GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS
UPDATES

APRIL-JUNE 2021

Contents

RECENT POLICY DEVELOPMENTS

I. European Union and United Kingdom

A. European Union

EU – EDPB Recommendations: On June 18, the European Data Protection Board ("EDPB") issued its final Recommendations on supplementary measures for data transfer tools, available here. The draft Recommendations released by the EDPB late last year raised significant concerns for many companies, including by taking a narrow view of the circumstances that companies can consider when assessing transfers to third countries. Five aspects of the Recommendations are worth flagging:

- ***Six-Step Process for Assessing Transfers.*** The final Recommendations retain the six-step process put forward last year by the EDPB, outlining how companies are to assess third country laws and identify any appropriate supplementary measures.
- ***Third-Country Assessments***. The final Recommendations significantly revise the guidance on assessing third-country laws. They also recognize that when a third country's law is problematic, a company can still transfer data without supplementary measures if it can demonstrate and document that the law is not interpreted and/or applied in practice to cover the relevant transfer. This focus on practical experience is similar in kind to the final SCCs, which recognize that companies may consider practical experience in certain circumstances.
- ***Information for Assessments***. When companies assess a third country's laws, they must rely on information that is "relevant, objective, reliable, verifiable and publicly available or otherwise accessible." The final Recommendations define each of these terms, including emphasizing that information is objective when it is "supported by empirical evidence based on knowledge gained from the past, not assumptions about potential events and risks." Annex 3 has also been broadened to list significantly more sources of information that companies may rely on in these assessments.
- ***Use Cases***. As you recall, GDA's comments to the EDPB on their draft Recommendations raised a number of concerns about the illustrative Use Case 7 (remote access to data for business purposes). The final Recommendations retain the most problematic aspects of several use cases, which state the EDPB is "incapable of envisioning" an effective technical measure to prevent access from infringing on data subject rights in each case.
- ***Continued Focus on Technical Safeguards***. The final Recommendations remain focused on technical safeguards, without equally emphasizing the utility of contractual and organizational safeguards. For example, paragraph 53 states that "[c]ontractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation and/or practices. Indeed there will be situations where only appropriately implemented technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes."

Other sources: Covington, DLA Piper, Hunton, IAPP, MayerBrown, NLR, OneTrust.

EU – New SCCs: On June 4, the European Commission issued new standard contractual clauses (SCCs) for data transfers. The Global Data Alliance (GDA) and BSA | The Software Alliance issued supportive statements. (GDA here, BSA here).

The final SCCs retain the modular approach introduced in the draft SCCs published last year. Under this approach, the SCCs include both a general set of clauses, which apply to all transfers, and four "modules" designed to apply to four distinct types of transfers. This scope addresses one of the key challenges with the former SCCs: namely, that they did not apply to transfers originated by processors. As with the draft SCCs, the final SCCs anticipate that companies will assess the laws of the country to which data is transferred – and now specify that both the laws and "practices" of that country are relevant to such an assessment. *(See also Note below re "EU Data Transfer Project" describing our coordination of country-specific legal summaries for the benefit of GDA members).*

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

Finally, companies will need to transition their new contracts to the new SCCs by Sept. 27, 2021. For previously concluded contracts, companies may continue to rely on the old SCCs until Dec. 27, 2022. (See Article 4 of the implementing decision.) Other coverage: Bird&Bird, BakerMcKenzie, DLAPiper, Covington, HoganLovells, Gibson Dunn.

EU – Third Country Adequacy Assessments: The European Commission is expected to complete its assessment of the existing adequacy decisions with Third Countries during the summer. This evaluation exercise is a requirement under the GDPR and should have been completed by May 2020. DG Justice is expected to release this report in the form of a Communication that would address the general situation of the adequacy regime, including in light of the Schrems II ruling. Individual Third Country adequacy decisions will be analyzed in the annex. The Commission report is expected to be constructive and leave room to Third Country for improvement where weaknesses may have been identified, rather than recommending any drastic measures such as suspension of the decision. The European Parliament is expected to deliver a report on the Commission's assessment.

EU-UK Adequacy: On June 28, the European Commission has adopted its two adequacy decisions for the United Kingdom: one under GDPR and one under the Law Enforcement Directive (both attached). The adequacy decisions, in the form of Commission implementing decisions, take immediate effect. EU Member States had already given their positive opinion on the two draft decisions on June 16. An initial analysis shows that the final text of the adequacy decision under the GDPR has been slightly edited in a few areas:

- It includes a carve out for UK immigration control purposes (recital 6; article 1); it refines the definition of "competent authorities" under the Data Protection Act 2018 (recital 123);
- It also contains additional references to the sharing of data with third country intelligence service throughout section 3.3.1.1 Investigatory powers exercised in the context of national security;
- In case the level of protection afforded by the UK is no longer adequate, the decision now sets a three-months period for UK authorities to take appropriate measures (as opposed to a "reasonable timeframe" in the draft decision), with a possible extension depending on circumstances;
- Finally, the Decision shall expire on 27 June 2025, unless extended.

This late hour adoption avoids a cliff-edge scenario but does not fully alleviate European concerns regarding UK's ambitions to adapt its data privacy framework, in particular regarding onward transfers and new sets of SCCs currently being developed by the UK Information Commissioner's Office, as evidenced by the language in recitals 281-282 of the decision.

The history of the UK adequacy process may be instructive for future adequacy negotiations with other countries. The EU's formal approval process ran through the Article 93 Committee of Member States. The overall context for that process became complex in the run up to the June 28 decision:

- The ECHR ruled on May 24 that the UK bulk surveillance regime failed to meet "end-to-end safeguards" to ensure interception operations are properly checked. In particular the ruling notes that no independent watchdog reviews interception authorizations in the UK. This ruling focused on the 2000 RIPA legislation, which has since then been replaced by the 2016 Investigatory Powers Act. The European Commission references the latter in its draft adequacy decision; the ruling is not expected to have a direct impact on the draft adequacy decisions although it comforts the case that Commission made in these draft decisions that the ECHR has competence over third country national security matters. It is worth noting that the ECHR held a similar ruling regarding Sweden's bulk interception regime.

- The European Parliament adopted a non-binding resolution that called for the draft adequacy decisions to be amended by the Commission. The resolution underlines concerns about the UK's broad exemptions for national security and immigration; the lack of effective oversight by the UK DPA (ICO) and Courts over the use of this national security exemption, and concerns regarding onward transfers of data and bulk access to data by law enforcement. The resolution has no formal bearing on the approval process but constitutes an unhelpful development. The Parliamentary resolution followed two earlier resolutions by groups within the Civil Liberties (LIBE) Committee:
    - The first resolution asked the Commission to amend its draft adequacy decisions to bring them in line with EU court rulings and concerns raised by the European Data Protection Board it its April 14 opinion. France and the UK both addressed formal letters to the LIBE Committee Chair to express concerns over this Resolution and to underline the importance to continued data flows between the block and the UK. In its letter, France supports amendments that would recognize that "the UK has […] significantly reformed its surveillance laws and introduced safeguards which go beyond the conditions defined by the CJEU in its Schrems II ruling and which go beyond the safeguards provided in the surveillance laws of most Member States."
    - The second resolution was put forward by other political groups in support of the Commission's draft adequacy decisions.

EU-US Privacy Shield: EU-US Privacy Shield negotiations continue, but the timeline remains unclear. On June 10, the GDA and BSA submitted a letter to President Ursula von der Leyen and President Biden in relation to an enhanced Privacy Shield agreement. The GDA letter underscored the benefits of Privacy Shield to EU and US citizens and businesses alike. Other groups have made similar appeals. For example, a group of German associations published a joint paper on the need to preserve international data transfers following the CJEU *Schrems II* ruling. In the letter, the German business community calls upon the European Commission to negotiate an effective successor to the Privacy Shield as quickly as possible and to improve standard contractual clauses (SCCs) for EU data transfers. They also call on the DPAs to formulate EU-uniform criteria that give companies guidance on a permissible approach to data transfers to third countries and encourage adjusting the standards of the GDPR, which are in some cases narrow and not universally recognized.

EU Data Transfer Project: We have received from Covington & Burling reviews undertaken as part of the post-*Schrems II* EU data transfer project. These reviews, covering **Australia, Brazil, India, Mexico, Hong Kong, Singapore, and the Philippines**, provide a descriptive, informational cataloging of the relevant legal environment in selected countries, based upon which each company can perform its own fact-specific legal assessment for each type of data transfer that it conducts. Please feel free to share these documents with your in-house privacy and data protection counsel. If there is member support and participation, we would consider requesting additional reviews for the **United States, China, Malaysia**, or other countries of interest to the membership.

EU-Japan Summit: On May 27, EU and Japan held their annual summit as the EU-Japan Strategic Partnership turns 20. Discussions covered COVID resilience, sustainable trade, connectivity, industrial policy and R&D among others. The Summit Conclusions show a commitment to "continued cooperation to Data Free Flow with Trust with a view to facilitating safe and secure cross-border data flows through enhancing security and privacy." Both partners will seek to accelerate the review process of the mutual data adequacy arrangement, building on a successful meeting at Commissioner's level.

B. France

French DPA Activity Report: The CNIL (Commission Nationale de l'Informatique et des Libertés) released its activity report on 20 May, recapping all the major milestones of 2020, including the CJEU Schrems II ruling and Brexit. Looking ahead, the report identifies "data hosting in a sovereign cloud" as a priority for next year. According to the report, a sovereign cloud "is the best protection against overly intrusive foreign legislation and this ambition is not limited to health data. We know that everything cannot change overnight but the strong reprimands from the Court of Justice of the European Union must encourage all the actors concerned to act in this direction."

