GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

UPDATES

Q4 2024

RECENT POLICY DEVELOPMENTS

EMEA

EU – Trade Agreement with MERCOSUR: On December 6, the EU and the economies comprising the MERSOCUR (Brazil, Argentina, Uruguay, Paraguay) announced the conclusion of an updated negotiating outcome for the EU-MERCOSUR trade agreement. (Although the trade agreement was initially finalized in 2019, it did not advance through the political review process). The EU-MERCOSUR Trade Agreement does not contain a digital trade or e-commerce chapter that focuses on cross-border data transfers or other international digital governance issues. The Agreement does include new provisions on the cross-border provision of services, including new provisions on telecommunications, aviation, professional, and other services that depend upon cross-border data. Full text here; Chapter-by-chapter here; EU Fact Sheet here; Services Chapter here; EU Services Schedule here; Mercosur Services Schedule here.

EU – EDPB Guidance on Data Transfers: On December 3, the European Data Protection Board (EDPB) published guidelines on Article 48 of the EU General Data Protection Regulation (GDPR) regarding data transfer requests **from third-country public authorities directly to private entities (controllers or processors) in the EU**.

The guidelines aim to clarify the rationale and objectives of Article 48 of the GDPR on "Transfers or disclosures not authorised by EU law", including its interaction with other GDPR provisions on international data transfers. The EDPB provides recommendations for controllers and processors in the EU by analyzing the applicability of various legal basis for processing data and grounds for transferring it under the GDPR. The guidelines reiterate strict requirements for transferring data in response to requests from non-EU public authorities, including law enforcement agencies (LEAs).

The EDPB explains that Article 48 of the GDPR applies in situations where a controller or processor in the EU receives a decision or judgment directly from an administrative authority or a court in a third country requiring the transfer or disclosure of personal data. The EDPB considers that such requests constitute **any official requests that come from all kinds of public authorities of the third country**, including those supervising the private sector such as tax authorities, as well as **LEA and national security authorities**, etc.

The EDPB reaffirms that where data processed in the EU are transferred or disclosed in response to a request from a third country authority, the **"two-step test"** is mandatory:

- First, there must be a **legal basis for the data processing** in Article 6 of the GDPR;
- Secondly, there must be a **ground for transfer** in Chapter V of the GDPR.

The EDPB emphasizes that the main objective of Article 48 of the GDPR is to clarify that judgments or decisions from third country authorities cannot automatically and directly be recognised or enforced in

an EU Member State, thus underlining the legal sovereignty vis-a-vis third country law. Therefore, the EDPB stresses that a **request from a foreign authority does not in itself constitute a legal basis for the processing or a ground for the transfer**.

Legal basis. The EDPB states that where the processing of personal data is carried out in order to fulfil a legal obligation based on an international agreement, Article 6(1)(c) provides an explicit legal basis (**legal obligation**). As a result, the EDPB is of the opinion that, where there is an applicable and enforceable international agreement in place, Article 6(1)(c) (legal obligation) in conjunction with Article 6(3) would be the appropriate legal basis for the transfer provided that the conditions of these provisions are fulfilled.

- The EDPB further specifies, that in situations where disclosure based on an international agreement is not mandatory, but such cooperation is still allowed under EU or Member State law, Article 6(1)(e) (**public interest**) could be used as a legal basis for the processing of personal data since it can be considered necessary for the performance of the task carried out in the public interest.

- In the **absence of an international agreement**, or if the agreement does not provide for a legal basis under Article 6(1)(c) (legal obligation) or 6(1)(e) (public interest), other legal basis under Article 6 could be considered. The EDPB, however, concludes that the application of other legal basis may not be always possible and in any case must be carefully examined on a case-by-case basis. While the guidance does not foreclose relying on **legitimate interest** as a legal basis for data processing, it identifies criteria to be considered in applying the balancing test (including the seriousness of the relevant alleged offenses and the reasonable expectations of the data subject) and emphasizes that the EDPB has previously taken the view that individuals' rights and freedoms override the controller's interest in complying with a LEA request to avoid sanctions for non-compliance.

As for grounds for transfer, the EDPB explains that Chapter V of the GDPR lists the grounds for transfers, starting with the European Commission's adequacy decisions under Article 45. If there is no adequacy decision, appropriate safeguards may be provided for by one of the transfer tools foreseen in Article 46. The derogations in Article 49 could apply in a limited number of specific situations.

- **However, the EDPB states that Article 48 is not a ground for transfer**, as the provision itself contains no data protection safeguards but clarifies that decisions or judgments from third country authorities cannot be recognized or enforced in the EU unless an international agreement provides for this. Therefore, the EDPB states that **before responding to a request from a third country authority falling under Article 48, the controller or processor in the EU must identify an applicable ground for transfer elsewhere in Chapter V**.

- Article 46(2)(a) could provide a ground for transfer, given the appropriate safeguards are provided for by "a legally binding and enforceable instrument between public authorities or bodies" i.e. an **international agreement** within the meaning of Article 48. The agreement must provide for **direct cooperation** between private entities and public authorities. It must also entail **appropriate safeguards** which must be capable of ensuring that data subjects whose personal data are transferred are afforded a level of protection essentially equivalent to that, which is guaranteed within the EU. In this case, the EDPB concludes that the international agreement may serve as a ground for transfer.

- If there is **no international agreement** or the agreement does not provide for appropriate safeguards under Article 46(2)(a), other grounds for transfer could apply, including the derogations in Article 49.

The EDPB underlines that in addition to ensuring compliance with the GDPR, a controller or processor may need to comply with additional requirements following from other legal instruments, e.g. national procedural rules or international agreements providing for cooperation with the third country authority.

EU – Data Privacy Framework: On October 9, the European Commission published its first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework (DPF). The main finding is that that the US authorities have "successfully put in place all the necessary elements required to support the framework's data protection standards", though it recognizes that "experience with the practical application of the safeguards applying both to the processing of data by certified companies and to access to data by public authorities is necessarily limited after just one year of operation". The report specifically highlights – and welcomes- the implementation of critical safeguards to ensure that national security authorities' access to personal data is limited to what is strictly necessary and proportionate.

EU – New EU Commission 2024-2029: Strong & Centralized Digital Portfolio, Experienced Trade Commissioner: Under EU Commission (EC) President Ursula Von der Leyen's (Conservative EPP, Germany) allocation of portfolios, the EU Digital portfolio went to former MEP who already worked on digital issues, Henna Virkunnen (Conservative EPP, Finland). She received the title of Executive Vice-President for Tech Sovereignty, Security and Democracy, and is also entrusted with the "Digital and Frontiers Technologies portfolio. This means she will be the lead (and sole) member of the EC to work on digital files, and will have authority over the DG CONNECT (the Commission's administration in charge of Digital issues).

