inclusive, open, fair and non-discriminatory digital economy that fosters the application of new technologies, allows businesses and entrepreneurs to thrive, and protects and empowers consumers, while addressing the challenges, related to digital divides, privacy, data protection, intellectual property rights, and online safety. We acknowledge the importance to counter disinformation campaigns, cyber threats, online abuse, and ensuring security in connectivity infrastructure. We remain committed to further enable data free flow with trust and promote cross-border data flows. We will advance a more inclusive, human-centric, empowering, and sustainable digital transformation. We also reaffirm the role of data for development, economic growth and social well-being.

I. Joint Declaration on Privacy and the Protection of Personal Data

Joint Declaration on Privacy and the Protection of Personal Data: On October 1, it was announced that Taiwan, Thailand, and the Philippines endorsed the EU-led Joint Declaration on privacy and the protection of personal data, which was originally signed on by the EU, Australia, Comoros, India, Japan, Mauritius, New Zealand, the Republic of Korea, Singapore, and Sri Lanka at the at the Forum for Cooperation in the Indo-Pacific held in Paris on February 22. The Joint Declaration states in relevant part:

> To foster data free flow with trust – which, as also acknowledged by the G20 Rome Leaders' Declaration, is key to harness the opportunities of the digital economy – it is vital to ensure, as guaranteed by our respective legal frameworks, respect for individuals' right to privacy and the protection of personal data as a core value and fundamental freedom. ... To achieve this goal, we intend to foster international cooperation to promote high data protection and privacy standards based on certain core elements increasingly shared across the Indo-Pacific region, Europe and beyond, such as:
>
> - Comprehensive legal frameworks and policies covering both the private and public sectors;
> - Core principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, limited data retention, data security and accountability;
> - Enforceable rights of individuals, such as access, rectification, deletion, and safeguards with respect to automated decision-making such as transparency and the possibility to challenge the outcome;
> - Safeguards for international transfers to enable cross-border data flows by ensuring that the protection travels with the data;
> - Independent oversight by a dedicated supervisory authority and effective redress.
>
> We commit to foster and further develop international policy discussions and cooperation regarding data protection and cross-border data flows with trust, both bilaterally and multilaterally, in order to promote this shared vision and increase convergence amongst our data protection frameworks.

J. IPEF

Indo-Pacific Economic Framework: From December 10-15, representatives of the 14 negotiating parties met in Brisbane, Australia, according to a readout issued on Thursday by USTR and Commerce. USTR reportedly shared texts with partners on several areas in the trade pillar, including trade facilitation, agriculture, services domestic regulation, and transparency and good regulatory practices, according to the readout. In addition, Commerce shared text on the supply chain and fair economy pillars as well as a "concept paper" on the clean economy pillar. As regards cross-border data transfers, data localization, and other digital trade priorities, the negotiating parties reportedly discussed conceptual priorities, according to an article in InsideTrade.

K. OECD

During Q4 2022, the OECD advanced work on a range of policy priorities that implicate cross-border data transfers and cross-border access to knowledge, information, and technology. These include:

OECD – Declaration on a Trusted, Sustainable and Inclusive Digital Future: On December 15, the OECD released the Declaration on a Trusted, Sustainable and Inclusive Digital Future. Among other things, the Declaration reflects OECD members' commitment cross-border data access necessary "to working together and with all stakeholders to pursue: values and rights in the digital age, technology governance, connectivity, markets and the economy, technology supply chains, digital divides, mis- and disinformation, online safety, children in the digital environment, consumers, digital security, privacy, data governance, data free flow with trust, and digitalisation for environment sustainability."