French Cloud Strategy: On May 17, the French Government unveiled the contours of its long-awaited Cloud Strategy, which primarily aims at addressing the perceived lack of protection against cybersecurity threats and trust concerns related to Third Countries' governments access to data. During the press conference, the French Government presented the strategy's high-level objectives with an expected digital sovereignty tone including through localization requirements. The strategy has not yet been fully presented and many concepts, details and practical implications are still unclear. Based on the information made available, the new strategy is built on three pillars.

- The first one amounts to creating a "Trusted Cloud" Label, which according to French officials is in direct response to the CJEU Schrems II ruling. Cloud services seeking to obtain the 'trusted cloud' label would have to comply with two types of requirements: technical protection, including by obtaining the SecNumCloud certification from ANSSI (French cybersecurity agency); and legal protection, by meeting two conditions to ensure immunity from extraterritorial legislation: the servers would have to be located in France, and companies would have to be European and owned by Europeans. The strategy also envisages new types of partnerships, for instance through technology licensing.
- The second pillar focuses on modernizing the public sector by putting cloud at the center of its digital transformation.
- The third pillar focuses on industrial policy and foresees that the French recovery plan will be partially earmarked to support the emergence of new cloud offering meeting the requirements set out above.

An administrative decision is expected to be issued soon with more details about the Strategy. Press statement and transcript are available here (only in French).

C. United Kingdom

UK-US New Atlantic Charter: On June 10, the United States and the United Kingdom announced a New Atlantic Charter. The Charter addresses several issues directly or indirectly relevant to cross-border data policy, including shared commitments to:

> Para. 4. "[R]esolve to harness and protect our innovative edge in science and technology to support our shared security and deliver jobs at home; to open new markets; to promote the development and deployment of new standards and technologies to support democratic values; to continue to invest in research into the biggest challenges facing the world; and to foster sustainable global development"; and
>
> Para. 6. "[A]n inclusive, fair, climate-friendly, sustainable, rules-based global economy for the 21st century. We will strengthen financial stability and transparency, fight corruption and illicit finance, and innovate and compete through high labour and environmental standards."

Additionally, the Charter expresses support for: (a) democracy and open societies; (b) open and fair trade; and (c) collaboration in matters of health, climate change, defense, and other priorities.

UK – Electronic Communication Security Regulations: The Department of Digital Culture, Media and Sports (DCMS) is working on the draft UK Electronic Communications (Security Measures) Regulations 2021. The framework will contain three parts: (1) a Telecoms security Bill containing general duties; (2) a Statutory Instrument and (3) a Code of Practice to support the implementation of the Bill. The development of the Code of Practice will then be led by telecoms regulator Ofcom and will allow for stakeholder formal feedback over the summer. The Code of Practice is expected to be finalized early 2022.

On June 10, the GDA had submitted comments to the UK Department for Digital, Culture, Media and Sport (DCMS) regarding the UK Electronic Communications (Security Measures) Regulations 2021. The GDA will meet with DCMS on June 20 to discuss data localization requirements in those measures, which would require network providers to, among other things:

(1) "maintain the operation of… a public electronic communications network located in the United Kingdom, without reliance on persons, equipment or stored data located outside the United Kingdom." (Art. 3.3(f));

(2) "ensure that tools enabling monitoring or audit cannot be accessed from outside the United Kingdom…" (Art. 4.3(f)); and
(3) "avoid dependence on persons, equipment or stored data located outside the United Kingdom" (Art. 5.3(h)).

UK – CPTPP Accession: On June 2, the United Kingdom was formally accepted to begin the accession process into the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). Official press statement here. The UK's accession process offers an opportunity to seek to upgrade CPTPP commitments or produce similar (but non-binding) outcomes in relation to cross-border data transfers between CPTPP members and the United Kingdom.

UK National Data Strategy: On May 18, the UK updated its National Data Strategy aimed at fostering better use of data across businesses, government, civil society and individuals. The draft Strategy was submitted to a public consultation in December and the GDA submitted comments. The Strategy addresses effective use of data across five priority missions, including unlocking the value of data across the economy; securing a pro-growth and trusted data regime; and championing the international flow of data. The UK has since December acted on a number of these missions, including in relations to international data transfers such as commitments in the FTA with Japan and reciprocal free flows of personal data with all non-EU countries that the UK recognizes as adequate (including Japan, Canada and Israel). Several other deliverables are longer-term prospects or ongoing processes (e.g., adequacy decision with the EU). More details can be found here.

UK-New Zealand MOU on Cross-Border Privacy Enforcement: On May 12, the UK Information Commissioner's Office (ICO) and New Zealand's Office of the Privacy Commissioner (OPC) announced a Memorandum of Understanding regarding collaboration on cross-border privacy enforcement issues. MOU link here. ICO press statement here.

II. Middle East & Africa

A. Kenya

Kenya – General Data Protection Implementing Regulations: Pursuant to its General Data Protection law, Kenya has published draft implementing regulations (as well as draft enforcement regulations and regulations to register data processors and controllers). The implementing rules include the following cross-border data features:

- Consent and Notification requirements: In addition to notifying data subjects of the risks of a future data transfer, each transferring entity must ascertain, prior to the data transfer, that: (a) the recipient in the transferee country is bound to a standard of privacy protection (at least) comparable to that found in Kenya; (b) the data subject consents to the transfer, and that the subject's rights will be protected; and (c) the transferred data will not be used for any other intended purpose.
- Transfer agreements: Each transferring entity must enter into a written agreement with the recipient of personal data requiring future "unlimited access" by the transferring entity to the data, as well as an identification of the countries to which the data may be transferred.
- Transfer guarantees: Cross-border transfer restrictions are not permitted where the transfer is deemed pemissibled under under legal provisions (section 48 (c) of the Act) or whether such restrictions: (a) arbitrarily or unjustifiably discriminate against any person; (b) impose a restriction on trade; or (c) are greater than are required to achieve a policy objective.
- Data protection safeguards deemed appropriate: Any country to which data is being transferred is deemed to have "appropriate data protection safeguards" (as required by section 49(1) of the Act) if that country has: (a) ratified the African Union Convention on Cyber Security and Personal Data Protection; (b) reciprocal data protection agreement with Kenya; (c) an adequate data protection law as shall be determined by the Data Commissioner.

B. South Africa

South African National Data and Cloud Policy –

On June 18, GDA staff attended a virtual consultative forum/colloquium on the South Africa draft Data and Cloud Policy, hosted by the Department of Communications and Digital Technologies on June 18. The GDA was invited to this stakeholder colloquium following our submission to the public consultation. Minister Stella Ndabeni-Abrahams opened the event by explaining that the draft policy is not to control or decide how data should be used, but rather meant as an enabler for social and economic development. On May 12, the Global Data Alliance filed its submission to the South African Department of Communications and Digital Technologies on the proposed National Data and Cloud Policy. That Policy contains the following cross-border data elements:

- 10.4.1 All data classified/identified as critical Information Infrastructure shall be processed and stored within the borders of South Africa.
- 10.4.2 Cross-border transfer of citizen data shall only be carried out in adherence with South African privacy protection policies and legislation (POPIA), the provisions of the Constitution, and in compliance with international best practise.
- 10.4.3 Notwithstanding the policy intervention above, a copy of such data must be stored in South Africa for the purposes of law enforcement.

III. Asia-Pacific

A. Australia

Australia-UK Trade Agreement: On April 23, the UK and Australia announced that both countries had reached consensus on most elements of a comprehensive free trade agreement. Based on provisions of the Australia-Singapore Digital Economy Agreement and the UK-Japan Comprehensive Economic Partnership Agreement, it is to be expected that both countries will also agree to reasonably ambitious digital trade outcomes. We are reaching out to relevant authorties to learn more.

Australia – Review of the Japan Australia Economic Partnership Agreement: On May 17, the Australian Department of Foreign Affairs and Trade (DFAT) commenced a public consultation as part of a general review of the Japan-Australia Economic Partnership Agreement (JAEPA). DFAT notes that their approach to the review will consider outcomes agreed to in subsequent agreements including the CPTPP and the Regional Comprehensive Economic Partnership (RCEP).

B. Bangladesh

Bangladesh National Cloud Policy Submission: On May 12, the GDA filed comments on cross-border data restrictions in Bangladesh's National Cloud Policy. The National Cloud Policy contains strict data localization requirements, stating in in relevant part that, "[t]he primary location of cloud service provider's data storage must be in Bangladesh. Information may be allowed to be taken outside Bangladesh for back-up and retrieval purposes where such information do not have any personal, sensitive or any such information and information which is not harmful to the security and critical information infrastructure of Bangladesh, all that information should be hosted in those countries where the Government of Bangladesh has multilateral or bilateral relations for unconditional and instantaneous laws can prevail."

C. China

China – Data Security Law: On June 10, the Data Security Law (DSL) was passed at the 29th session of the Standing Committee of the 13th National People's Congress (NPC). The Data Security Law will take effect on September 1, 2021. Additional coverage here: Bloomberg. The DSL:

- Continues application of the 2017 Cybersecurity Rules on exportation of data by critical information infrastructure operators;
- Requires the State Internet Information Department to draft rules for all "other data handlers" (i.e., not just CII operators) to restrict those other handlers' exportation of "important data";
- Applies to "[any person] handling important data";
- Requires the State to create a "categorical and hierarchical system for data protection" as well as "catalog of" for "important data"
- Requires that the authorities assess the "importance" of data based on the following criteria:
    - Economic development
    - Social development
    - National security
    - The public interest, or
    - Lawful rights and interests of citizens or organizations
- Authorizes each region and department to set a "catalog of important data" within that region and in corresponding industries and sectors
- Requires the State to create a "monitoring and early warning system" for important data, which will apparently help it prevent the exportation of "important data"

Following the swift enactment of the Data Security Law (DSL), the Cyberspace Administration of China will be developing subsidiary legislation for the DSL next. The Data Security Regulations has been identified as a work item under the State Council's 2021 Legislative Work Plan. Other sources: Covington, CPO Magazine, DLA Piper, Federalist, Hogan, IAPP, JD Supra, Lexology, Ruibai, SCMP, WSJ.