The Trade Portfolio is entrusted to Maroš Šefčovič (Socialist S&D, Slovakia), a 3-time Commissioner (Education and Culture, Energy, and Inter-institutional Relations). Mr. Šefčovič's deep experience will likely give him some margin of manoeuvre as he is reporting to Executive Vice-President Stéphane Séjourné (Liberal Renew, France), France's former, short-timed, Foreign Affairs Minister, entrusted with the "Prosperity and Industrial Strategy" portfolio. Issues could arise with regards the negotiations of Free Trade Agreements (FTAs), which the EU is negotiating but with respect to which France faces oppositional political pressure at home.

Finally, the "Democracy, Justice and Rule of Law" portfolio is allocated to Michael McGarth (Liberal Renew, Ireland) whose mission letters mentions the mere "enforcement of the General Data Protection Regulation (GDPR) but not its review.

Saudi Arabia – Regulations on Transfers of Personal Data: The Saudi Data and AI Authority has published Saudi Arabia's regulations on transfers of personal data. The regulations provide for:

- Art. 3: Publication of a list of "adequate" jurisdictions for purposes of cross-border data transfers;
- Art. 4: Exemptions for controllers;
- Art. 6: Data transfer risk assessments.

Saudi Arabia – Standard Contractual Clauses: The Global Data Alliance submitted comments to the Saudi Data and AI Authority (SDAIA) on Saudi Arabia's draft Standard Contractual Clauses ("SCCs"). The comments contained the following recommendations: (1) Work on developing a framework to recognize SCCs in other countries, including those in the European Union; (2) Re-evaluate the legal propriety, necessity, and feasibility of the draft SCC "data quality" obligations (i.e., a formal obligation on data importers to proactively assess data quality, to inform data exporters of any inaccuracy, and to destroy inaccurate or low quality data); (3) Re-evaluate – in light of prevailing international practice – the proposed obligation for Data Importers to inform Data Exporters about data subject requests; and (4) Undertake at least one more round of review and revisions to the draft SCCs, and once the SCCs become effective, offer a 18- to 24-month transition period for the new SCCs.

Türkiye – Customs Duties on Electronic Transmissions: On December 11, 2024, the GDA joined an industry letter raising concerns with the Government of Türkiye regarding its opposition to provisions in the WTO E-Commerce Agreement relating to customs duties on electronic transmissions. A copy of that submission can be found here.

UAE – Abu Dhabi Healthcare Information and Cyber Security Standard: On October 16, 2024, the Global Data Alliance submitted comments to share with authorities in the United Arab Emirates and the United States regarding cross-border data restrictions in the Abu Dhabi Health Cyber Standard. These restrictions take the following forms: (1) Restrictions on the ability to access health data stored in Abu Dhabi from outside of Abu Dhabi; (2) Restrictions on the ability to transfer health data from Abu Dhabi to other jurisdictions; and (3) Restrictions on the ability to store health data anywhere other than Abu Dhabi. More specifically,

- Communications and Operations Management control number 9 (e) mandates that covered entities shall: "[e]nsure PII and PHI or its backup is not stored, processed or transferred outside UAE, except in cases where a valid exemption is issued by [the Department of Health]."

- Control number 9(f) mandates that covered entities shall "[e]nsure that employees of the entity and third-party users involved in service delivery fulfil their responsibilities and provide assistance from within the UAE, unless a valid exemption has been issued by the DoH."

- Control number 11 mandates that: "Transfer of Health Information outside the UAE is normally not allowed unless exception to do so is granted by DoH."

- Data Privacy Policy Article 1.4(d) states that a covered entity:

    - "Should ensure that only people who are physically present in the UAE or who have a valid license to practice their profession there have access to systems and applications that contain protected health information."

    - [S]hall not transfer health information and its copies in any form, whether encrypted, anonymized, deidentified, pseudonymized, etc., are not stored, processed, or transferred outside the UAE. Any exemptions must be approved by entity management and then submitted to the Department of Health (DoH) for further approval."

UK – Digital Economy Agreement with Ukraine: On September 1, 2024, the UK-Ukraine Digital Economy Agreement entered into force. The Agreement includes the following commitments:

- Cross-Border Transfer of Information by Electronic Means: Promotes the benefits of cross-border access to knowledge, information, and data – while also giving each Party wide discretion to develop its own regulatory requirements regarding such transfers. More specifically, this provision prohibits arbitrary, discriminatory, or disguised restrictions on cross-border data transfers, as well as those that are more restrictive than required to meet a legitimate public policy objective.

- Localization of Computing Facilities: Contains a commitment to refrain from measures that mandate construction or use of local computing facilities as a condition of conducting business in the territory. It also affords discretion to Parties to derogate from this commitment for legitimate public policy purposes.

- Financial Information: Contains commitments to refrain from financial data localization mandates, unless a service supplier is "not able to ensure access to information required for the purposes of financial regulation and supervision."

- Personal Data Protection: Mandates the adoption of legal frameworks for personal data protection, including disciplines regarding (a) collection and usage limitation; (b) data quality;

(c) purpose specification; (d) security safeguards; (e) transparency; (f) individual participation; and (g) accountability

- Cyber Security: Contains new provisions on cybersecurity, including from a workforce development and training perspective. It also calls on the Parties to use risk-based approaches to manage cyber security risks and to detect, respond to and recover from cyber security events

United Kingdom – CPTPP Accession: The United Kingdom has officially acceded to the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP). Coverage in: The Diplomat; Deutsche Welle, Modern Diplomacy.

APAC

Australia – Privacy Amendment Bill passes Parliament. On November 29, the Australian Parliament passed the Privacy Amendment Bill 2024 (**Bill**). This is the first tranche of amendments following the Government's commitment to reform the Privacy Act 1988 (**Privacy Act**) in 2023. Among other things, the Bill introduced a "whitelist" mechanism to prescribe countries with substantially similar privacy laws to facilitate overseas data transfers. GDA supported this mechanism while also recommending that this mechanism prescribe the Cross Border Privacy Rules and ISO 27701 standards as certification schemes that would fulfil the criteria for substantial similarity (see: GDA's submission in October 2024). Other key amendments introduced include a new statutory tort for serious privacy invasions, transparency obligations for automated decisions, and criminalization of doxing. Members can access the finalised Bill and explanatory memoranda at: Privacy and Other Legislation Amendment Bill 2024 – Parliament of Australia.

China – CAC Publishes Draft Cross-Border Data Certification Mechanism: On January 3, 2025, the Cyberspace Administration of China (CAC) published the draft Measures for Certification of Personal Information (PI) Protection for Cross-Border Transfer. This certification mechanism is one of three approved data transfer mechanisms. (The other two are security assessments and standard contracts).

This mechanism applies only to non-Critical Infrastructure Information (CII) businesses transferring sensitive personal data of fewer than 10,000 individuals or non-sensitive personal data of fewer than 1 million individuals. The certification mechanism is not available for transfers of "important data" or to data transfers by CII operators. The mechanism also does not aim to alter any exemptions established in Chinese law.

The certification mechanism applies not only to transfers from China, but also to onward data transfers by overseas data handlers located outside China – thus potentially increasing CAC's oversight of data processing activities by overseas businesses.

Certification institutions are required to obtain permits from China's Certification Commission and make a filing with the CAC. The public consultation period for the draft Certification Measures will end on February 3.