OECD – Declaration on Government Access to Personal Data Held by Private Sector Entities: On December 14, the OECD published on a Declaration adopting seven principles on government access to personal data held by the private sector. The core principles are intended to describe common values and practices of OECD member countries and to distinguish OECD members from non-democratic countries that lack the same commitment to the rule of law. These will help support cross-border digital trust conducive to an environment supportive of data transfers. The seven principles address:

- Legal basis. Under this principle, government access to personal data held by private sector entities is provided for and regulated by the country's legal framework.
- Legitimate aims. This principle recognizes that government access is to support the pursuit of specified and legitimate aims, and is carried out in a manner that is not excessive in relation to those aims.
- Approvals. Under this principle, prior approval requirements for government access are established in the legal framework, to ensure that access is conducted in accordance with applicable standards, rules, and processes.
- Data handling. This principle recognizes that personal data acquired through government access can be processed and handled only by authorized personnel, and will be subject to internal controls.
- Transparency. This principle recognizes that a legal framework for government access is clear and easily accessible to the public, and that mechanisms exist for providing transparency about government access to personal data. Those mechanisms include public reporting by oversight bodies, as well as individual notification where applicable. The principles specifically recognize that private sector entities are allowed to issue aggregate statistical reports regarding access requests, in conformity with the legal framework.
- Oversight. This principle recognizes that mechanisms exist for effective and impartial oversight.
- Redress. This principle recognizes that the legal framework provides individuals with effective judicial and non-judicial redress to identify and remedy violations. These may include, subject to applicable conditions, terminating access, deleting improperly access or retained data, restoring the integrity of data, and the cessation of unlawful processing, as well as compensation for damages suffered by an individual depending on the circumstances.

More broadly, the OECD's Declaration states that where a government's legal framework requires that transborder data flows are "subject to safeguards," OECD members "take into account a destination country's effective implementation of the principles as a positive contribution towards facilitating transborder data flows in the application of those rules." The Declaration also recognizes a call for additional work by the OECD on identifying safeguards and protecting privacy in the context of purchasing commercially available personal data, in accessing publicly available personal data, and in receiving voluntary disclosures of personal data by law enforcement and national security authorities. BSA statement. OECD statement.

OECD – Declaration on Building Trust and Reinforcing Democracy: On November 18, the OECD released the Declaration on Building Trust and Reinforcing Democracy. Among other things, the Declaration underscore the importance of cross-border data access and transfers in order to "[m]aintain open government as a core element of our democratic systems, while continuing our ongoing and open dialogue on public governance with non-OECD Members, with a view to maintaining peace, stability and free flows of goods, services as well as data and information flows"; and to "[c]ollect data, regularly take stock of progress and undertake comparative analyses of the experiences and good practices of countries (at national, regional and local level) in strengthening participation representation and openness."

OECD – Declaration on Transformative Solutions for Sustainable Agriculture and Food Systems: On November 4, the OECD released the Declaration on Transformative Solutions for Sustainable Agriculture and Food Systems. The Declaration underlines the key role of developing transformative and innovative policies towards more sustainable and resilient agriculture and food systems. To this end, it calls on Adherents to *inter alia* enhance research collaboration and knowledge sharing, and strengthen international cooperation, while also measuring sustainable agricultural productivity growth, developing metrics to

measure climate change mitigation and adaptation, and measuring trade's contribution to sustainable transformation of agriculture and food systems. Many of the Declaration's objectives are premised on the ability to access and transfer technology, knowledge, and information across borders, as outlined in the GDA's overview of Cross-Border Data Transfers & Sustainable Agriculture.

L. Trade & Technology Council

US-EU Trade & Technology Council: The Fourth Ministerial Meeting of the US-EU Trade & Technology Council (TTC) is planned for Spring or early Summer in Sweden. Additionally, the Trade & Technology Dialogue is hosting a TTC stakeholder event on January 31 at 9:00 ET / 15:00 CET. Additional details here; Registration link here.

On December 5, the US and the EU held the Third Ministerial Meeting in College Park, Maryland. The meetings were led by European Commission Executive Vice Presidents Vestager and Dombrovskis, as well as Secretary of State Blinken, Secretary of Commerce Raimondo, US Trade Representative Tai. Key outcomes included:

- A Joint AI Roadmap (link here)
- A Report on the Impact on AI on US and EU Workforces (link here)
- Efforts to advance democratic values online
- Pilot projects/Task Forces on: (a) privacy enhancing technologies; (b) AI & workforce issues; (c) quantum computing; (d) transatlantic trade in dual-use export-controlled items; (e) shared priorities in standards development; and (f) Chinese non-market practices that impact US and EU exports of medical devices and other products

See here for the TTC Joint Statement and the White House Fact Sheet

M. World Trade Organization

WTO – JSI E-Commerce Negotiations: The next WTO Trade Ministerial will be held in the United Arab Emirates the week of February 26, 2024. The following Ministerial will be hosted by Cameroon.

