GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

Comments on the Draft Amendments to the Personal Data Protection Law

December 15, 2022

The Global Data Alliance[1] (GDA or Alliance) supports Saudi Arabia's efforts to improve standards of personal data protection in Saudi Arabia. The Alliance respectfully submits several comments and recommendations regarding PDPL Article 28 as it relates to cross-border data policy in Saudi Arabia. Generally speaking those recommendations urge Saudi Arabia to explore revisions to Article 28(1) to better promote data protection and data security; (2) to eliminate data transfer restrictions that are greater than necessary; (3) to eliminate aspects that discriminate against non-national persons or technologies, or against particular economic sectors; and (4) to allow enterprises and citizens (including workers and consumers) in Saudi Arabia to benefit from cross-border access to best-in-class technology from across the globe.

In addition to the GDA's comments and recommendations on PDPL Article 28 below, we have included two Appendices. Appendix I compiles evidence from the World Bank, the World Trade Organization, the United Nations (including UNCTAD), the OECD, the World Economic Forum, and other organizations that have carefully studied various countries' cross-border data policies, and the economic and policy implications of those policies. Appendix II contains excerpts from the GDA's Cross-Border Data Policy Principles.

I. Introduction

The GDA supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine data security, innovation economic development, and international trade. Alliance member companies are significant investors in Saudi Arabia, collectively employing thousands of Saudi Arabian citizens and working to advance growth, innovation, and cross-sectoral diversification in Saudi Arabia.

The ability to transfer data securely across transnational digital networks is of central importance to the national policy objectives of many countries, including Saudi Arabia. Data transfers support COVID-19 recovery, digital connectivity, cybersecurity, fraud prevention, anti-money laundering, and other activities relating to the protection of health, privacy, security, and regulatory compliance.

This ability also supports shared economic prosperity. Cross-border access to marketplaces, purchasers, suppliers, and other commercial partners allow Saudi enterprises in all sectors to engage in mutually beneficial international transactions with foreign enterprises. Data transfers, which are critical at every stage of the value chain for companies of all sizes, support global supply chains and promote productivity, safety, and environmental responsibility. This ability also supports scientific research and development across borders.

II. Comments and Recommendations regarding PDPL Article 28

The GDA welcomes several of the changes that have been made to the PDPL to date. For example, relative to the prior draft of Article 28, the elimination of references to "extreme necessity" in the criteria in Article 28.2 is a welcome change. The GDA continues to recommend that Saudi Arabia consider additional revisions to the PDPL's cross-border data elements as to ensure that Saudi Arabia achieves its policy objectives without generating unintended consequences. We elaborate below.

A. Article 28.1(a) – Conflicts with Other Country Laws and Difficulty in Administration

We urge Saudi Arabia to revise Article 28.1.a to avoid unintended legal conflicts with other countries' legal frameworks and difficulties in administration. For the reasons explained below, we recommend that Saudi Arabia revise the text of Article 28.1.a as follows:

> (1) Controller may transfer Personal Data outside the Kingdom or disclose Personal Data to an entity outside the Kingdom in accordance with the following:
>
> a. ~~If the~~ To any country to which the Personal Data is to be transferred, provided that the Competent Authority has **not** determined that such country lacks:
>
> i. ~~has~~ regulations that ensure appropriate protection of Personal Data and protection of the rights of Personal Data Subjects;
>
> ii. ~~has~~ a supervisory entity that imposes appropriate procedures and measures on Controllers to protect Personal Data; and
>
> iii. ~~so that the~~ standards of Personal Data protection ~~in that country are not less than~~ broadly equivalent to the standards provided for under this Law and the Regulations.
>
> b. The Competent Authority shall adopt~~s~~ evaluation criteria for the requirements set out in paragraph (1.a) of this Article.

We explain the foregoing recommendations below.

First, **we recommend that Saudi Arabia adopt the so-called "Accountability Principle," and remove the presumption in draft Article 28.1.a that personal data transfers are to be prohibited to most other countries**. As stated in the GDA's Cross-Border Data Policy Principles:

> **Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders.** The presumption favoring the movement of data across digital networks reflects the reality of international economic relations today: Data moves seamlessly and securely across globally or regionally distributed cloud-based digital networks that do not match up neatly with national boundaries.
>
> Digital networks lie at the heart of our interconnected global economy. They support millions of daily transactions occurring all over the world, across every sector and at every stage of the value chain, including at the R&D, product design, regulatory approval, manufacturing, finance, marketing, sales, and post-sale service stages.
>
> Countries should not disturb the longstanding practice and presumption that data can move seamlessly and responsibly across these networks. Cross-border data transfers are already estimated to contribute trillions of dollars to global GDP. Sixty percent of global GDP is expected to be digitized by 2022, and six billion consumers and 25 billion devices are expected to be digitally connected by 2025. Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing. The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance. Many Regional Trade Agreements (RTAs) reflect this presumption.[2]

Currently, the draft text of Article 28.1.a only permits personal data transfers to countries affirmatively determined to offer protection "no less than the standards" provided in Saudi Arabia. This formulation essentially prohibits all personal data transfers except to a very small universe of countries – a universe of countries that could be even **zero**.