China – CAC Publishes Report on Cross-Border Data Transfer Approvals: On January 2, 2025, the CAC announced the results of its regulatory activities vis-à-vis outbound cross-border data transfers in 2024. CAC stated that:

- The CAC carried out 285 security assessment projects and recorded 1,071 contracts as of December, with 27 applications failing to clear security assessment;
- Processing times for online applications decreased to ~30 working days – down from 45 days.

- The CAC approved more than 90 per cent of data exports in 2024;
- The less than 10 per cent blocked were either deemed as unnecessary or did not meet security standards;
- Businesses also no longer have to submit information on cross-border e-commerce, shipping, payments or visa processing for official security checks, or in connection with the opening of as well as bank accounts, booking flights, or reserving hotels;
- It is seeking to facilitate global exchanges and the sharing of capital, information, technology, talent, goods and other resources;
- Data transfers must still undergo a security assessment if they relate to critical information infrastructure, involve non-sensitive personal information of over one million people within a year, or include "sensitive information" of more than 10,000 people.
- The Beijing and Tianjin pilot free trade zones had created a "negative list" for outbound data transfers, with industries not on the list being open to data transfers without the need for government approval.
- Major cities such as Beijing, Shanghai, Guangzhou and Hangzhou have set up data outbound service centres and service platforms to offer guidance to companies.

China – Global Cross-Border Data Flow Cooperation Initiative: On November 16, at the 31st APEC Economic Leaders' Meeting, President Xi Jinping announced during a speech at APEC that China would lead a Global Cross-Border Data Flow Cooperation Initiative. The Cyberspace Administration of China (CAC) later published that Initiative, which contained a "call to action" for collaboration among governments to "facilitate" data transfers; "respect" diverse data governance systems; and "ensure" non-personal data security.

China – Beijing Data Transfer Negative List: The Beijing Municipal Internet Information Office, Beijing Municipal Commerce Bureau and Beijing Municipal Government Services and Data Administration Bureau ("Regulator") jointly issued the Data Export Management List (Negative List) of China (Beijing) Pilot Free Trade Zone ("Negative List") and the Administrative Measures for the Negative List ("Administrative Measures"). Sources: DGC Briefings; Hunton Andrew Kurth; Sidley. According to Hunton's Alert, "the Administrative Measures propose rules referencing 13 categories and 41 subcategories of data and for uniform identification of important data.

The Negative List lists five industries – automotive, pharmaceutical, retail, civil aviation and artificial intelligence – which are more important in practice for cross-border data transfers and outlines 23 business scenarios and 198 data elements for these industries. In certain of these scenarios, the Negative List relaxes the thresholds triggering the need for the security assessment, filing of the standard contract for cross-border transfers ("SC") and certification of protection of personal information. The Regulator will update the Negative List over time as needed."

The preliminary conclusions from DGC Briefings follow:

"Beijing's negative list does not specifically include as many industries as Tianjin's negative list. But it is still a very comprehensive list with long descriptions of data types and data subcategories. Add on the fact that there are various thresholds in this document that are different from the thresholds in the CBDT Regulations issued earlier this year (e.g. cumulative export of basic PI, diagnosis, healthy physiological info of >50k subjects starting from 1 Jan of the current year), and the compliance burden shoots up for companies using the FTZ and caught under the groups.

[It is concerning to see] "'AI training data' on a negative list. … [The inclusion of AI training data on the Beijing list] may inspire other provinces and even countries, to start placing restrictions on the export of data they think will be used to train AI."

Hong Kong – Protection of Critical Infrastructure Bill: On December 11, the Hong Kong Legislative Council conducted a second reading of the "Protection of Critical Infrastructure Bill."

India – DPDP Act Rules: On January 3, 2025, MeitY published the Digital Personal Data Protection Rules, 2025 (**Draft Rules**), the long-awaited rules to implement the Personal Data Protection Act (DPDP Act). Draft Rules here; Explanatory note here; comments to be submitted through portal here by Tuesday, February 18. While the DPDP Act made significant progress on key issues in the five years between its introduction and its passage in 2023, we remain concerned with several aspects of the Act and the new implementing Draft Rules. These include:

- *New restrictions on international data transfers*. Although the DPDP Act made significant progress on this issue, the final Act presumes that data can be transferred but reserves broad authority for the Central Government to restrict transfers. The Draft Rules contain two restrictions: (1) for all transfers, companies must comply with any requirements the Central Government sets with respect to making transferred data available to a foreign government (Draft Rule 14); (2) for significant data fiduciaries, the Central Government may specify data that the company cannot transfer outside of India (Draft Rule 12).

- *Concerning requirements for significant data fiduciaries*. While the DPDP Act envisions additional obligations for companies designated as significant data fiduciaries, the Draft Rules do not clarify the process by which the Central Government can designate a company as a significant data fiduciary. The Draft Rules also detail new requirements for data protection impact assessments and audits, including requiring significant data fiduciaries to submit to the Data Protection Board a report on those assessments and audits with "significant observations" from them. (Draft Rule 12.)

More specifically, under the DPDP Act, the Central Government can notify any data fiduciary or class of data fiduciaries as a "significant data fiduciary" subject to additional obligations including: (1) appointing an India-based data protection officer, (2) appointing an independent data auditor to evaluate the company's compliance with the Bill, (3) undertaking periodic data protection impact assessments, (4) undertaking periodic audits, and (5) other measures to be prescribed by regulation. The Central Government may determine a company is a significant data fiduciary based on factors it considers relevant, including the potential impact on the sovereignty and integrity of India, electoral democracy, security of the state, and public order. *Notably, the Draft Rules do not clarify the process for classifying a data fiduciary as a significant data fiduciary*. Instead, the Draft Rules focus on the additional requirements for significant data fiduciaries, including concerning new limits on transferring data outside of India. (Draft Rule 12.) Under the Draft Rules, a significant data fiduciary must:

- Conduct annual data protection impact assessments and an audit to ensure compliance with the Act
- *Submit to the Board a report with "significant observations" from the impact assessment and audit*
- Conduct due diligence on algorithmic software used to host, display, modify, publish, transmit, store, update, or share personal data, to ensure such software does not pose a risk to data principals' rights
- *Ensure personal data specified by the Central Government is not transferred outside of India.*

Furthermore, under the final DPDP Act, companies are permitted to transfer data outside India, but the Central Government is given broad authority to "restrict the transfer of personal data by a data fiduciary for processing to such country or territory outside India" upon notification. *The Draft Rules continue to reflect that broad authority to restrict transfers – and expressly contemplate that the Indian Government can limit companies' ability to transfer data if it can be made available to another government after transfer.* The Draft Rules state that transfers are subject to restrictions as the Central Government may impose by general or special order with respect to "making such personal data available to any foreign State or to any person or entity under the control of or any agency of such a State." (Draft Rule 14.)

MeitY seeks comments on the Draft Rules by Feb. 18. We intend to file comments and will circulate a draft submission for members' review in the coming weeks. We have also included our initial analysis

of the Draft Rules below, for your reference. Please reach out as your teams review the new rules and identify concerns and/or questions.