During the fourth quarter of 2022, WTO members engaged in the WTO Joint Statement Initiative (JSI) Negotiations on E-Commerce (JSI e-commerce negotiations) accelerated discussions of several priority areas – privacy, data transfers, and data flows. Participants have set a goal to issue a revised consolidated text by the end of 2022.

GDA made submissions to JSI negotiators on its priorities relating to the JSI e-commerce negotiations and the Moratorium on Customs Duties on Electronic Transmissions (E-commerce Moratorium). GDA provided comments to Australia, Barbados, Colombia, Costa Rica, EU, Japan, Mexico, New Zealand, Singapore, Switzerland, and the United States.

The GDA has recommended that WTO negotiators agree to commitments relating to *inter alia*:

- Cross-Border Transfer of Information by Electronic Means: Across all sectors, Parties shall not prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of a business.
- Location of Computing Facilities: Across all sectors, Parties shall not impose requirements to use or locate computing facilities in their own territory as a condition for conducting business.

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

To address the cross-border impacts of any data regulations that involve incidental restrictions on data transfers, we urge WTO digital trade negotiators to clarify that such data regulations:

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

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

GDA WORK PRODUCT AND OTHER PUBLICATIONS

A. Argentina

Global Data Alliance, *Comments re Argentina's Proposal for a Draft Law on the Protection of Personal Data*
Digital Policy Alert, Implemented Resolution No. 255/2022 expanding definition of sensitive data regarding genetic data (Original source here)
IAPP, Argentina finalizes proposed data protection reform (Original source here)
IAPP, Draft bill on personal data protection

B. Australia

Global Data Alliance, *Australia: GDA Submission re WTO JSI E-Commerce Negotiations*
Global Data Alliance, *Australia: GDA Submission re IPEF Cross-Border Data Commitments to Department of Foreign Affairs and Trade*
BestLawyers, The Future of Trade is Digital
InnovationAus, Australia-UK free trade deal at odds with data localisation push
InnovationAus, Privacy Act Review complete after three years

C. Barbados

Global Data Alliance, *Barbados: GDA Submission to Permanent Mission of Barbados to the World Trade Organization re WTO JSI E-commerce Negotiations*

D. Belarus

Data Guidance, National Data Protection Center announces amendments to data transfer rules (Original sources here and here)

E. Canada

Global Data Alliance, *Comments on Model Canadian Digital Trade Agreement*
BLG, Cross-border transfers of personal information outside Québec: new requirements for businesses
JDSupra, Canada's Long Awaited Privacy Bill Introduced: How Does it Stack Up?
Office of the Privacy Commissioner, G7 data protection and privacy authorities discuss data protection and the flow of data across borders
Gowling, Canada proposed privacy law second reading
Lexology, Guide to doing business in Canada: privacy law

F. China

Bloomberg Law, China Data Privacy Laws, WeChat Muddy Cross-Border Inquiries
Data Guidance, CAC announces implementation of personal information protection certification
Deacons, Hong Kong PDPC's new guidance on cross-border data transfers
Dentons, Cross-border data transfer in China
DLA Piper, China - Clarifications of data classification and grading requirements
Ejinsight, Cross-border data flow to empower Hong Kong digital drivetrain EJINSIGHT
IAPP, What to know about China's new cross-border data transfer security assessment guidelines
IAPP, China seeks input on revised cross-border data processing guidelines (original source here)
JDSupra, Spotlight on Greater China: recent developments governing health related data and HGR
JDSupra, Data transfers / data sharing in a global environment (Hong Kong)
JDSupra, Outbound data transfers of personal information in China
JDSupra, As China Cross-Border Data Transfer Security Assessment Requirement Comes Into Effect, New Guidelines Posted for Security Assessment Application
JDSupra, Data transfers in a global environment: Data cross-border transfers from China
Lexology, As China Cross-Border Data Transfer Security Assessment Requirement Comes Into Effect, New Guidelines Posted for Security Assessment Application
Lexology, What Hong Kong business needs to know about data transfer - security assessment requirements for cross border data transfer in China
Lexology, PRC Published the Guide to Applications for Security Assessment of Outbound Data Transfers