China – Law Countering Foreign Sanctions: On June 10, the National People's Congress approved the Law Countering Foreign Sanctions. The Law states that, "China has the right to take corresponding countermeasures" when another country "uses various pretexts or its own laws to contain or suppress China, take discriminatory restrictive measures against Chinese citizens and organizations, and interfere in China's internal affairs." Although the Law does not specifically reference data-related restrictions, it is within the scope of the broad authority granted under the Law to impose such measures. The language of this Law also echoes provisions in the draft Personal Information Law that do specifically envision the imposition of data transfer restrictions in response to corresponding measures taken by other countries. Additional coverage here: Reuters, Diplomat, WSJ, NPR.

China – Draft Personal Information Protection Law: On June 2, BSA submitted to the National People's Congress a multi-association letter effort regarding the draft Personal Information Protection Law (PIPL) and the draft Data Security Law (DSL). On behalf of BSA and the GDA, BSA staff gathered support from 32 global associations for this multi-industry letter. The letter underscored that data transfers support many important priorities, including international sales and marketing, transnational research and development, cybersecurity, fraud monitoring and prevention, anti-money laundering, anti-corruption, and a broad range of other activities relating to the protection of health, privacy, security, intellectual property, and regulatory compliance. The letter raised the following concerns:

(1) data localization requirements for "personal information" (PIPL Art. 40) and highly restrictive data transfer provisions for "important data" and "personal information" (DSL Art. 30, PIPL Arts. 38-40);
(2) lack of definition or overbroad scope for key concepts that implicate data localization requirements and data transfer restrictions, including what constitutes "important data," a "justified need," or a "large volume [of data]" (PIPL Art 40; DSL Art. 30);
(3) mandates for data assessments requiring governmental notification and/or approval in conjunction with the data localization and data transfer provisions noted above (PIPL Art. 38(1), 40; DSL Arts. 29, 30);
(4) proposed data transfer "standard contracts" that, while encouraging, may not be interoperable with standard contractual clauses under the EU General Data Protection Regulation (GDPR) or other established personal data protection frameworks (PIPL, Art. 38(3));
(5) the absence from the PIPL of other internationally recognized data transfer mechanisms, such as intra-corporate binding rules, trustmarks and regional certifications (PIPL, Art. 38); and
(6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established. (PIPL, Art. 39).

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

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

This recent sectoral implementation of these data localization measures illustrates increasing data transfer restrictiveness in China.

China – Automotive Data Management Rules; Connected Vehicle Data Security Requirements: On May 12, China issued data management rules for automotive applications. These measures illustrate how the cross-border data restrictive approaches of the DSL and PIPL can be specifically elaborated for particular sectors. Below is a comparison of all three sets of measures. See below for more details:

	Personal Information Protection Law (2nd Draft – April 2021)	Data Security Law (enacted May 2021)	Automotive Data Management Regs (ADMR) (1st Draft – May 2021) / Connected Vehicle Data Security Requirements (CVDSR) (Draft – May 2021)
Extraterritorial Application?	Yes	Yes	Yes
Scope of Covered Data?	"Personal info" is any information that can identify natural persons	"Important data" is any record of information deemed to be "important" from perspective of economic, social, national security, public interest, or private interests.	"Personal data" is any data about the owner, driver, driver, passenger, pedestrian, etc.; "Important data" includes data from official facilities, mapping data, data on vehicle flows/types on roads, and voice over video data, and other public interest data.
Do Safety/ Security/ Risk Assessments Require Official Notification/ Approval?	Sometimes. • Official approval of safety assessment required prior to any cross-border data transfers. (Art. 38). • Official approval of security assessment required for CII operators and large-scale personal data processors (Art. 40) • Personal information risk assessment records to be retained by processors for at least 3 years (Art. 54).	Yes. • Official notification/transmittal required for important data risk assessment reports	Yes. • State cyberspace department shall, in conjunction with other departments, conduct a data security assessment

Are Data Localization Mandates and/or Data Transfer Restrictions Imposed?	Yes. • Critical Information Infrastructure (CII) operators and large-scale personal data processors must store data in China, and may only transfer data with official approval (Art. 40) • Personal information processors may only transfer data overseas if they conduct an officially-organized safety assessment (or meet other conditions), and fulfill certain notification obligations. (Arts. 38, 41). • China can restrict data transfers to overseas individuals or organizations whose personal data processing activities China deems harmful to its interests (Art. 42). • China can also impose reciprocal data transfer restrictions vis-à-vis countries that restrict transfers to China (Art. 43).	Yes. • Critical Information Infrastructure (CII)operators must store personal data and important data in China. If strictly necessary, CII operators may seek an exception from this rule based on an official approval for such transfer following a data security assessment conducted by government authorities. (Art. 30). • All other data handlers must store "important data" in China, subject to official security management procedures for the export of data. (Art. 30).	Yes. • Operators (e.g., automotive OEMs, etc.) must store personal data and important data in China. If strictly necessary, the operator may seek an exception from this rule based on an official approval for such transfer following a cross-border transfer security assessment conducted by government authorities. (ADMR, Art. 12) • Operators are subject to strict legal obligations in connection with any transfer (supervising foreign data recipients; legal liability; data type, scope, use, and process limitations; governmental reporting requirements, etc.) (ADMR, Arts. 13-19) • Strict prohibition of any cross-border transfer of Data relating to roads, buildings, topography, traffic participants, among others, and the vehicle location and track data, collected by a connected vehicle from the environment outside the vehicles through cameras, radar and other sensors (CVSDR, Art. 7.1)

D. India

India-EU Connectivity Partnership: India and the European Union have announced the restart of EU-India trade negotiations and the launch of a EU-India Connectivity Partnership, whose stated aim is to build "transparent, inclusive, and rules-based connectivity between EU and India and with third countries and regions including Africa, Central Asia, Indo-Pacific." The Connectivity Partnership factsheet calls for "joint work on regulation and support for private investments in physical infrastructure across all sectors: digital, transport, energy, and people-to-people." It also describes forthcoming work on strong and secure connections submarine cables, satellite networks, 5G, cross-border payments, and warning services." Additional coverage here: Bloomberg, Reuters, Nikkei, FT.

India-UK FTA negotiations: The United Kingdom has launched a consultation regarding UK-India FTA negotiations. The Department for International Trade consultation seeks, "[w]ide input from consumers and businesses [to] ... craft a deal that includes closer cooperation in future-focused industries such as science, technology and services, creating high-value jobs across the country. Formal negotiations are expected to begin later this year." We welcome your views as to whether the GDA should participate. Consultation questionnaire here. Background note here.

E. Japan

Japan PPC Annual Report: On June 3, Japan's Personal Information Protection Commission (PPC) issued its 2021 annual report. The report highlights that PPC's ongoing discussions with DG Justice and with the US Department of Commerce on data transfer issues, as well as ongoing engagement on the OECD Privacy Guidelines, the OECD Trusted Government Access workstream, and efforts to promote the APEC CBPR system.

Japan Consolidation of Personal Data Protection Laws: On May 12, a bill was tabled in Japan's National Diet entitled, "Act for the Improvement of Related Laws for the Formation of a Digital Society". This amendment to the Act on the Protection of Personal Information would consolidate three laws related to personal data protection (the Act on the Protection of Personal Information, the Act on the Protection of Personal Information Held by Administrative Agencies and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies) and centralize jurisdiction under PPC, which has passed the Diet. The Government is aiming to achieve GDPR adequacy for academic and research sectors for personal data transferred from EU to Japan by applying requirements on security measures etc. to these sectors which had previously been excluded for use in academic studies. At this point, there are no indications that this consolidation would negatively impact cross-border data flows.

Japan – Implementation of the Amended Act on the Protection of Personal Information: On June 18, GDA filed comments to the Personal Information Protection Commission (PPC) on the Guidelines for the Amended Act on the Protection of Personal Information (APPI) enacted in June 2020. The draft Guidelines elaborates on the new requirement to enhance information to be provided to data subject for the purposes of cross-border data flows, and GDA requested PPC to release consolidated information on the personal information protection system in foreign countries, to avoid disparities in the information to be provided by various business operators, and to provide further clarity on the information regarding the existence of other systems that may have significant impact on the rights and interests of the data subject.

Japan's PPC had previously released the finalized Commission Rules (Japanese link) for the Act on the Protection of Personal Information (APPI) which was amended in 2020 and will come into full effect on April 1, 2022. GDA filed comments earlier seeking clarification on the new requirements added in the amended APPI, such as providing to data subject the name of the country to which the data will be provided for the transfer based on consent. PPC clarified that the "foreign country" refers to the country in which the third-party recipient is located, not the foreign country where the server on which the third-party recipient stores personal data is located. As for the requirement to periodically check the data protection measures of the third-party recipient for the cross-border transfer based on the establishment of a system conforming to standards prescribed by PPC rules, the required frequency to confirm the status and the type of reporting will further be elaborated in the upcoming Guidelines. We have prepared draft comments asking the PPC to release consolidated information on foreign countries' personal information protection systems, which would improve consistency in the application of Japan's cross-border data transfer framework. We have also asked the PPC to provide further clarity on the meaning of "other systems that may have significant impact on the rights and interests of the data subject."