India – US-India ICT Working Group: On Thursday, October 17, BSA/GDA participated in the US – India ICT Working Group meeting held on Thursday, October 17 in New Delhi. The discussion featured a session on *Cross-Border Data Transfers* besides other policy issues in the ICT sector. GDA's report, the Cross-border Data Policy Principles, was quoted during the session on data transfers. The meeting was attended by government officials from the US State Department, the Ministry of Electronics and Information Technology, the Department of Telecommunications, and the Ministry of External Affairs besides industry participants from both US and India.

India – CBPR Workshop: BSA and GDA participated in a Technical Workshop on Cross Border Data Transfers and the Global Cross Border Privacy Rules (CBPR) Framework, hosted by nasscom, the Data Security Council of India, the Ministry of Electronics and Information Technology, and the Ministry of External Affairs. BSA and GDA met with government officials from India's Ministry of Electronics and Information Technology (MEITY) and the US Embassy in New Delhi to discuss provisions on cross-border data transfers with regards to implementing rules of the Digital Personal Data Protection Act 2023 (**DPDP Act**). We also organized a Privacy Discussion and luncheon with public and private sector experts to discuss issues related to implementing rules of the DPDP Act 2023 and international data transfers. BSA and GDA members and representatives from India's Ministry of Electronics and Information Technology (MeitY), Singapore's Infocomm Media Development Authority & Ministry of Trade and Investment, US Department of State, Department of Commerce & Federal Trade Commission attended the discussion.

Indonesia – Personal Data Protection Law: Indonesia's Personal Data Protection Law (PDP Law) came into force on October 17, two years from the date of promulgation. However, as of October 29, the two regulations supporting the PDP Law have not yet been issued: a Presidential Regulation to establish the independent personal data protection institution, and a Government Regulation setting out implementing rules for the PDP Law.

Indonesia – Government Regulation 71: BSA engaged officials from the Ministry of Communications and Informatics (KOMINFO) earlier this month on amendments to the **Government Regulation 71** (GR71). These amendments are likely to include data localization requirements as a way to encourage investments in local data centers. KOMINFO Minister Budi Arie **commented** that Indonesia is trailing Malaysia in attracting data center investment. At our meeting, we highlighted our concerns regarding data localization and Indonesia's ability to meet CPTPP and OECD commitments. While KOMINFO officials shared that they were targeting October 20 as their deadline for issuing amendments to GR71, as of October 29, no public consultation nor final document for GR71 has been issued.

Indonesia – CPTPP Accession: Indonesia has announced its application for accession to the **Comprehensive and Progressive Trans Pacific Partnership** (CPTPP). In our discussion with officials in charge from the Coordinating Ministry of Economic Affairs, Indonesia's main concerns under the e-commerce chapter are likely to include interconnection charge sharing, source code provision and customs duties on digital goods. Officials stressed that Indonesia is in early stages of the accession process.

Indonesia – Presidential Election: President Prabowo Subianto was sworn in on October 20. His speech highlighted many goals for his presidency, including tackling corruption and poverty, achieving food and energy security and continuing Indonesia's longstanding policy of non-alignment. Prabowo selected a very large cabinet with 48 ministers, up from 34 under President Joko Widodo (Jokowi). Prabowo also kept on many ministers from Jokowi's cabinet, including Finance Minister Sri Mulyani and Coordinating Minister for Economic Affairs Airlangga Hartarto. Another senior Jokowi official,

former Coordinating Minister for Maritime Affairs and Investment Luhut Pandjaitan will head the National Economic Council. Career bureaucrat Budi Santoso was appointed Trade Minister and Meutya Vidia Hafid, a former journalist before she became a politician, will lead the newly renamed Communications and Digital ministry. Hafid said she would focus on data protection, online safety for children and ensuring the internet is accessibility for all.

Japan – Industry Data Sub Working Group: On December 9, GDA participated in the Ministry of Economy, Trade and Industry's Industry Data Sub Working Group to continue discussion on developing a manual on international data governance, which aims to support companies to identify risks associated with cross-border data transfers and deepen understanding on appropriate data governance practices. The manual is planned to be released early next year. Previously, on September 24, BSA staff (Tomoko) testified in Tokyo before the Industry Data Sub-Working Group of the Ministry of Economy Trade & Industry (METI). In response to METI's questions, we outlined the cross-border data policy environment that Japanese stakeholders face across the APAC region and the globe; the types of risk assessments and mitigation strategies that some companies undertake to protect their industrial (non-personal) data in the course of cross-border data transfers to relatively more restrictive destination markets. If you would be interested in reviewing the GDA's presentation slides or notes, please let Joe or Tomoko know.

Japan - Asia Pacific Privacy Authorities (APPA) Forum: On November 26 and 27, Japan's Personal Information Protection Commission (PPC), hosted the 62nd APPA Forum, attended by APPA members and guests, including data protection and privacy authorities and other international networks. Discussions were held on a variety of common privacy issues, including cross-border data transfer and Data Free Flow with Trust (DFFT) – details can be found in the 62nd APPA Forum Communique. A side event involving multi stakeholders was also held on November 27 to discuss corporate initiatives and challenges on DFFT and safeguarding personal information using PETs.

Japan – Japan-EU Expansion of Adequacy Recognition Framework: Japan's Personal Information Protection Commission (PPC) and the European Commission is currently discussing the expansion of the EU's adequacy decision for Japan to also cover data flows to academia and the public sector (see joint statement released on June 20). As part of this effort, the PPC is proposing amendment to the Rules of PPC, to develop provisions to enable foreign country designation for cross-border transfers by the public sector under Article 71 of the Act on the Protection of Personal Information. PPC hopes to publish the proposed amendment and put it into effect by the fall of this year, after the conclusion of public comment period.

Japan – Economic Policy Consultations with United States: A US-Japan Fourth Economic Policy Consultative Committee Vice-Ministerial Meeting was held with Undersecretary of State Jose Fernandez, Undersecretary of Commerce Marisa Lago, Japanese Senior Deputy Foreign Minister Akahori Takeshi and Vice Minister of Economy, Trade and Industry Matsuo Takehiko. The leaders discussed the importance of promoting and protecting critical and emerging technology, as well as expanding the global market share and commercialization of Open Radio Access Network (Open RAN) technology, among other topics. State department release can be found here.

Malaysia – Personal Data Protection (Amendment) Act: Following the July 31, 2024 passage of Malaysia's Personal Data Protection (Amendment) Act, the Act now awaits royal assent and publication in the Federal Gazette before it go into effect. That process is expected to conclude by October 2024. For GDA purposes, the most significant change in the Amendment is the removal of the whitelisting regime for cross-border data transfers.