Lexology, China to Toughen Penalties for Cybersecurity Breaches
Lexology, Data Transfers: Protecting personal data by contractual means
Lexology, Data Transfers: Hong Kong personal data importers and transfer impact assessments
Mayer Brown, Revised Specification for Certification of Cross-border Transfers of Personal Information Issued in China
Lexology, China to Toughen Penalties for Cybersecurity Breaches
Lexology, Data Transfers: Protecting personal data by contractual means
Lexology, A Brief Review of China's New Data Protection Law: A Comparative Analysis
Reed Smith, China issues new Implementation Rules for Personal Information Certification
South China Morning Post, US think tank warns Hong Kong over the economic costs of imposing strict data rules to align with mainland
World Economic Forum, How China's data rules will impact its trade competitiveness

G. Colombia

Global Data Alliance, *GDA Submission re WTO JSI E-Commerce Negotiations*

H. Costa Rica

Global Data Alliance, *GDA Submission re WTO JSI E-Commerce Negotiations*

I. Denmark

Computing.co.uk, Denmark latest to conclude Google Analytics is unlawful
IAPP, Danish DPA renders decision against Google Analytics transfers
MUO, Why Google Is Banned From Danish Classrooms

J. EU

Global Data Alliance, *GDA Submission re WTO JSI E-Commerce Negotiations*
Atlantic Council, Privacy and Cross-Border Digital Currency
Biometric Update, EU makes next move on EU-US data flow by finding agreement adequate
CPO Magazine, Risk-Based Approach to International Data Transfers Necessary to the Future of Cross-Border Data Flows Under GDPR
Dentons, Personal data transfers to the US - still an issue?
Digital Journal, Several countries in the EU follow the ban on Google Analytics
EDPS Website, EU-wide cybersecurity requirements to protect privacy and personal data
EPRS Website, Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086
Euractiv, EU Council Set to Revise Cloud-Related Provisions in New EU Data Law
Euractiv, How MEPs Want to Reshape the Data Act
European Commission, EU-U.S. Data Privacy Framework, draft adequacy decision
Hogan, Impact of European Commission support for EU-U.S. Data Privacy Framework and next steps - Hogan Lovells Engage
IAPP, MEPs take issue with UK GDPR reform plans
IAPP, A view from Brussels: The European Commission EU-US draft adequacy decision (iapp.org)
IAPP, From Privacy Shield to the Trans-Atlantic Data Privacy Framework
IAPP, MEPs take issue with UK GDPR reform plans
IAPP, EU-US draft adequacy decision arrives, EU process begins in earnest
IAPP, Microsoft Rolls Out Data Boundary for EU Customers
JDSupra, EU To Review New EU-US Data Transfers Framework
Lexology, The GDPR International Data Transfer Regime: the case for Proportionality and a Risk-Based Approach
Lexology, Data Act and the interplay with existing regulations
Lexology, EDPB guidance on supplementary measures for data transfers