Japan RCEP Ratification: On April 28, Japan's National Diet ratified the Regional Comprehensive Economic Partnership (RCEP). Singapore and China have already completed their ratification processes. (JP / ENG). RCEP groups the 10 ASEAN members -- Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam -- plus Japan, China, South Korea, Australia and New Zealand. RCEP is expected to boost Japan's GDP by 2.7 percent and create 570,000 jobs. In relation to data transfers, RCEP falls short of other international agreements, as reflected in its: (1) limitation of data transfers/localization obligations to "positive list" commitments in services chapter, (2) subjectification of the "necessity" test, (3) subjective and non-justiciable "national security" exception, and (4) non-application of binding dispute settlement) fall significantly below international best practices and all prior agreements.

F. Korea (Republic of Korea)

Korea Adequacy: The European Commission announced on June 17 that it reached an agreement with South Korea negotiators on the draft data adequacy agreement for transfers of personal data to the Republic of Korea under the EU's General Data Protection Regulation. Korea's Personal Information Protection Commission (PIPC) also issued a statement available here. The formal approval involves 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 (in a comitology procedure). Once this procedure is completed, the Commission will adopt the adequacy decision. The whole process is expected to take several weeks. This follows a March 30 agreement on the data adequacy agreement for transfers of personal data to Korea (joint statement). Based on recent statements by EU Justice Commissioner Didier Reynders, the draft decision should not contain the same sunset clause as the UK draft decisions requiring an affirmative re-approval, but should rather require a regular assessment every four years as per the GDPR. Other sources: IAPP, K&L, NLR.

Korea-US Free Trade Agreement: The Korea-United States (KORUS) FTA financial services committee meeting was held on June 2, 2021, and reportedly covered, among other things, data localization and data transfer restrictions administered by the Korea Financial Services Commission. Although foreign reinsurers should be permitted to transfer data to related entities in other countries, other restrictions on the use of cross-border cloud services in the financial services sector will remain in place for the present time. *See also* the GDA's recent submission on Korea's Partial Amendments to the Personal Information Protection Act.

G. Malaysia

Malaysia Digital Economy Blueprint: Malaysia released its Digital Economy Blueprint. A pillar of that Blueprint is to "strengthen cross-border data transfer mechanisms and protection to facilitate seamless data flows." Malaysia outlines a vision to "ensure cross-border data flows for commerce are seamless, safe and secure," with a view to enhanc[ing] cross-border data transfer mechanisms in both PDPA and international trade policies, and to "streamlin[ing] mechanisms related to data usage, storage and transfers."

H. Singapore

Singapore Digital Economy Agreements: The GDA submitted comments in response to Singapore IMDA's solicitation of views on digital economy agreements. The GDA noted that Digital Economy Agreements (DEAs) benefit both Singapore and its trading partners as cross-border data transfers are critical in the workplace, in health, in innovation and in international trade. As reflected in the GDA's Dashboard of Trade Rules on Data Transfers and the GDA Cross-Border Data Policy Principles DEA data transfer rules should:

- 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 transfer restrictions greater than necessary;
- Not discriminate against foreign service providers by treating cross-border data transfers less favorably than domestic data transfers;
- Apply across all sectors, including financial services;

- Be developed and maintained in accordance with good regulatory practices;
- Be aligned with accountability models consistent with international best practices; and
- Help foster the development of trust-based frameworks that are interoperable and support the seamless and responsible movement of information across borders.

These core features of data transfer frameworks enjoy broad support from industries around the world.

I. Taiwan

Taiwan – Relaunch of US-Taiwan TIFA Negotiations: After a long hiatus, the United States and Taiwan have announced the restart of bilateral Trade and Investment Framework Negotiations on June 30.

J. Thailand

Thailand Personal Data Protection Act: The Thai cabinet has approved the postponement of the full enforcement of the Personal Data Protection Act (PDPA) slated for June 2021 to May 31, 2022. Besides the need to manage the ongoing pandemic in Thailand, another key reason cited for the postponement was due to the fact that several key procedures linked to the PDPA have yet to be completed, including the appointment of the 16-member Personal Data Protection Committee. Work on the subsidiary legislation for the PDPA has also reached an impasse as it will require the approval of this yet to be appointed Committee. The Ministry of Digital Economy and Society also plans to hold a focus group discussion in mid-June with industry stakeholders on the implementation of the PDPA.

K. Vietnam

Vietnam Regulatory Review Submission: BSA and the GDA contributed inputs into Vietnam's ongoing regulatory review process, highlighting concerns previously raised in the GDA's comments regarding cross-border data transfers and data localization mandates in Vietnam's personal data protection implementing decree. Vietnam's draft Decree on Personal Data Protection sets four preconditions that must be fulfilled prior to a cross-border data transfer out of Vietnam: data subject consent; storage of original data in Vietnam; proof that the country to which data is being transferred offers an equivalent or higher level of data protection; and written approval from the Vietnam Personal Data Protection Commission. The Ministry of Public Security is reportedly aiming to have the Decree become effective on 31 December 2021.

IV. Americas

A. Brazil

Brazil – ANPD Candidate List: The Brazilian Data Protection Authority (ANPD) announced a shortlist of 122 candidates to join the National Data Protection Council. This consultative body will be tasked with providing input on the ANPD board's decision. The nominees were put forward by research centers, business associations, unions, and other civil society organizations. There are 13 seats available in total, split into 5 categories of representation. On May 5, the ANPD selected three nominees per category and dispatched them to President Jair Bolsonaro who is yet to make the final appointment decision

B. Canada

Canada – OPC Report on Digital Charter Implementation Act (Bill C-11): Canada's Office of the Privacy Commissioner has issued 60 recommendations to ensure that Bill C-11 enhances privacy protections for Canadians. The OPC also issued a separate report on Bill C-11's Treatment of Cross-Border Transfers of Personal Information. The Report itself posits that cross-border data transfers present "inherent risks for privacy, different from the risks associated with domestic transfers of information." The report contains 14 recommendations relating to trans-border data flows. Selected recommendations follow:

- Recommendation 10: Organizations should be required to provide specific notice of any risks regarding access to personal data by the authorities of the service provider's country.
- Recommendation 11: Bill C-11 should include a provision that requires organizations to assess whether a contract with a service provider will maintain substantially the same protection as afforded by the CPPA, taking into account the legal data protection regime in place in the country of a service provider that will be collecting, using or disclosing personal data on their behalf.
- Recommendation 12: The Commissioner may request an organization to demonstrate the effectiveness of any safeguards put in place to govern data transfers; The Commissioner be specifically empowered to prohibit, suspend, or place conditions on, offshore transfers of data where substantially similar protection is not in place.

Canada – Quebec Bill No. 64: Following our engagement on the data transfer provisions of Bill No. 64, we received a response from Minister Caire, Quebec's Minister responsible for government digital transformation, addressing the data transfer concerns raised in a GDA submission, and identifying responsive legislative amendments introduced into the legislation. The legislative amendments track those that we previously identified to GDA members (email of March 29 @ 5:29 pm EDT).

C. Mexico

Mexico – USMCA Free Trade Commission Meeting: Mexico hosted the inaugural Free Commission Meeting of the United States-Mexico-Canada Agreement (USMCA) on May 17-18, marking the first trilateral meeting among Mexican Secretary of Economy Tatiana Clouthier, US Trade Representative Katherine Tai and Canadian Minister of Small Business, Export Promotion and International Trade Mary Ng.

D. Ecuador

Ecuador – Data Protection Law: The Personal Data Protection Law of Ecuador has been published in the official register. This follows the Bill's approval by the National Assembly and assent from the President. The Bill, which contains elements based on GDPR, stipulates that cross-border data transfers will be allowed to other countries that guarantee an adequate level of protection, which the DPA will stipulate in a list. Even if the DPA determines that a country's level of protection is not adequate, cross-border data transfer safeguards may be relied upon for data transfer purposes.

E. Paraguay

Paraguay - Proposed Law on the Protection of Personal Data: Proposed legislation on personal data protection has been introduced into the Paraguayan Congress. Bill text can be accessed here.

F. Peru

Peru - Bill Creating the National Authority for the Protection of Personal Data: The Peruvian government introduced into the Peruvian Congress a bill that would address a range of data protection issues. The bill text can be accessed here.

G. United States

United States – Deputy USTR Confirmation Hearings: On June 24, the Senate Finance Committee held confirmation hearings for Sarah Bianchi (nominee for Deputy USTR for Asia, Africa, Investment, Services, Textiles, and Industrial Competitiveness), and Jayme White (nominee for Deputy USTR for Western Hemisphere, Europe, the Middle East, Labor, and Environment). There was a heavy focus in the hearing on China-related trade and on cross-border data policy. Noting that cross-border digital services exports measured $876 billion, Sen. Wyden and other lawmakers posed questions about digital authoritarianism, data localization mandates, and data transfer restrictions. In response, Ms. Bianchi underscored the importance of "working with allies… on digital trade," while underscoring a greater focus on supply chain security and expedited mechanisms to resolving trade disputes. Asked about trade agreement provisions on data transfers and data localization, Ms. Bianchi stated that the USMCA and the US-Japan digital trade agreement "provide a good model" on cross-border data policy, and also stated that "we should and we can" expand digital trade with Asia-Pacific allies. Statements by Bianchi, White, and Sen. Wyden here. Transcript here.

United States – Forthcoming Solicitation of Comments on Supply Chain Executive Order: On June 24, Deputy Assistant Commerce Secretary for Manufacturing Monica Gorman announced that agencies leading the one-year reports mandated under the White House Supply Chain Executive Order will fairly soon issue requests for stakeholder input. One of the mandated reports relates to the "industrial base for the development of ICT software, data, and associated services."