Under section 129 of the PDPA, outbound data transfers permitted either by: (a) a whitelisting mechanism (akin to an EU adequacy determination); or (b) alternative conditions mechanism (i.e., if the user can comply with at least one of the conditions in Article 129(3) of the PDPA). No jurisdictions have been "whitelisted" to date, and the Amendment will remove the whitelisting mechanism entirely. Instead, data users or controllers may now transfer personal data if they can demonstrate that the recipient jurisdiction's laws are substantially similar to, or offer an adequate level of protection equivalent to, the PDPA. This framework effectively shifts the burden of demonstrating "adequacy" to private entities, but offers greater flexibility than in jurisdictions in which transfers are predicated on (slow and halting) governmental adequacy determinations.

The Personal Data Commissioner is also currently developing the Cross-Border Data Transfers Guidelines to clarify the obligations of controllers under amended PDPA section 129. The Commissioner is also reportedly considering adoption of commonly used transfer mechanisms, such as standard contractual clauses, binding corporate rules, or certification mechanisms. For more information, please see Alert from Christopher & Lee Ong.

Malaysia – Senior Officials' Dialogue with United States: The 6th Malaysia-U.S. Senior Officials' Dialogue was held in Malaysia, led by Ministry of Foreign Affairs Secretary General Dato' Sri Amran Mohamed Zin and Assistant Secretary of State for East Asian and Pacific Affairs Daniel Kritenbrink. Several topics for future cooperation were discussed, including science and technology, Small and Medium Enterprise (SME) development and capacity-building. The dialogue commemorated the 10th anniversary of Malaysia-United States Comprehensive Partnership. Malaysia will have the opportunity to drive the ASEAN agenda next year as ASEAN Chair.

Taiwan – US-Taiwan Trade Agreement: On December 9, the United States announced that the US-Taiwan Trade Agreement went into force. Although the agreement does not contain a digital trade or e-commerce chapter, it does the following important commitments: (1) Chapter II: Trade Facilitation, which includes provisions on data transfers for e-invoicing, logistics, express shipping, freight forwarding, customs clearance, and other trade facilitative purposes; (2) Chapter III: Good Regulatory Practices, which include provisions on evidence-based rulemaking, administrative rulings; and other priorities; and (3) Chapter IV: Domestic Services Regulation, which governs licensing or qualification requirements imposed that allow/deny a person to supply a financial service or any other service. There are also chapters on Anti-Corruption and Small Businesses.

Thailand – Digital Economy Framework Agreement: Prime Minister Paetongtarn of Thailand expressed support to ASEAN's efforts to update and upgrade its free trade agreements with dialogue partners. As chair of the negotiations for the ASEAN Digital Economy Framework Agreement, Thailand aims to complete talks by 2025 to establish new mechanisms for economic growth within ASEAN. The PM has also engaged in bilateral meetings with ASEAN nation counterparts, proposing to strengthen cooperation with Singapore, Brunei, Cambodia, and Vietnam in areas such as the digital economy, AI, and digital transportation.

Thailand – US-Thai Digital Cooperation: Additionally, the Thai Prime Minister met with U.S. Secretary of State Antony J. Blinken, reaffirming Thailand's commitment to collaborate with the United States. They discussed enhancing cooperation on urgent public safety issues, including drug problems, online scams, and disaster management. Both leaders emphasized the importance of promoting increased trade and investment between the two nations. Blinken expressed the U.S.'s desire to work with Paetongtarn on initiatives to "better the lives of our people," focusing on economic growth, security, and climate change. They agreed to implement new technologies and share expertise to mitigate disaster risks and damages, highlighting the multifaceted nature of their bilateral relationship.

Vietnam – National Assembly enacts Data Law. On November 30, Vietnam's National Assembly passed the Data Law. The Data Law, proposed by the Ministry of Public Security, regulates both personal and non-personal data. Under the Data Law, businesses in Vietnam need obtain approval from the relevant authorities when "critical data" and "core data" (which are broadly and vaguely defined) are transferred overseas. Another concerning aspect of the Data Law is the new powers for the relevant authorities to access sensitive and personal information, including potentially from "data administrators" that process data on behalf of business customers. The Data Law is set to go into effect on July 1, 2025.

The Global Data Alliance had previously submitted **comments** to the public consultation by the Ministry of Public Security (**MPS**) on the draft Data Law. We raised concerns on the need for approval by relevant authorities prior to transferring "critical data" and "core data" overseas. Since the close of the public consultations on September 1, the MPS submitted the draft to the Ministry of Justice (**MOJ**) and the MOJ has sent out its appraisal report on the draft. MPS is in the process of revising the draft Data Law and appears to be moving on the process much faster than that of previous laws and decrees.

Vietnam – Personal Data Protection Law: On September 24, 2024, Vietnam published the draft Personal Data Protection Law. (Commentaries: DGC Briefing, Dezan Shira Firm, Baker McKenzie, Nishimura Law Firm). Public comments are due by November 24, 2024. GDA intends to comment. The PDPL contains a large number of new restrictions on the ability to transfer data across borders. The draft law is scheduled for enactment in May 2025, with an effective date of January 1, 2026. (For more information, please see email from Wai San dated Sept. 24, 2024). The draft law imposes obligations to conduct transfer impact assessments, to make impact assessments available to government authorities, and to face severe penalties (including cancellation of the authority to transfer data) for any violations.

The definitional scope of "data transfer" is very broad.

- Article 2(24) defines "overseas transfer" to include not only the act of transferring data, but also the act of accessing data from outside of Vietnam: (i.e., the "use of cyberspace, equipment, electronic means or other forms of transfer of personal data of Vietnamese citizens to a location outside the territory of the Socialist Republic of Vietnam or the use of a location outside the territory of the Socialist Republic of Vietnam for the processing of personal data.")

- Article 45 further defines transfers to include: (a) Sharing personal data with recipients outside [Vietnam]; (b) Sharing personal data at an overseas [or meeting]; (d) Publishing personal data in cyberspace that is received by persons outside [Vietnam]; (dd) Providing personal data to other organizations, enterprises and individuals for the purpose of carrying out business activities; and (e) Providing personal data on the fulfillment of legal obligations abroad or according to the laws of the host country.

The foregoing provisions imply the sharing of personal information within Vietnam will be treated as a transfer if it is accessed by those outside of Vietnam, even if that was not the intention and even if that outcome was not foreseeable. Additionally, subparagraphs (c) and (dd) raise questions as to whether provision to a Vietnam-based subsidiary of a foreign enterprise or to a non-national in Vietnam would be deemed to constitute a "transfer."

Vietnam – Draft Digital Technology Industry (DTI) Law: The Global Data Alliance submitted **comments** to the public consultation by the Ministry of Information and Communications (**MIC**) on the draft DTI Law. We raised concerns regarding notification requirements for cross-border transfers present in the draft law published on the MIC's public consultation website ("Draft 2"). We

commended the MIC for removing these requirements in subsequent drafts of the Law ("Drafts 3 and 4") and called for regulations to encourage cross-border data transfers.

Since the close of the public consultations in early September, the Legislative Institute under the National Assembly's Standing Committee held a **legislative conference** on the draft Law. There was also a new version of the DTI Law released, a "Draft 5." It appears that notification requirements for cross-border transfers continue to be absent from this latest Draft 5.