Lexology, Deadline for Third Country Personal Data Transfers: EU Standard Contractual Clauses
Littler Mendelson, International Data Transfer of HR Data From the EU to Non-EU Entities
Mintz, EU Personal Data Transfers Deadline: New SCCs must be put in place by December 27, 2022
Mondaq, UK GDPR Data Transfer Compliance - Data Protection - European Union
National Law Review, Europe Data Privacy Laws and U.S. Civil Discovery
Noyb, 6 Months of "agreement in principle", EU-US agreement in fact still missing
Orrick, 10 Things to Know about the European Commission's Questions and Answers on the GDPR Standard Contractual Clauses
Pharmtech, Updated Guidance to the European Data Governance Act
Pinsent Masons, UK and non-EU businesses to face more uncertainty in GDPR data breach reporting
Pinsent Masons, International transfers and Schrems II: obligations under the EU and UK GDPR
RTE, European Commission defends its Irish data monitoring
Reuters, Microsoft to roll out 'data boundary' for EU customers from Jan. 1
TechCrunch, TikTok privacy update in Europe confirms China staff access to data as GDPR probe continues
TechCrunch, EU confirms draft decision on replacement US data transfer pact
The Lancet Oncology, The impact of GDPR on data sharing for European cancer research

K. Germany

Hamburg DPA, Data Protection in the United States
IAPP, Hamburg DPA advises on EU-US Data Privacy Framework
Morgan Lewis, German Court Rules EU Subsidiaries of US Cloud Providers Can Provide IT Services in European Union

L. Gulf Cooperation Council

Global Data Alliance, *Submission re Gulf Cooperation Council-United Kingdom FTA Negotiations*

M. India

Global Data Alliance, *Comments on Digital Personal Data Protection Bill*
Analytics India Magazine, The End Of Data Globalisation
Atlantic Council, How India's new digital rules can demonstrate a commitment to good regulatory practices
Atlantic Council, India's new data bill is a mixed bag for privacy
Atlantic Council, India's data localization pivot can revamp global digital diplomacy
CPO Magazine, Fourth Draft of India Data Protection Bill Proposes Government Exception From All Provisions
CXO Today, Data Localization Takes Back Seat
Digital Policy Alert, RBI released Regulatory Framework for Digital Lending including provisions on data localisation (Original RBI source)
DW, India: Data privacy rules in play under new draft bill
East Asia Forum, Resurrecting Data Regulation in India
East Asia Forum, India's data protection dilemma
Economic Times of India, 'New data protection bill likely to be tabled in winter session'
ET Telecom, Data Protection Bill: New data Bill draft to allow storage in trusted nations
Fortune India, Business News, Strategy, Finance and Corporate Insight
Hindu Business Line, Right to Privacy will prevail over Right to Information in case of conflict: Rajeev Chandrasekhar
Hindustan Times, Digital Personal Data Protection Bill: IFF seeks transparent consultations
Hindustan Times, Govt eyes 'personal, sensitive data' rules | Latest News India - Hindustan Times
Hindustan Times, India's data protection bill will be 'simple and modern'
IAPP, India considers limited startup exemption in draft data protection bill
IndianExpress, Data protection, telecom bills to be passed by Aug 2023: Union Minister Ashwini Vaishnaw
Lakshmikumaran & Sridiharan, Indo-Pacific Economic Framework and future of cross-border data flows
Lexology, India's Data Protection Muddle

LiveLaw, The Digital Data Protection Bill, 2022 And The Concerns Associated
Medianama, Cross-border data flows, geopolitics, and India's stance
Medianama, Why India should consider deanonymization risks in NPD and privacy law
Medianama, Data protection bill might allow data transfers only to whitelisted countries
MEITY Website, Digital Personal Data Protection Bill – Request for Comments
Mint, Clarity sought on cross-border data flow
Mint, Revised data protection law ready, will ease compliance
Mondaq, Digital Trade Clauses In FTAs And India's Data Industrialization Goals: The Bilateral Way Forward
Mondaq, A Dive Into The Digital Personal Data Protection Bill, 2022
Money Control, There will be multiple intermediaries defined in upcoming digital laws: Rajeev Chandrasekhar
Moneycontrol, Will India's proposed data protection regulator have enough powers as global peers?
Reserve Bank of India - Press Releases (rbi.org.in)
ORF, Data flow and privacy - India's role as the G20 President
ORF, Digital Personal Data Protection Bill 2022: Reservations and recommendations
Quartz, Big Tech will love India's draft data protection bill
The Dialogue, Principle-Based Frameworks Towards Cross-Border Data Transfers
The Economic Times, In data, we trust: The simpler and smaller draft data protection Bill is a mixed bag
The Economic Times, Draft DPDP bill draws from experiences of several countries
The Economic Times, Data localisation to be scrapped in new Bill, Amazon layoffs to hit India staff
The Economic Times, Data Protection Bill: View: India's Data Protection Bill has a privacy problem
The Economic Times, New Data Bill Allows Storage in Trusted Countries
The Hindu, Are data localisation requirements necessary and proportionate?
The Indian Express, Rajeev Chandrasekhar: EU's GDPR more absolutist, not possible for us … our law will be clear on data misuse
The Indian Express, India Data Management Office | Non-personal data regulator after consultations: MoS IT
The Times of India, Personal Data Privacy – Does India need regulations like Europe's GDPR and USA's CCPA
Times of India, 'India's new data bill safeguards citizens without stifling innovation