US-EU Trade and Technology Council: On June 15, the United States and the European Union announced the launch of a US-EU Trade and Technology Council (TTC) having the "aim of promoting a democratic model of digital governance." The EU-US Summit Statement describes the TTC as addressing priorities including cross-border data transfers, data governance, technology standards, ICT security, export and investment screening, and other issues. On cross-border data transfers, the Summit Statement declares as follows:

> We commit to work together to ensure safe, secure, and trusted cross-border data flows that protect consumers and enhance privacy protections, while enabling Transatlantic commerce. To this end, we plan to continue to work together to strengthen legal certainty in Transatlantic flows of personal data. We also commit to continue cooperation on consumer protection and access to electronic evidence in criminal matters.

On the US side, the negotiations will reportedly be led by USTR and the Departments of Commerce and State.

United States – Executive Order on Sensitive Data in Software Apps Associated with Foreign Adversaries: On June 9, 2021, the President signed an Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries ("App Data EO"), which builds on Executive Order 13873 (2019) ("ICTS Supply Chain Transactions EO") to evaluate whether transactions involving certain foreign software apps threaten American data. Fact Sheet here. Other media: NYTimes, WSJ, WaPo. The App Data EO lays out several new factors to consider in evaluating App Data risks, including:

1. the scope/sensitivity of data collected;
2. number/sensitivity of users;

3. indicia of control, coercion, or cooption by persons associated with: (a) a foreign adversary or (b) malicious cyber activities;
4. use of the app to conduct surveillance, such as through access to sensitive or confidential government or business information, or sensitive personal data; and
5. ability to undertake thorough and reliable third-party auditing of the app or address risks by independently verifiable measures.

The App Data EO directs:

1. The Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) to provide a vulnerability assessment to Commerce by Aug. 8, 2021;
2. Commerce to provide the White House with a report by Oct. 7, 2021 containing recommendations to "protect against harm from the unrestricted sale of, transfer of, or access to United States persons' sensitive data, including personally identifiable information, personal health information, and genetic information, and harm from access to large data repositories by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary";
3. Commerce to provide the White House with additional recommended executive and legislative actions to address these risks by Dec. 6, 2021;
4. Commerce to continually evaluate software app transactions that pose an undue risk of sabotage, subversion, catastrophic effects, or otherwise unacceptable risk to US national security or safety of US persons.

United States – Executive Order on Cybersecurity: On May 12, the White House has issued a cybersecurity executive order, which includes a section requiring companies providing services to the Federal Government to share cybersecurity threat information, which could potentially include threat information collected across borders or in other jurisdictions. Among other things, this section directs the Office of Management and Budget and others to review and eventually standardize contract language for IT and OT, ICT service providers report to the Federal Government when they discover an incident. Additional coverage here: NYTimes, WaPo, NextGov, DefenseOne.

United States – USTR Tai Testimony to Congress: On May 12-13, USTR Ambassador Katherine Tai testified before the Senate Finance Committee (SFC) and the House Ways and Means Committee (HWM) in relation to the President's 2021 Trade Policy Agenda. Amb. Tai did not address cross-border data policy issues in her opening statements to the Senate or House, but the opening statement of Senator Wyden and the statement of Senator Crapo addressed digital trade barriers and cross-border data barriers. Asked about the Administration's position on digital trade, Amb. Tai acknowledged the importance of engaging on "the economy we have right now and … shaping the economy that we have into the future," while also noting USTR's interest in worker-centered digital trade policies. Questions also arose regarding TPP following a bipartisan letter by Sens. Carper, Cornyn and others urging USTR to reconsider TPP participation. SFC link here and HWM link here.

United States – Annual Special 301 Report: On April 30, USTR published its 2021 Special 301 Report. In response to this year's solicitation, the GDA filed a Special 301 submission in February 2021. BSA issued a press statement underscoring the importance of greater US government focus on data localization mandates and unnecessary data transfer restrictions as innovation barriers.

United States – Quadrennial National Intelligence Council Report: The 2021 Report warns technology-related competition poses "potentially cascading risks and implications for economic, military, and societal security." The NIC Report predicts that, [c]ontrol of key sites of exchange, including telecommunications, finance, data flows, and manufacturing supply chains, will give countries and corporations the ability to gain valuable information, deny access to rivals, and even coerce behavior."

United States – NTIA / World Telecommunications Development Conference: On June 7, the GDA submitted comments in response to a solicitation by the National Telecommunications and Information Administration (NTIA) development and policy objectives for global connectivity – focusing on the UN Sustainable Development Goals and the World Telecommunications Development Conference in November 2021. GDA's comments provided evidence to demonstrate how data transfers and digital connectivity help support the UN SDGs. *See also* GDA primer, *Cross-border Data Transfers & Economic Development: Access to Global Markets, Innovation, Finance, Food, and Healthcare*.

United States Congress – Selected Legislation (April – June 2021)

US Innovation and Competition Act (USICA): On June 8, the US Senate has passed the US Innovation and Competition Act (USICA). USICA contains provisions that would renew and extend the GSP Program and include digital trade provisions requiring USTR to evaluate the extent to which a beneficiary developing country: "(A) has refrained from imposing, or has eliminated, digital trade barriers, including unnecessary or discriminatory data localization or data transfer restrictions; and (B) has taken steps in the digital environment to support consumer protections, the privacy of personal information, and open digital ecosystems." USICA would also require USTR to "consider the viability and utility of negotiating digital trade agreements with like-minded countries and to what degree such agreements may provide an opportunity to address digital barriers, deter censorship, promote the free flow of information, support privacy, protect sensitive information, protect communications regarding human and worker rights, and promote digitally enabled commerce." BSA issued a supportive statement. Other media: The Hill, Politico, InsideTrade.

Digital Trade for Development Act: Representative Lahood has introduced the Digital Trade for Development Act, a legislative proposal that would allow the Office of the US Trade Representative to consider whether a beneficiary developing country (BDC) under the Generalized System of Preferences (GSP) had refrained from imposing, or had eliminated, data localization mandates, cross-border data transfer restrictions, or other digital trade barriers. Bill text here. Press statement here. BSA backgrounder here. Other media: Inside Trade.

Trade Preferences and American Manufacturing Competitiveness Act of 2021: On June 22, House Ways and Means (HWM) Republican lawmakers introduced the Trade Preferences and American Manufacturing Competitiveness Act of 2021. This bill includes both the bipartisan Senate bill's GSP provisions on labor, gender, human rights, and environment, and the bipartisan Senate bill's provisions on cross-border data transfers, data localization and support for privacy of personal information, and consumer protections online. This bill closely resembles the eponymous Senate bill, the Trade Preferences and American Manufacturing Competitiveness Act of 2021.

Generalized System of Preferences and Miscellaneous Tariff Bill Modernization Act of 2021: On June 17, HWM Democratic lawmakers introduced the Generalized System of Preferences and Miscellaneous Tariff Bill Modernization Act of 2021.That bill contains provisions the bipartisan Senate GSP bill on labor, gender, human rights and environmental issues, but omits provisions from the bipartisan Senate bill that would authorize USTR to evaluate a beneficiary developing country's digital trade policies and its support for privacy of personal information and consumer protections online.

Protecting Americans' Data from Foreign Surveillance Act: Senator Ron Wyden introduced a bill entitled, "'Protecting Americans' Data From Foreign Surveillance Act of 2021," which would establish a government process to: (a) identify and publish categories of personal data that could be exploited by foreign governments; and (b) identify upper thresholds for the transfer of such personal data outside of the United States. The bill would establish new licensing requirements under the Export Administration Regulations for the export, reexport, or in-country transfer of such data above the identified thresholds. (Press statement and bill text here).

Strategic Competition Act. There are several pending bills that include provisions that touch on data transfer matters. These include the "Strategic Competition Act," which would authorize the Department of State to establish the ''Digital Connectivity and Cybersecurity Partnership'' to help countries: (1) increase secure Internet access and digital infrastructure in emerging markets; (2) protect technological assets, including data; (3) adopt policies and regulatory positions that foster and encourage open, interoperable, reliable, and secure internet, the free flow of data, multi-stakeholder models of internet governance, and procompetitive and security information communications technology policies and regulations; among other objectives. The Act also encourages USTR to negotiate bilateral and plurilateral agreements relating to digital goods with the European Union, Japan, Taiwan, the member countries of the Five Eyes intelligence-sharing alliance, and other nations, as appropriate."

V. International Organizations

A. G7

G7 – On June 13, the G7 Leaders issued a Summit Communiqué that included a commitment to champion data free flow with trust. This is a welcome development given the increasing urgency for like-minded economies with a shared respect for transparent and accountable governance to find common ground on cross-border data transfers. The Communiqué contains an endorsement of the G7 Digital Ministers' Roadmap for Cooperation on Data Free Flow with Trust, which recognizes that:

1. The "ability to move and protect data across borders is essential for economic growth and innovation";
2. Countries should "enhance cooperation on data governance and data protection, identify opportunities to overcome differences, explore commonalities in regulatory approaches, and promote interoperability";
3. The OECD's work on *trusted government access to personal data held by the private sector* can help clarify the relationship between data protection, privacy, and lawful access regimes, and the valid need for governments to access personal data in the private sector; and

4. There is an interest in greater cross-border sharing of data among governments in priority sectors.

The GDA issued a supportive press statement and has consulted with both the US and UK governments regarding opportunities for GDA to support the DFFT Roadmap. The Summit State follows a G7 Digital and Technology Ministerial Declaration, which describes the DFFT Roadmap as a "plan for delivering tangible progress on [the DFFT]… agenda, building confidence for businesses and individuals to use technology, as well as driving economic and social value."