WESTERN HEMISPHERE

Brazil – Resolution CD / ANPD No. 19/2024: The Brazilian Data Protection Authority (ANPD) has published Resolution CD/ANPD No. 19/2024 – Brazil's regulations governing international data transfers. Consistent with BSA and GDA advocacy, the regulations promote streamlined and interoperable transfer mechanisms; recognize the importance of cross-border data transfers for various commercial and public policy goals; and advance principles of accountability and transparency. The Regulations address international data transfers in four scenarios:

- To countries or international organizations that provide adequate protection, as recognized by the ANPD, or
- When a controller guarantees protections consistent with the LGPD through the use of:
    - Specific contractual clauses (with new text for Brazilian SCCs contained in Annex II)
    - Standard contractual clauses
    - Global corporate standards

Notably, the Regulations create a process for the ANPD to recognize "equivalent contractual clauses" from other countries or international organizations, subject to certain criteria and processes.

Brazil – New ANPD Resources on Cross-Border Data Transfers: The Brazilian Data Protection Authority (ANPD) has launched a specific page on international data transfers on its official website. This online resource aims to ensure greater transparency and make it easier for companies and citizens to understand the relevant legal mechanisms governing the movement of personal data outside Brazil territory. These include contractual clauses and binding corporate rules. The webpage also offers detailed guidance on how to make and respond to informational requests vis-à-vis ANPD. There is also a Frequently Asked Questions (FAQ) section. Situations not covered by the FAQ can be resolved through the Fala.Br channel.

Brazil – Commercial Dialogue with the United States: Consistent with the GDA's 2024 recommendations for the US-Brazil Commercial Dialogue, discussions at the 22nd meeting of the U.S.-Brazil Commercial Dialogue focused on "promoting increased trade and continued collaboration across a variety of areas, including standards, intellectual property, trade in the digital economy, and working to prevent, reduce, and remove non-tariff trade barriers." Both countries also signed a Memorandum of Understanding on Good Regulatory Practices to "exchange of best practices to ensure that regulations contribute to creating a stable and transparent business environment, improving government efficiency and reducing regulatory duplication." Commerce readout here.

US – Department of Treasury Final Rule on Overseas Investments in Countries of Concern: January 2, 2025 is the effective date for the US Department of the Treasury's October 28, 2024 Final Rule on outbound investment restrictions. To aid compliance, Treasury has also issued Frequently

Asked Questions, Guidelines for National Interest Exemptions, as well as templates to submit mandatory notifications regarding (1) Notifiable Transactions; (2) Actions of a Controlled Foreign Entity; and (3) Post-Transaction Knowledge. These requirements are intended to implement President Biden's Executive Order 14105 of August 9, 2023, "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern." The Final Rule provides the operative regulations and a detailed explanatory discussion regarding its intent and application.

In the Outbound Order, the President directed the Secretary of the Treasury to issue regulations that:

1. prohibit U.S. persons from engaging in certain transactions with persons of a country of concern involving a defined set of technologies and products that pose a particularly acute national security threat to the United States, and

2. require U.S. persons to notify Treasury of certain other transactions with persons of a country of concern involving a defined set of technologies and products that may contribute to the threat to the national security of the United States.

The Final Rule issued today provides details on the subsets of technologies and products within the three sectors identified in the Outbound Order -- semiconductors and microelectronics; quantum information technologies; and artificial intelligence -- and fully implements a new program that will help address the advancement of key technologies and products by countries of concern that may use them to threaten US national security. The foregoing materials – as well as contact information for Treasury personnel – can be found at: Outbound Investment Security Program | U.S. Department of the Treasury.

US – Department of Justice Promulgation of Regulations on Americans' Sensitive Personal Data: On December 26, 2024, the Department of Justice (DoJ) National Security Division issued a Final Rule to implement Executive Order 14117. An unofficial version of the Final Rule is available here; the official version will be published in the Federal Register.

The Final Rule will become effective 90 days after publication in the Federal Register, with certain affirmative requirements regarding due diligence and audits for restricted transactions (subpart J), annual reports (§ 202.1103), and reports on rejected prohibited transactions (§ 202.1104) becoming effective 270 days after publication in the Federal Register. Press release; Fact sheet.

The Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) also issued the final security requirements with which U.S. persons engaged in restricted transactions must comply.

The final DoJ rules followed an October 29, 2024 DoJ Notice of Proposed Rulemaking on Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons. These draft rules reflected many positive changes attributable to the efforts of BSA and GDA members to persuade the DOJ to offer exemptions for a range of cross-border data scenarios relevant to the membership, including: (1) travel-related transactions; (2) corporate group transactions; (3) drug, biological product, and medical device authorizations; (4) ether clinical investigations and post-marketing surveillance data; (5) certain human biospecimens; (6) transactions required or authorized by Federal law or international agreements; and (7) telecommunications data.

On November 29, the GDA submitted its comments to the Office of Data Security within the US Department of Justice's National Security Division. GDA also performed outreach to the Office of Management & Budget (Office of Information & Regulatory Affairs), the State Department, the Commerce Department, and the Justice Department's Office of Legal Policy, Civil Division, and other parts of the US government. GDA prepared two non-public memoranda elaborating on civil rights and

cybersecurity concerns in those contexts. Finally, GDA has been undertaking quiet outreach to academics and public interest groups in this regard.

US – Department of Commerce AI Diffusion Rules: As of late December 2024, the Biden administration reportedly plans to impose a new regime that would allocate or restrict exports of AI chips based on a given country's strategic ties with the US. The program would block adversaries from accessing chips while allowing allies full access. Other countries would be permitted to buy semiconductors based on quotas. We have been monitoring these discussions and plan to weigh in at an appropriate juncture.

US – USTR Section 301 Investigation into Chinese Acts, Policies, and Practices relating to Semiconductor Technology: On December 23, 2024, the Office of the US Trade Representative (USTR) initiated an investigation into China's acts, policies, and practices related to targeting of the semiconductor industry for dominance. The investigation is to be conducted under Section 301 of the Trade Act of 1974, as amended. According to USTR, "[e]vidence indicates that China seeks to dominate domestic and global markets in the semiconductor industry and undertakes extensive anticompetitive and non-market means, including setting and pursuing market share targets, to achieve indigenization and self-sufficiency. China's acts, policies, and practices appear to have and to threaten detrimental impacts on the United States and other economies, undermining the competitiveness of American industry and workers, critical U.S. supply chains, and U.S. economic security."

US – USTR Solicitation of Comments for Annual Special 301 Intellectual Property Review: On December 6, 2024, USTR published its solicitation of input for the annual "Special 301" review regarding the state of intellectual property (IP) protection and enforcement around the world. The solicitation seeks input on "those countries the 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 has filed comments with USTR for the Special 301 in recent years. Our 2024 comments can be found here.

US – President's Export Council Recommendations on Artificial Intelligence: On December 10, the President's Export Council issued recommendations to advance US leadership in the development and regulation of AI. Several of these recommendations underscore the importance of data transfers and cross-border access to information in the AI context. This includes recommendations for:

- Industry-wide, cross-sectoral data-sharing frameworks should be promoted to facilitate the creation of specialized AI tools. In particular, AI differs from other technologies through the critical role of data, which makes access to massive amounts of data essential in order to maintain competitiveness in any industry sector… [as well as] consortia and data sharing forums to support SMEs, civil society organizations and other social impact organizations in collecting, cleaning, storing and utilizing large datasets...