N. Indonesia

ANTARA News, Data flow management crucial for digital economy: ministry
Asia Business Law Journal, China >Cybersecurity regulations> Comparison with India, Indonesia, Taiwan
CPO Magazine, Indonesia Data Protection Law Includes Potential Prison Time, Asset Seizure, Right to Compensation for Data Breaches
Data Guidance, Personal Data Protection Law – What You Need to Know
DLA Piper, Personal Data Protection Law PDPL Now in Force
JDSupra, What you need to know about the Personal Data Protection Law
Lexology, The impact of the new personal data protection law in Indonesia
Lexology, Indonesia's New Personal Data Protection Law and the Impact on M&A Transactions
Lexology, 2022 Indonesian Data Protection Law overview
Lexology, Indonesia's New Personal Data Protection Law
Lexology, Indonesia Passes Historic Personal Data Protection Bill
Open Gov, Indonesia Approves Personal Data Regulations

O. Israel

Global Data Alliance, *GDA submission re Israel-United Kingdom FTA Negotiations*
Data Guidance, Israel: PPA issues opinion clarifying PPL definitions
IAPP, Israel opens consultation on EEA data transfer rules

P. Japan

Global Data Alliance, *GDA Submission re WTO JSI E-Commerce Negotiations*

IAPP, Japan, UK reach digital partnership

Q. Mexico

Global Data Alliance, *GDA Submission re WTO JSI E-Commerce Negotiations*
Global Data Alliance, *GDA Submission re UK-Mexico FTA Negotiations*

R. Moldova

Data Guidance, SCCs for International Data Transfers

S. Namibia

FYI Africa, Stakeholders meet on data protection bill – Namibia

T. Netherlands

IAPP, Dutch DPA says cloud storage policy contains privacy risks (Dutch DPA statement here)

U. New Zealand

Global Data Alliance, *New Zealand: GDA Submission re WTO JSI E-Commerce Negotiations*

V. Nigeria

Global Data Alliance, *Nigeria: GDA Comments on Personal Data Protection Bill*
IAPP, Comment Period Opens on Nigeria's National Data Strategy
NITDA, National Information Technology Development Agency (NITDA) Calls for Stakeholder Engagement on National Data Strategy

W. Russia

Brookings, Russia is weaponizing its data laws against foreign organizations
Digital Policy Alert, Russian court imposes fine on Snap, Match Group, Hotels.com, Spotify and WhatsApp for non-compliance with data localisation requirement (Original court decision)
Digital Policy Alert, Russia & Ukraine – Cybersecurity risk and data transfers

X. Saudi Arabia

Global Data Alliance, *Saudi Arabia: GDA Comments on Draft Amendments to Personal Data Protection Law*
IAPP, Comments sought on Saudi Arabia data protection law
JDSupra, Saudi Arabia Issues Amended Data Protection Law for Consultation

Y. Singapore

Global Data Alliance, *Singapore: GDA Submission re WTO JSI E-Commerce Negotiations*
Singapore PDPC, Amendments to Enforcement under the Personal Data Protection Act (PDPA) in updated Advisory Guidelines and Guide

Z. South Africa

JDSupra, Cross-border data transfers under the protection of personal information Act 4 of 2013