B. OECD

OECD – The OECD Trusted Government Access workstream seeks to identify common principles around government access to data held by the private sector. BSA staff has been supporting the OECD's Committee on Digital Economy Policy ("CDEP"), which is advancing a workstream on trusted government access to data. CDEP issued a Dec. 2020 statement identifying seven potential safeguards around trusted government access to data. They are:

- The legal bases upon which governments may compel access to personal data;
- Requirements that access meet legitimate aims and be carried out in a necessary and proportionate manner; Transparency;
- Approvals for and constraints placed on government access;
- Limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards;
- Independent oversight; and
- Effective redress.

The drafting group is to consult with other relevant OECD committees, stakeholders, and then submit the text to the Council. It is possible that the text could be approved by the Council by the end of 2021.

C. World Bank

World Bank – The World Bank has published the World Development Report 2021 – Data For Better Lives. The Global Data Alliance filed a submission last year in response to the World Bank's solicitation of comments. In addition to the **main report** itself, the World Bank offers discrete resource pages regarding the deployment of data for purposes of economic development, including pages on: (1) Statistical evidence and data and analysis; (2) Country case studies; (3) Background research; and (4) Cross-border data transfers. The World Bank also published reports relating to cross-border data transfer issues. These include the following:

- Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation. This paper, jointly published by the WDR 2021 team and the World Bank's International Trade Unit (ETIRI), analyzes costs associated with cross-border data transfer restrictions (among other aspects of privacy frameworks) for companies of various sizes and sectoral profiles, as well as for the governmental authorities that administer these frameworks. The paper analyzes GDPR, US privacy rules (HIPAA, GLBA, COPPA, state rules), and Chinese cross-border data transfer restrictions (including the App Rules, Cybersecurity Law, 2018 Specification, 2020 Specification, 2020 Personal Finance Information Protection Technical Specification, Data Security Law, etc.). See id., pp. 6-9. The report concludes with several "Lessons for Data Privacy in Developing Countries," including the following: (1) Ensuring clear rules; (2) Recognize the cost of data localization; (3) Strive for interoperability; (4) Consider burdens on small enterprises; and (5) Establish a model that is conducive to cross-border data transfers.

- Regulating Personal Data: Data Models and Digital Services Trade. This paper analyzes the development impacts of fragmentating data transfer rules in different countries on the basis of three different regulatory models – open (39 countries), conditional (40 countries), and limited (11 countries). The paper highlights different metrics demonstrating that limited data transfer rules correlate with lagging economic development indicators.

D. World Economic Forum

World Economic Forum – WEF held its first Global Technology Governance Summit in collaboration with the Centre for the Fourth Industrial Revolution (C4IR) Network. In connection with the summit, WEF published several White Papers, including:

- Advancing Data Flow Governance in the Indo-Pacific: Four Country Analyses and Dialogues. This paper describes the environment for data transfers in India, Thailand, the Philippines, and Vietnam. It contains citations to legal authorities governing data transfers in each case, as well as evidence on the benefits that each of those economies derive from data transfers. The authors also published a blog entitled, 5 Ways to Ensure Trust When Moving Data Across Borders.

- Data Driven Economies – Foundations for Our Common Future. This paper covers various of data governance topics, emphasizing "[m]ore coordinated and harmonized approaches to data governance policy and cross-border data flows [t]o … help enable responsible and ethical global interoperability. …When the next pandemic arrives, governments and industry need to react swiftly and effectively, starting with sharing information without hesitation or friction."

- Rebuilding Trust and Governance: Towards Data Free Flow with Trust. This paper proposes a trust-based governance framework, on the grounds that, "without trust, information stops flowing, and innovation falters. Some believe the best way to protect people and societies from the potential harms of digital technology is to build barriers to the flow of data. We do not think that is feasible or desirable..[T]he better option is to make data flows safer, more transparent and more trustworthy. This is the premise of the Japanese Government's Data Free Flow with Trust (DFFT) initiative, which seeks to promote safe, reliable cross-border data sharing, and the Trust Governance Framework in this paper."

E. World Trade Organization

World Trade Organization – The WTO announced that its annual Public Forum will take place from September 28-30, 2021. The 2021 theme is "Trade beyond COVID-19: Building Resilience".

WTO Joint Statement Initiative on E-Commerce: On June 24, the WTO ambassadors for Australia, Japan, and Singapore (the co-convenors the JSI E-Commerce negotiations) spoke at the Global Services Summit on cross-border data negotiations in the JSI talks. The following observations were made:

- Cross-border data transfers and data localization are among the most challenging negotiation topics;
- Some WTO Members contend that cross-border data policy should excluded from the talks;
- Other Members (e.g., EU, US, CPTPP Parties) agree that certain data localization or data transfer issues should be addressed, but do not agree on how to do so;
- Some Members have moved quickly to establish strict data transfer restrictions and data localization mandates in domestic law, complicating the prospects for WTO negotiating outcomes;
- Agreement on data transfer negotiating positions among the US, EU, Japan, and other advanced economies would be highly beneficial.

WTO 12th Ministerial Conference: On June 23, WTO Director General Ngozi Okonjo-Iweala spoke at the Global Services Summit about the prospects for the 12th Ministerial Conference, scheduled for late November 2021. The Director General observed that the WTO Moratorium on Customs Duties on Electronic Transmissions will be up for renewal at that time. Australia, the EU, Japan, Singapore, and the United States (among others) favor a permanent renewal of the Moratorium. Countries including India and South Africa have raised concerns about a renewal of the Moratorium. This WTO Moratorium is relevant to the GDA's work, as its end could prompt some countries to attempt to impose customs duties or related border restrictions on cross-border data transfers. BSA has consistently advocated for renewal of the WTO Moratorium and has raised concerns about the imposition of customs restrictions on cross-border data transfers, as summarized below. *See e.g.*, BSA's Indonesia GSP submission and BSA backgrounder for WTO members. *See also* ECIPE and OECD studies on the subject.

RECENT WORK PRODUCT

From April – June 2021,the GDA submitted comments or issued other publications on the following:

UK Electronic Communications (Security Measures) Regulations 2021: On June 10, the GDA submitted comments expressing concerns with the Security Measures' data localization elements.

EU-US Privacy Shield: On June 9, the GDA and BSA submitted a letter to President Ursula von der Leyen and President Biden in relation to an enhanced Privacy Shield agreement.

World Telecommunications Development Conference: On June 7, the GDA submitted comments to the National Telecommunications and Information Administration (NTIA) in response to NTIA's solicitation of comments in the Federal Register, Connecting the Unconnected Worldwide in Light of the ITU's WTDC-21.

China Draft Personal Information Protection Law and Data Security Law: On June 2, the GDA filed a multi-association letter regarding the draft Personal Information Protection Law and the draft Data Security Law. BSA staff led this multi-association process, gathering support from 32 associations across sectors including the advanced manufacturing, automotive, electronics, financial services, insurance, health, pharmaceutical, and telecommunications sectors.

Singapore Digital Economy Agreements: On May 24, the GDA filed comments on Singapore's digital economy agreement program.

Bangladesh National Cloud Policy Submission: On May 12, the GDA filed comments on cross-border data restrictions in Bangladesh's National Cloud Policy.

Canada's Accession to Digital Economy Partnership Agreement: On May 3, the GDA filed comments regarding Canada's prospective accession to the Digital Economy Partnership Agreement.

South Africa National Data and Cloud Policy: On May 12, the GDA filed comments on cross-border data restrictions in the proposed South Africa National Data and Cloud Policy.

Vietnam Regulatory Review: BSA and the GDA contributed inputs into Vietnam's ongoing regulatory review process, highlighting concerns previously raised in the GDA's comments regarding cross-border data transfers and data localization mandates in Vietnam's personal data protection implementing decree.

OECD Trusted Government Access Workstream: The GDA helped lead drafting of a multi-industry statement supporting OECD's work on shared principles for government access to data. The statement also highlights concerns about the economic and commercial impact of disruptions to cross-border data flows stemming from a lack of clarity, transparency, and consistency around these issues.

Cross-Border Data Transfers & Innovation: GDA's primer on Data Transfers & Innovation highlights that countries can foster innovation with the right mix of policy tools, including cross-border access to technology; the ability to share knowledge, ideas, and information across international IT networks; and improved digital connectivity and inclusiveness.

Cross-Border Data Transfers & Economic Development: GDA's primer on Data Transfers & Economic Development focuses on the role of cross-border data transfers and digital connectivity in ensuring access to global markets, innovation, finance, food, and healthcare in emerging economies.