- [A] coordinated, inter-agency approach [to AI innovation], especially in managing data flows, ensuring interoperability, and reinforcing ethical standards across sectors, including in agriculture, which is a critical infrastructure and requires cybersecurity standards and best practices.

- [A] network of AI Ethics, Regulation, and Transparency (ERT) centers to foster real-time information sharing and collaboration. These centers would serve as hubs to support businesses in managing data flows and optimizing AI-driven supply chains with built-in resilience, as well as offer guidance to trade partners on compliance, best practices, and innovation-friendly approaches.

US – White House National Security Memo on AI: On October 24, 2024, the White House issued its first public national security memo on AI, outlining the administration's approach to promoting AI development for national security purposes, including cybersecurity and counterintelligence, while protecting human rights and privacy. The approach focuses on three objectives:

(1) Ensuring that the US leads the world's development of safe, secure, and trustworthy AI, including actions to improve chip supply chains diversity and security; protecting work on AI from spying or theft by foreign adversaries; and bolstering key drivers of AI progress, such as technical talent and computational power.
(2) Harnessing cutting-edge AI technologies to advance the USG national security mission while protecting human rights and democratic values. The Commerce Department's AI Safety Institute will serve as the primary checkpoint for testing new systems before deployment. Guardrails will include guidance for agencies to monitor, assess, and mitigate AI risks related to invasions of privacy, bias and discrimination, safety, and other human rights abuses. A companion Framework to Advance AI Governance and Risk Management in National Security is expected to outline further instructions for agencies.
(3) Advancing international consensus and governance around AI. Building on progress made on AI governance with the G7, UN and others, the US will lead in developing effective global norms and engaging in institutions rooted in international law, human rights, civil rights, and democratic values.

US – Submission on Foreign Cross-Border Data Trade Barriers: On October 17, 2024, the GDA submitted comments to the USTR in response to its solicitation of input regarding foreign trade barriers. GDA's submission addressed the following topics: (1) Economic Benefits of Cross-Border Data Transfers; (2) Economic Costs of Data Transfer Restrictions and Data Localization Mandates; (3) Policy Arguments Relating to Data Transfer Restrictions and Data Localization Mandates; (4) Cross-Border Data Policies in International Agreements; and (5) The GDA Cross-Border Data Policy Principles. The GDA submission also discussed specific challenges in Brazil, Cambodia, China, India, Indonesia, Saudi Arabia, South Korea, Turkey, the UAE, and the EU (among other jurisdictions).

US – Connected Vehicles Rulemaking: On September 26, 2024, the US Department of Commerce's Bureau of Industry and Security (BIS) published a Notice of Proposed Rulemaking (NPRM) that would prohibit the sale or import of connected vehicles integrating specific pieces of hardware and software, or those components sold separately, with a sufficient nexus to China or Russia. This prohibition sweeps more broadly than the more focused approach advocated by the GDA in its 2024 Comments to BIS.

The proposed rule focuses on hardware and software integrated into the Vehicle Connectivity System (VCS) and software integrated into the Automated Driving System (ADS). These are the critical systems that, through specific hardware and software, allow for external connectivity and autonomous driving capabilities in connected vehicles. Malicious access to these systems could allow adversaries to access and collect our most sensitive data and remotely manipulate cars on American roads. The

proposed rule would apply to all wheeled on-road vehicles such as cars, trucks, and buses, but would exclude vehicles not used on public roads like agricultural or mining vehicles.

BIS and its Office of Information and Communications Technology and Services (OICTS) have found that certain technologies originating from the PRC or Russia present an undue risk to both U.S. critical infrastructure and those who use connected vehicles. The proposed rule can be found here. Comments are due within 30 days.

US – Commerce Department Efforts to Promote the Digital Economy. On September 20, 2024, the Commerce Department's International Trade Administration outlined the following efforts to strengthen U.S. competitiveness and trade in the digital economy. Excerpts follow:

1. **New Global Digital Economy Reporting**: To better inform and serve MSMEs, ITA's Country Commercial Guides will now include a separate chapter on the digital economy. This chapter provides practical and actionable information to help U.S. businesses stay informed of the latest trends, opportunities, and challenges impacting the digital economy. U.S. businesses can access this new information on Trade.gov. Going forward, the Digital Economy chapter will be updated annually.
2. **Training Digital Attachés and Growing Linkages with Leading U.S. Tech Companies**: Based in U.S. embassies around the world, ITA's digital attachés specialize in promoting commercial exchange, tackling market access barriers and developing partnerships. Working with the Business Council for International Understanding (BCIU) and others in industry, ITA plans to strengthen the professional development of its digital attachés by training our staff and enhancing linkages with leading U.S. Fortune 500 and small and medium-sized tech companies through substantive engagement before those Attachés arrive in their overseas posts. This experience will empower commercial diplomats to be stronger advocates for U.S. commercial interests in foreign markets and help strengthen U.S. leadership in the digital economy.
3. **Supporting MSME Tech Exporters**: In collaboration with the Economic Development Administration (EDA), ITA's U.S. Commercial Service offices recently developed a support mechanism to aid the 31 Tech Hubs, designated by EDA last year, to build their capacity to provide tailored advice and support that helps to maximize the growth potential of MSMEs working with each Hub.
4. **Digital Economy Trade Missions:** With the growth of barriers to trade in the digital economy, beginning this year, ITA is pursuing more executive-led commercial diplomacy trade missions focused exclusively on U.S. exports of digitally-enabled services. These missions would feature government-to-government policy engagement with the support of participants from the U.S. business community. They would also target different regions. ITA will continue to organize several business development trade missions in sectors like Cybersecurity and Financial Technology.

US – Congressional Hearing on Cross-Border Data & Digital Trade: On September 20, 2024, the House Ways & Means Committee (Trade Subcommittee) held a hearing entitled, "Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules. The hearing examined the importance of digital trade rules to the U.S. economy, freedom of expression and human rights abroad, and the ability of small businesses to operate in remote markets with small workforces. BSA and GDA actively worked with congressional offices and witnesses to prepare for the hearing, drawing on GDA advocacy materials.

In one representative exchange Suzan DelBene (D-WA), co-chair of the Digital Trade Caucus, noted: "if we step back from the negotiating table until Congress acts, we run a serious risk of harming the very objectives, such as defending American companies, protecting privacy, and supporting a free and open internet, that have been core to U.S. policy for many years." Rep. DelBene posed this question: "Does the U.S. entering into trade agreements prevent Congress or the Administration from legislating or regulating on important issues domestically?"