AA. Spain

Hogan, Spanish DPA's First Direct Decision on Google Analytics

BB. Switzerland

Global Data Alliance, *Switzerland: GDA Submission re WTO JSI E-Commerce Negotiations*
Global Data Alliance, *Switzerland: GDA submission re Switzerland-United Kingdom FTA Negotiations*
CPO Magazine, International Transfers of Personal Data and Privacy Contracting: How Switzerland Wins Over UK Both in Terms of Business-Friendliness and EU Convergence
Federal Chancellery of Switzerland, Swiss Cloud Strategy Bund
Federal Council of Switzerland, New Data Protection Rights from Sept. 1, 2023
Federal Council of Switzerland, Digital Transformation – Fields of Activity for Economic Policy
Morgan Lewis, Switzerland Publishes Adequacy List of Countries Receiving Personal Data Transfers – Publications

CC. Taiwan

Asia Business Law Journal, China >Cybersecurity regulations> Comparison with India, Indonesia, Taiwan

DD. Tanzania

Victory Attorneys, Brief Highlight and Analysis of The Tanzania Data Protection Bill, 2022
IAPP, Tanzania Parliament passes Personal Data Protection Bill
Data Guidance, Tanzania: Parliament passes Personal Information Protection Bill

EE. Thailand

Global Data Alliance, *Thailand: GDA Comments on Draft Notification on International Data Transfers*

FF. Turkey

Dentons, Data transfers under the Turkish data protection law
Gun & Partners, Draft Guideline On Processing Genetic Data
JDSupra, Data transfers under the Turkish data protection law

GG. United Arab Emirates

IAPP, UK, DIFC commit to updated data partnership

HH. United Kingdom

Global Data Alliance, *UK: GDA submission re United Kingdom Trade Negotiations*
AEM, Data Regulatory Trends in the UK – Change is Afoot Post-Brexit
ComputerWeekly, Tories to Replace GDPR
Cooley, US-UK Data Access Agreement: Top Five Things to Know
Dentons, UK perspective – data transfers / data sharing in a global environment (not only from a GDPR perspective)
Digital Journal, Wither GDPR? Data privacy and the big change to come
DCMS, Materials on UK-Japan Digital Partnership
EliteBusiness, Stripping GDPR down to its bare bones
Euractiv, New UK government to push for further divergence from GDPR
ICO, New Transfer Risk Assessment Tool

ICO, IDTA and TRA (IDTA Toolkit) impact assessment
JDSupra, Deadline for New UK Contract Requirements for Personal Data Transfers Is Here
JDSupra, U.K. Unveils Replacement GDPR, then Retracts It
Lexology, International Data Transfers Time to Plan, Time to Act
Lexology, Genetic information - global privacy considerations - an Australian and UK perspective
Lexology, UK Government grants South Korea a data adequacy status
Lexology, Data protection | UK Regulatory Outlook
Marketing Week, UK government to replace GDPR with 'truly bespoke' data privacy regime
MarketingWeek, Marketing trade bodies raise concern over 'daunting' GDPR replacement plan
Mayer Brown, Deadline to update template contracts to address international personal data transfers outside the UK
Mint, Data flow, whisky among key UK demands in free trade pact
Mondaq, The New Proposal To Reform Data Protection And Privacy Regulations In The United Kingdom
Mondaq, The New Proposal To Reform Data Protection And Privacy Regulations In The United Kingdom
Moore Barlow LLP, Where is your data – new requirements for international data transfers
Morgan Lewis, Managing the Challenges of Cross-Border Outsourcings
National Law Review, New British Data Protection System to Replace UK GDPR
Quastels, UK GDPR Data Transfer Compliance
Tech Monitor, Data Protection Bill: Consultation to delay UK GDPR replacement
TechCrunch, UK pauses data reform bill to rethink how to replace GDPR
The Drum, Britain to scrap GDPR rules and go it alone on data privacy
The New European, The pointless war on GDPR