MEDIA AND OTHER PUBLICATIONS

Below is a curated list of third party publications relevant to cross-border data policy:

Asia Pacific Privacy Authorities, 55th APPA Forum Communiqué
ALLEA, et al., International Sharing of Personal Health Data for Research
Analysis Group, The Importance of Cross-Border Data Flows: An Economic Analysis of Restrictions on Extra-EU Data Transfers
Asian Development Bank, Digital Connectivity and Low Earth Orbit Satellite Constellations: Opportunities for Asia and the Pacific
Atlantic Council, How to leverage the Quad to counter China's Digital Sinosphere
Atlantic Council Blog, Do Continued EU Data Flows to the United Kingdom Offer Hope for the United States?
Axios, Businesses fall into transatlantic privacy hole
Baker McKenzie, Why the Biden administration should 'go big' on global data transfers solution
Barron's, How Nations Can Build Online Trust Through Trade
Bitkom et al., German Multi-Association Paper on Privacy Shield and Third Country Data Transfers
Borderlex, WTO e-commerce: Nigeria brings developing country exceptions for data flows into picture
Brookings Institution, US and EU tech strategy aren't as aligned as you think
Brookings Institution, Digital Trade Deal Ripe for the Indo-Pacific
Brookings Institute, Bridging the global digital divide: A platform to advance digital development in low- and middle- income countries
Cambridge University, The UK and the EU Personal Data Framework After Brexit: Another Switzerland?
Center for Economic Policy Research, Addressing Impediments to Digital Trade
Center for Global Development, Why Digitalization and Digital Governance Are Key to Regional Integration in Africa
Clinical OMICs, International Data Sharing Project Aims to Improve Rare Disease Diagnostics
CNIL, CNIL calls for changes in the use of US collaborative tools by French universities
Competitive Enterprise Institute, The UK Should Beware of Future Restrictions against UK-EU Data Flows
Confederation of Swedish Enterprise, Data transfer urge certainty
Court of Justice for the European Union, Annual Report
Covington, German Supervisory Authorities Probe Data Transfers
Covington, European Commission Publishes New Standard Contractual Clauses
Covington, Final Countdown to South Africa POPIA Compliance: Five Critical Steps to Take Before July 1st, 2021
Covington, China Sector-Specific Data Rules – Data Protection in the E-Commerce
Covington, China Sector-Specific Data Rules – Data Protection in the Financial Sector
CSIS, Governing Data in the Asia Pacific
CSIS, Advancing Data Governance in the G7
DigiChina, History Behind China's Personal Information Protection Law
DigiChina, With Auto Data, China Buckles In for Security and Opens Up for Future Tech
DigiChina, Translation: Several Provisions on the Management of Automobile Data Security (Draft for Comment)
DigiChina, China's Draft Privacy Law Adds Platform Self-Governance, Solidifies CAC's Role
DigiChina, Translation: Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft)
DigiChina, The Future of Taiwan in U.S.-China Technology Competition
Digital Europe, The importance of international data flows in the European financial ecosystem
DigitalEurope, Making the most of the GDPR to advance health research
DigitalEurope, EU-UK data transfers - a legal analysis supporting a swift adequacy decision
DigitalEurope, Data transfers and effectiveness of supplementary measures

East Asia Forum, Global digital governance can start in Asia
East Asia Forum, Avoiding a fractured digital global economy
East Asia Forum, Managing digital trade in Asia
Emerging Europe, Brexit and fintech: Little disruption so far, but data regulation needs urgent attention
EURACTIV, Connectivity is the starting point for the 2030 digital targets
EURACTIV, Health experts call for the GDPR revision for cross-border health data sharing
EURACTIV, China's third way on data governance
EURACTIV, Opinion: EU-US in collision course on privacy
EURACTIV, Opinion: Why the impasse on data flows threatens Europe's digital recovery
EURACTIV, Report: Europe may lose €2 trillion in 10 years if uncertainty over data transfers continues
EURACTIV, The untapped potential of data-driven healthcare
EURACTIV, Unleashing the power of data
Eurasia Review, Positive Tech Solutions Will Force The Recovery: Global Technology Governance Summit Concludes
European Council on Foreign Relations, Network effects: Europe's digital sovereignty in the Mediterranean
European Data Protection Board, Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the Lithuanian Supervisory Authority, under Article 28(8) GDPR
European Data Protection Board, Statement 04/2021 on International Agreements Including Transfers
European Data Protection Board, Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom
European Data Protection Supervisor, 2020 Annual Report
European Data Protection Supervisor, Caselaw Digest – Transfers of Personal Data to Third Countries
European Interest, Data Protection: MEPs call for clear guidelines on data transfers with the US
European Parliament Thinktank, EU-UK Trade and Cooperation Agreement: An analytical overview
European Parliamentary Research Service, EU-UK Private Sector Data Flows After BREXIT
European Parliament press statement, Data Protection: 541 MEPs call for clear guidelines on transfer of data to the US
European Voices on Surveillance, US and European Surveillance Law Regimes: Time to Adjust the Contrast?
Finextra, Open data will catalyse the UK's progress to net-zero
Foreign Affairs Magazine, Data Is Power
France CNIL, Guidance on Third Country Data Transfers
France CNIL, Comments on Standard Contractual Clauses
Frontier Economics, The Value of Cross-Border Data Flows to Europe: Risks and Opportunities
Future of Privacy Forum, Understanding Digital Data Flows
Future of Privacy Forum, South Korean Personal Information Protection Commission (PIPC) sanctions AI technology company for indiscriminate personal information processing
George Washington University, Digital Trade and Data Governance Hub Overview
German Saarland DPA, Steps to Implement Schrems II Decision in Relation to Third Country Data Transfers
German Hesse DPA, Steps to Implement Schrems II Decision in Relation to Third Country Data Transfers
German Association for Data Protection and Data Security, 10 Truths About GDPR Pseudonymization
GSMA, Accelerating mobile internet adoption: Policy considerations to bridge the digital divide in low- and middle-income countries
Hamburg DPA, Questionnaire to Assess Compliance with Schrems II of Data Transfers Practice
Hinrich Foundation, The Conventional Wisdom on China and the TPP is Wrong
Hinrich Foundation, Data governance and trade: The Asia-Pacific leads the way
IAPP, Enabling global transfers of epidemiological data
IAPP, Privacy Guide for Latin America
IAPP, Demystifying data transfers to US data importers: Looking at 'Schrems II' from a different angle
IAPP, Summary Table of Article 49 Derogations with Examples
IAPP, Top-10 do's and don'ts for service providers implementing the new SCCs with EU customers
IAPP, EU-US data transfer deal still work in progress
IAPP, 'Schrems II' DPA investigations and enforcement
IAPP, Getting acclimated with updated SCCs
IAPP, Keys to implementing the new SCCs
Internet Jurisdiction Policy Network, Cross-Border Data Toolkits: Access to Electronic Evidence; Content Moderation
Irish High Court, Judgment in Facebook v. DPC and Schrems
IT Pro Portal, Bridging cross border data sharing post-Brexit with simulated data
JD Supra, 11 Months After Schrems II – How Are Organizations Addressing Risk?
JD Supra, Navigating EU Data Transfers: Effects of Schrems II Start to Bite
JD Supra, The Proverbial Other Foot: Proposed U.S. Legislation Could Ban Personal Data Transfers to Ireland and Other U.S. Allies
JD Supra, GDPR and Data Transfers 2.0 – Navigating Through Post-Schrems II Waters
JD Supra, German Data Protection Authorities Want To Know What Companies Are Doing With Customer Data
JD Supra, GDPR and Data Transfers 2.0 – Navigating Through Post-Schrems II Waters
Lexology, High Court rejects procedural challenge against DPC's inquiry into EU-US data transfers

Lexology, Best Practices in Global Data Privacy
Lexology, Newly Approved GDPR Code of Conduct for SaaS and Cloud Service Providers
Lexology, The United Kingdom's road to adequacy: will personal data from the EEA be freely transferrable to the United Kingdom following Brexit?
Lexology, The new draft Standard Contractual Clauses – legal certainty for data transfers?
Lexology, Data transfers – will Asia lead the way?
Lexology, German Data Protection Authority Decides on Supplementary Measures for International Data Transfers
Lexology, Russia amends data protection law to increase personal data subjects' rights
Lexology, New standard contractual clauses catch-up to the ever evolving global data transfer landscape?
Lexology, A New Era for International Data Transfers: European Commission Adopts New Standard Contractual Clauses
Lexology, BCLP Global Data Privacy FAQs: What EU transfer options remain for international data transfers after Schrems II?
Lexology, UK data protection standards to be deemed adequate by the EU
Lexology, New standard contractual clauses catch-up to the ever-evolving global data transfer landscape?
Lexology, A New Era for Data Transfers: European Commission Adopts New Standard Contractual Clauses
Lexology, What EU transfer options remain for international data transfers after Schrems II?
Lowy Institute for International Policy, Is Southeast Asia ready for a US-China tech decoupling?
MLEX, Data localization accelerates globally as privacy is linked with data transfer restrictions
National Law Review, Transfers of Health Data from the European Union to the United States in a Post-Schrems II World
National Law Review, Portuguese DPA Orders Suspension of U.S. Data Transfers by Agency That Relied on SCCs
National Law Review, Data Protection After Brexit: How will GDPR and UK GDPR Affect U.S. Businesses?
National Law Review, EU Data Protection Regulators Adopt Guidance on Personal Data Transfers
New Statesman, In digital trade, the UK is becoming more like the US than the EU
NYU J. Int'l L & Pol., The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance
Observer Research Foundation, Sovereignty in a 'datafied' world: A framework for Indian diplomacy
Observer Research Foundation, A digital agenda for India's G20 presidency
Open Access Government, The ongoing data disruption of Brexit
OECD, Digital Trade Inventory: Rules, Standards, and Principles
OECD, Trade Finance for SMEs in the Digital Era
OECD, Trade & Gender: A Framework of Analysis
OECD, What future for science, technology and innovation after COVID-19?
Pearl Cohen, E.U. A Step Closer to Recognizing UK and South Korea as Adequate for Cross-Border Data Transfers
Pinsent Masons, UK guide on data transfer codes and certification anticipated
Politico, Europe to US: Pass new laws if you want a data-transfer deal
Politico, Biden seeks high-level data deal to repair EU-US digital ties
Politico, Facebook's US data transfers suffered a setback in Ireland. Here's what you need to know.
Presswire, European Parliament Motion Highlights Need for a Review of Data Protection Practices in the wake of Schrems II
Reuters, Facebook faces prospect of 'devastating' data transfer ban after Irish ruling
Reuters, Irish data regulator resumes Facebook data transfer probe
Scoop News NZ, EU-U.S. Data Flow Deal Possible?: Third Time Won't Be The Charm Without U.S. Surveillance Reform
Sidley Austin LLP, Swiss Data Protection Act – New Guidance by the Swiss Regulator
South China Morning Post, China's new Data Security Law promises steep punishments for unapproved overseas data transfers
Swiss Federal Data Protection and Information Commissioner, Guide for checking the admissibility of data transfers with reference to foreign countries
TechCrunch, European Parliament amps up pressure on EU-US data flows and GDPR enforcement
The Hill, Facebook loses bid to block Irish watchdog's data flow decision
The Federalist, China Quickly Passes New Law Hoovering Up Private Data That Could Include Yours
Trade for Development News, How can the "data revolution" work for developing economies?
TechCrunch, EU puts out final guidance on data transfers to third countries
The Wall Street Journal, China's New Power Play: More Control of Tech Companies' Troves of Data
Trade for Development News, How can the "data revolution" work for developing economies?
US Chamber of Commerce, U.S. Businesses Face the Specter of Data Localization in Europe
US Chamber of Commerce, Transatlantic Relations: Convergence in Principle, Divergence in Fact?
US Chamber of Commerce, Europe's Data Strategy: Promoting Innovation or Undermining Competition?
UNCTAD, Technology and Innovation Report
University of Cambridge, Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection
UK Department of Health and Social Care, Data saves lives: reshaping health and social care with data
UK Department for International Trade, Joint statement on UK-New Zealand trade talks
UK Taskforce on Innovation, Growth and Regulatory Reform, A Bold New Regulatory Framework for the UK (including Replacing the GDPR with a New UK Framework for Data Protection)
US Congressional Research Service, EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield
US Congressional Research Service, EU Digital Policy and International Trade
Wall Street Journal, China's New Power Play: More Control of Tech Companies' Troves of Data