Mr. Evangelos Razis (Workday) answered as follow: "No, we don't see any tension between privacy protections and strong digital trade rules. Many of the privacy frameworks, either that have been proposed here, and we agree federal privacy reform is long overdue, or, you know, the one of the 19 comprehensive state laws that have been enacted, have no tension with either USMCA or the US-Japan agreement. That's because those laws or bills don't enact data localization requirements, they don't restrict the free flow of transfers of information. And importantly, within USMCA, there's a pretty clear language that if there should be any tension in the future between domestic regulation and international trade agreements, U.S. law prevails."

US – International AI Governance Initiatives: On September 23, 2024, Secretary Blinken announced the Partnership for Global Inclusivity on AI with the private sector, which includes $10 million in U.S. foreign assistance on AI development, focused on expanding access with the hopes of working with Congress to provide $23 million more in the future. State department release can be found here. The US, along with 39 governments, released the Freedom Online Coalition Joint Statement on Responsible Government Practices for AI Technologies. Secretaries Raimondo and Blinken also co-hosted the inaugural meeting of the International Network of AI Safety Institutes in San Francisco on November 20-21, 2024. This brought together technical experts on artificial intelligence from each member's AI safety institute "in order to align on priority work areas for the Network and begin advancing global collaboration and knowledge sharing on AI safety." The initial members of the International Network of AI Safety Institutes are Australia, Canada, the European Union, France, Japan, Kenya, the Republic of Korea, Singapore, the United Kingdom, and the United States. Commerce readout can be found here.

US – Congressional Proposals to Restrict Remote Access to US Cloud Computing Resources: During October and November, we worked closely with Republican and Democratic offices on both sides of the Capitol to discuss industry concerns with the so-called Remote Access Security Act (RASA) (HR 8152), a proposal that would have restricted cross-border data access to US-based cloud computing resources from a wide array of economies pursuant to US export controls. Our advocacy sought to focus any potential restrictions under RASA on countries of concern, such as China and Russia, and to focus on high-risk technologies. Our efforts appear to have been successful to some extent, although the RASA legislation was not ultimately included in the National Defense Authorization Act (NDAA) package, but it is possible that this legislation may reemerge in a continuing resolution.

US – Congressional Proposals to Restrict US High Technology Investment in China: Congress has been seeking to further expand restrictions on US outbound investment in several high-technology areas, including AI, semiconductors, and quantum computing via the Comprehensive Outbound National Security Act of 2024 (COINS Act). The COINS Act was neither included in the final NDAA package, nor the Continuing Resolution stopgap spending bill. However, we expect investment restrictions vis-à-vis China to remain a US legislative priority in the 119th Congress. The COINS Act differs in some respects from the new Treasury Department outbound investment review framework. COINS bans US investment in 15 "prohibited technologies" that generally relate to the semiconductor, quantum computing and AI sectors, but also includes a mandatory reporting obligation relating to all AI

technologies, including “operational cooperation, such as through supply or support arrangements.” This could effectively require significant reporting by entities in all sectors that transfer data to China that is indirectly connected to an AI technology. This reporting obligation is much broader than the Treasury Department framework. We are reaching out to congressional offices to highlight the (possibly unintended) overbreadth of this text.

US – US-Taiwan Trade Agreement: See entry under “Taiwan.”

GLOBAL

G20 Trade and Finance Ministers Meetings: G20 trade ministers agreed on a set of non-binding principles to inform trade and sustainable development. The countries affirmed their “sovereign right to regulate and implement measures in pursuit of legitimate public policy objectives, including those related to sustainable development, in its economic, social and environmental pillars” as well as a call for policies that “seek to contribute to a favorable trade environment, for example, by promoting fair competition and inclusivity and, as appropriate, by minimizing negative impacts as much as possible,” among others. In addition, ministers expressed support to intensify work toward reforming the WTO. See the principles here.

IPEF – Ratifications: Singapore became the fifth IPEF member to ratify the IPEF Clean Economy Agreement, starting a 30-day clock toward entry into force. Singapore also ratified the Fair Economy Agreement (as the fourth signatory) and the overarching IPEF agreement (as the fifth signatory). Five countries must ratify each agreement before they can take effect. The IPEF Supply Chain Agreement is already in force for the eight countries that have accepted or ratified it. IPEF’s trade pillar continues to be under negotiation with no known progress reported.

IPEF – Supply Chain Summit: On September 10, 2024, the Commerce Department, in collaboration with the Council on Foreign Relations (CFR), hosted an inaugural Supply Chain Summit to highlight the work the Biden-Harris Administration and industry is doing to strengthen supply chain resilience. During the summit, Commerce launched a diagnostic supply chain risk assessment tool, called SCALE, which utilizes various indicators to assess structural supply chain risk across the US economy. The new tool has already been used to assess the vulnerabilities in US supply chains serving artificial intelligence data centers, an area of focus for Secretary Raimondo which she has called AI a critical industry in our rivalry with China. Commerce press release can be found here.

United Nations – On Sept. 22-23, 2024, the United Nations hosted the Summit of the Future (https://www.un.org/en/) - which brings together "world leaders to forge a new international consensus on delivering a better present and safeguarding the future." This includes a Global Digital Compact that includes the following commitments:

> **Cross-Border Data Flows:** We recognize the potential social, economic and development benefits of secure and trusted cross-border data flows, in particular for micro-, small and medium-sized enterprises. We will identify innovative, interoperable and inclusive mechanisms to enable data to flow with trust within and between countries to mutual benefit, while respecting relevant data protection and privacy safeguards and applicable legal frameworks (SDG 17).
>
> **Data Privacy and Security:**

(a) Draw on existing international and regional guidelines on the protection of privacy in the development of data governance frameworks (all SDGs);

(b) Strengthen support to all countries to develop effective and interoperable national data governance frameworks (all SDGs);

(c) Empower individuals and groups with the ability to consider, give and withdraw their consent to the use of their data and the ability to choose how those data are used... (SDGs 10 and 16);

(d) Ensure that data collection, access, sharing, transfer, storage and processing practices are safe, secure and proportionate for necessary, explicit and legitimate purposes...

(e) Develop skilled workforces capable of collecting, processing, analyzing, storing and transferring data safely in ways that protect privacy (SDGs 8 and 9).

Data for the SDGs: Increase financing for data and statistics from all sources ... (SDG 17); and strengthen efforts to collect, analyze and disseminate relevant, accurate, reliable and disaggregated data for better monitoring and policymaking ...

Interoperable Data Governance: We request the Commission on Science and Technology for Development to establish a dedicated working group to engage in a comprehensive and inclusive multistakeholder dialogue on data governance at all levels as relevant for development.

WTO – Trade in Services for Development Initiative: On September 13, 2024, the WTO launched a new initiative on Trade in Services for Development, which follows up on the recommendations contained in the joint publication entitled “Trade in Services for Development” launched by the WTO and the World Bank in 2023. The initiative is underwritten by the UK government. The initiative will include a Competitiveness Diagnostic Checklist that will help developing economies assess their competitiveness in services trade, define overarching national services trade policy objectives and prioritize technical assistance needs. Developing economies will also receive technical support to improve data collection and use of services trade statistics, as well as assistance on the identification and transparency of core services trade measures. The work program will also aim to help developing economies build on best practices to expand and diversify their services exports.