II. United States

Global Data Alliance, *US: Multi-industry Letter on the Indo-Pacific Economic Framework*
Global Data Alliance, *US: GDA Submission to USTR for National Trade Estimate Report*
Global Data Alliance, *US: GDA Submission re WTO JSI E-Commerce Negotiations*
Akingump, President Biden Signs Long-Awaited Data Transfer Executive Order
ArsTechnica, TikTok can keep operating in US under deal being worked out with Biden
Benesch, New UK Cross-Border Data Transfer Mechanisms Now in Effect
Brown Rudnick, Executive Order One Step Closer to EU-US Data Transfers
CPO Magazine, Privacy Shield Redux: Looking Ahead to a New EU-U.S. Data Transfer Framework
DataGuidance, International: Understanding data transfers under the new EU-US Data Privacy Framework
Fenwick, Reviving the Privacy Shield? New US Executive
IAPP, ODNI issues implementation directive on EU-US Data Privacy Framework redress
IAPP, UK-US data access agreement takes effect
IAPP, 'Data transfer theater:' The US and Israel take the stage
IAPP, The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC
IAPP, US executive order on Trans-Atlantic Data Privacy Framework imminent
IAPP, Implications of EU-US Data Privacy Framework as adequacy decision looms
IAPP, Report outlines EU-US Data Privacy Framework considerations for US Congress, and other updates
JDSupra, New Privacy Protections for US-EU Transfers Coming
JDSupra, New Executive Order Paves Way for Streamlined International Data Transfers
JDSupra, US data transfers
Lexology, The New EU-US Personal Data Transfer Framework
Lexology, The new US Privacy Shield 2.0 with Adequacy: One step closer to US Federal Privacy Laws?
Lexology, Does the UK-U.S. agreement under the U.S. CLOUD Act affect UK's adequacy under the GDPR?
Lexology, US adopts Executive Order to implement EU-US Data Privacy Framework
Medianama, Data Framework for Cross-Border Data Flows Between the EU and US
MeriTalk, Senators Urged to Wall off Data from Hostile Nations
NY Times, TikTok Seen Moving Toward U.S. Security Deal, but Hurdles Remain
NY Times, The Era of Borderless Data Is Ending
ORF, The international politics of data: When control trumps protection

Proskauer, EU-U.S. and UK-U.S. Data Transfer Deals Advance with White House Executive Order
Politico, Digital Bridge: EU-US data pact
Politico, US expected to publish Privacy Shield executive order next week – POLITICO
Security Boulevard, A New EO Updates Privacy Shield for EU, US Data Sharing
The Drum, Biden's Executive Order On Data Transfers To Offer Temporary Relief For Advertisers

JJ. Vietnam

Global Data Alliance, *Vietnam: GDA Comments on Draft Law on Telecommunications*
Nikkei, Data Localization Rules will Set Back Vietnam's Digital Economy
Vietnam Briefing, Vietnam's New Data Localization Regulation Concerns US Investors

KK. Global

ADB, Capturing the Digital Economy: A Proposed Measurement Framework and Its Applications—A Special Supplement to Key Indicators for Asia and the Pacific 2021 | Asian Development Bank (adb.org)
AFI, Digital Financial Services Regulation: Current State of Practice Report | Alliance for Financial Inclusion
Asia Business Law Journal, China >Cybersecurity regulations> Comparison with India, Indonesia, Taiwan
Brookings, The geopolitics of AI and the rise of digital sovereignty
Digital Policy Alert, Regulatory activity in cross-border data transfer and data localisation is ticking up
GovInsider, Why data localisation may not be a panacea for data privacy woes in ASEAN
IAPP, RIPD publishes guidelines for international data transfers
Medianama, G20 not right for discussing cross-border data flows, civil society orgs say
Nextgov, Over 40 International Business Groups Support Transatlantic Data Privacy Terms
Raconteur, For a stronger supply chain, just add a digital data thread
Red Iberoamericana de Proteccion de Datos, Publication of the Guide to the Implementation of Model Contractual Clauses for the International Transfer of Personal Data
TechHive Advisory, 2022 Africa Data Protection Roundup
The Diplomat, Southeast Asia's Data Localization Push Is a Double-Edged Sword