Wall Street Journal, Facebook Loses Bid to Block Ruling on EU-U.S. Data Flows
WashingtonPost, Wyden urges ban on sale of Americans' personal data to 'unfriendly' foreign governments
World Bank, Mapping Data Governance Legal Frameworks Around the World, World Development Report 2021
World Economic Forum, Digital Technology Can Help the World Prosper
World Economic Forum, How to harness AI and data portability for greater financial inclusion
Wilson Center, Transatlantic Digital Economy Series

- The changing nature of digital trade, current and future barriers, and ideas to overcome them
- The expanding digital frontier
- The Importance of Digital Services to the U.S. and European Economies
- On New Regulation of Europe's Digital Markets
- The Digital Revolution: Scenarios for Enhanced Transatlantic Cooperation
- Time for a U.S.—EU Digital Alliance

World Politics Review, The West's Wakeup Call on Digital Tech Standards
ZDNet, A major international data flow problem just got resolved. But another row is already brewing

SIX-MONTH LOOK AHEAD

The table below includes anticipated developments/milestones in the coming months.

Country / Market / Organization	Policy Development / Milestone	Key Dates
APEC	**APEC New Zealand Host Year**	**Dec. 2020 – Nov. 2021:** In 2021 APEC (hosted by NZ, schedule here) will include meetings focused on cross-border data and other digital policy matters. Major meetings include SOM2 (**May 18-June 4**), Trade Ministers' Meeting (**June 4-5**), SOM3 (**Aug 10-Sept. 3**), and the Economic Leaders' Meeting, APEC Ministers' Meeting, and the Concluding Senior Officials' Meeting (week of **Nov. 8**).
AUSTRALIA	**Privacy Act Review**	**TBD (2021):** In late October 2020, the Australian Government announced the commencement a review of the Privacy Act conducted by the Attorney-General's Department. To start the review, the Government has released an issues paper for public comment. The review process should continue throughout 2021.
BRAZIL	**Personal Data Protection Law**	**August 1, 2021:** The provisions of the Brazilian Personal Data Protection Law (LGPD) regarding fines/penalties for non-compliance will enter into force on August 1, 2021.
CHINA	**New rules impacting data transfers and data localization**	**Ongoing:** In April 2021, China published second drafts of the Data Security Law, as well as a draft Personal Information Protection Law. China also recently published the Automotive Data Management Rules. The NPC subsequently approved the Data Security Law, which is scheduled to take effect on September 1, 2021.
EU	**Evaluation of Adequacy Decisions**	**Q2 2021:** The European Commission is expected to complete its evaluation of adequacy decisions with 11 countries (all but Japan which follows a different calendar)**by summer 2021**. This evaluation may lead to adjustments in the implementation of these adequacy decisions, in particular in view of the ECJ ruling.
EU-US	**Negotiations on Privacy Shield replacement**	**Ongoing:** The EU and US launched discussions on August 10, 2020 and are currently ongoing. In March, both countries released an announcement regarding their intensification of those negotiations.
EU	**Bilateral FTA negotiations**	**Ongoing:** The EU is currently negotiating bilateral FTAs with Australia and New Zealand, both of which are tabling CP-TPP language on data flows. The EU also relaunched its FTA negotiations with India in May 2021, and launched a EU-India Connectivity Partnership.
G7	**G7 UK Host Year**	**Jan. – Dec. 2021:** The G7 (hosted by the UK) includes workstreams on digital trade, digital health, and digital technology (including data free flow with trust)(DFFT). Under DFFT, the G7 may address government access, regulatory cooperation on data protection, data sharing, and data localization. The G7 February Joint Leaders' statement addressed data transfers, as did the April 2021 Digital and Technology Ministerial Declaration. In addition to the regular G7 members, Australia, India and South Korea are participating as guests in 2021. The G7 Technology Ministerial took place on **April 27 to May 1**, and the G7 Summit took place on **June 11-13, 2021**.
G20	**G20 Italy Host Year**	**Jan. – Dec. 2021:** The G20 (hosted by Italy; schedule here) has a workstream focused on cross-border data flows (along with workstreams focused on digital transformation, measurement of data flows, the developing country connectivity gap, inclusive AI, etc). Digital Economy Task Force meetings are scheduled for **May 17**, and **August 4**. The Digital Economy Ministers' Meeting will be held on **August 5**. Trade & Investment Group meetings are

		scheduled for **May 3-4**, and **October 10-11**. The Trade Ministers' Meeting will be held on **October 12**. The Leaders' Summit is scheduled for **October 30-31, 2021**.
INDIA	**Personal Data Protection (PDP) Bill**	**April – July 2021:** The Joint Parliamentary Committee (JPC) got an extension to present its report on PDP by June or July 2021 during the monsoon session of the Parliament. Once the report is tabled, the updated Bill would have to be published and then passed by both houses. Given increase in COVID-19 cases across the country and general delay in submission of the report, the timeline for the completion of this policy process is unclear.
INDIA	**Non-Personal Data (NPD) Governance Framework**	**Ongoing (2021):** GDA submitted comments to the Committee of Experts on Non-Personal Data Governance Framework on January 29, 2021. The Committee will review the comments and is expected to submit the updated Framework to MeitY, but timing on this next step is unclear.
JAPAN	**Consolidation of Personal Data Protection Laws**	**Ongoing (2021):** A draft law to consolidate three laws related to personal data protection (the Act on the Protection of Personal Information, the Act on the Protection of Personal Information Held by Administrative Agencies and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies) and centralize jurisdiction under PPC has passed the Diet on May 12. The Government is aiming to achieve GDPR adequacy for academic and research sectors for personal data transferred from EU to Japan by applying requirements on security measures etc. to these sectors which had previously been excluded for use in academic studies. At this point, there are no indications that this consolidation would negatively impact cross-border data flows. The PPC is planning to compile Cabinet Order and Enforcement Rules for Administrative Organs and Incorporated Administrative Agencies as well as Guidelines for academic and research organization by summer. The Cabinet Order and Enforcement Rules for local governments are planned to be drafted by this winter.
JAPAN	**Implementation of the Amended Act on the Protection of Personal Information**	**Ongoing (2021):** GDA filed comments to the Personal Information Protection Commission (PPC) on the Guidelines for the Amended Act on the Protection of Personal Information (APPI) enacted in June 2020. The draft Guidelines elaborates on the new requirement to enhance information to be provided to data subject for the purposes of cross-border data flows, and GDA requested PPC to release consolidated information on the personal information protection system in foreign countries, to avoid disparity in information to be provide from respective business operators, as well as to provide further clarity on the information regarding the existence of other systems that may have significant impact on the rights and interests of the data subject. .
UK	**Bilateral FTA negotiations**	**Ongoing (2021):** In addition to the trade/economic partnership agreements concluded in 2020 with the EU, Japan, Kenya, Singapore, Turkey, and Vietnam the UK has proposed or launched FTA negotiations with Australia, India, EEA/EFTA, New Zealand, and the United States. It has also stated an interest in negotiating accession to the CPTPP. Discussions on these agreements will continue throughout 2021.
US	**Bilateral Digital Trade Negotiations**	**Suspended:** The United States launched FTA negotiations with Kenya and the United Kingdom during the Trump Administration. It remains to be seen whether and how soon the Biden Administration will advance these negotiations.
WORLD TRADE ORGANIZATION	**Various:** Joint Statement Initiative (JSI) Digital Trade Talks; Committee and General Council Meetings; Public Forum; Ministerial Conference	**Ongoing:** Several WTO processes are potentially relevant to cross-border data flows and data localization measures. This includes the JSI digital trade negotiations, which include ongoing small group meetings, as well as plenary meetings in April and June 2021. Additionally, the 2021 WTO Public Forum is scheduled for **September 28-30**, and the WTO's 12th Ministerial Meeting is Scheduled for the **week of November 29**.
OTHER: IAPP	**IAPP Webinars**	**June 28:** 'Schrems II' Data Transfers Impact: Steps to Protect and Enable Transfers. Details and registration here.
OTHER: GSMA MWC	**MWC 2021**	**June 28 – July 1:** MWC21 – Details here.