The presumption that Saudi Arabia must substantially isolate itself from other countries unless and until those countries have been determined to offer "no less" data protection than Saudi Arabia would be detrimental to Saudi Arabia's economic, political, and social interests without offering any meaningful personal data protection benefits.[3] For additional information on the risks that Saudi Arabia would face, please see the extensive literature on the significant risks and challenges that the EU would face if data transfers from the EU were limited to the 13 countries[4] currently deemed to be adequate under the GDPR, and blocked to all other countries.[5]

In lieu of an approach that would isolate Saudi Arabia from other countries, the GDA recommends that Saudi Arabia adopt the so-called "accountability principle," which reflects the prevailing international legal norm relating to the cross-border movement of data.[6] Under this principle, organizations that transfer data globally should implement procedures to ensure that data will continue to be protected, even if it is transferred to countries other than where it was first collected. The accountability principle was first developed by the OECD,[7] and was subsequently endorsed and has been integrated in many legal systems including the EU,[8] Japan,[9] New Zealand,[10] Singapore,[11] and Canada.[12] This principle is also a significant feature of the APEC Privacy Framework,[13] the APEC Privacy Recognition for Processors (PRP) system,[14] the APEC Cross Border Privacy Rules (CBPR) system,[15] and the ASEAN Model Contractual Clauses.[16]

For the foregoing reasons, we urge Saudi Arabia to adopt the Accountability Principle. If Saudi Arabia must stipulate restrictions in its law, we recommend that it replace the current presumption against personal data transfers with a presumption that data transfers are permitted except where provided otherwise.

Second, we urge Saudi Arabia to replace the requirement for "no less" standards of protection with a requirement for "broadly equivalent" standards of protection. The "no less" standard could reasonably be misunderstood to require "the same or greater" standards of protection.[17] Such an interpretation would require identical or stronger levels of protection – a very narrow and exacting requirement that few – if any – countries might satisfy. Again, if companies or their legal advisors – or the Competent Authority – are unable to identify any countries with at least the identical set of data protection provisions to those provided by Saudi Arabia, they may perceive there to be no country to which data can be transferred from Saudi Arabia. Such an outcome would be highly detrimental to Saudi Arabia's interests. For this reason, we urge Saudi Arabia to apply a standard of assessing whether another country's standards of personal data protection are "generally equivalent" or "broadly equivalent" to those in Saudi Arabia.

Finally, we recommend that Saudi Arabia consider including an interpretative note to Article 28.1.a along the lines of the the standard of outlined in Article 44 of the EU General Data Protection Regulation (GDPR), which states as follows: "All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

B. Article 28.2 – Lack of Data Transfer Mechanisms

PDPL Article 28 does not contain most of the data transfer mechanisms that are found in (for example) GDPR Articles 45- 50 or any of the mutual recognition principles that are reflected in the Global Cross-Border Privacy Rules Forum. These types of data transfer mechanisms are a critical part of any data protection law that addresses cross-border data transfers.

We urge Saudi Arabia to explore approaches in Article 28 to ensure that appropriate transfer mechanisms are available under Saudi law and interoperable with other global frameworks. Among other things, we recommend that Saudi Arabia allow, consistent with prevailing international norms and best practices, for a framework of cross-border data transfer mechanisms (including contractual arrangements, binding corporate rules, codes of conduct, certification mechanisms, mutual recognition frameworks, adequacy arrangements, or other means of protecting data that is being transferred). Such mechanisms should be available even for countries that Saudi Arabia has determined **not** to offer appropriate data protections. By including a wide range of alternative transfer mechanisms in the PDPL, Saudi Arabia will avoid unintended harms that would isolate and disconnect it from the legal frameworks of regional and global partners.

Finally, as stated in the GDA's Comments on Draft Executive Regulation of the Saudi Personal Data Protection Law,[18] we urge Saudi Arabia not to require case-by-case advance governmental approval for the use of data transfer mechanisms. Such *ad hoc* approval requirements would reduce legal predictability and would be unnecessary in light the government's existing authority to set transfer conditions under such transfer mechanisms.

C. Article 28.2 – Grounds for Data Transfers in Exceptional Circumstances

Taken together, the current framing of Article 28.1.a and the absence of data transfer mechanisms reflects a restrictive approach to data transfers. Article 28.2 would permit derogations from this restrictive approach where such transfers are: (1) for preserving the public interest, public health, public safety, or protecting the life or health of a specific individual or individuals; (2) relating to performing an obligation under an international agreement to which the Kingdom is a party; or (3) done in performance of an obligation of the Personal Data Subject. The GDA welcomes the inclusion of these exceptions and welcomes the revised drafting from "extremely necessary" to "is for". We make several additional suggestions.

First, while the exceptions are helpful, we respectfully suggest that they are not a substitute for the data transfer mechanisms (as suggested in comment 2 above). In that regard, we observe that those data transfer mechanisms should be available in all cases – even absent application of a particular exception – because the transfer mechanisms themselves are designed to ensure that Saudi data protection standards are respected with respect to data that is being transferred. In sum, if a listed exception is available, then data may be transferred without reliance on an enumerated data transfer mechanism. On the other hand, if a listed exception is not available, then data may be transferred on the basis of an enumerated data transfer mechanism.

Second, the GDA considers the final three exceptions – relating to public interest, international commitments, and contract obligations – to be particularly important. We suggest that these exceptions be clarified as follows:

a. Article 28.2.a: We recommend that Saudi Arabia develop interpretative guidance or an illustrative list of examples of the "public interest," such as "to protect Saudi Arabia's cybersecurity or other security interests; to promote compliance with Saudi Arabia's regulatory requirements; to promote Saudi Arabia's international relations; to promote economic opportunity for Saudi Arabia; and to achieve other outcomes in the public interest of Saudi Arabia."

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

c. Article 28.2.c: Revise this provision to add the following underlined text: "…in performance of an obligation of the Data Subject, the Controller, or the Processor..." This change would recognize that the data controller or processor may also be subject to contractual obligations that require the transfer of data, and that such obligations should be respected.

III. Conclusion

The GDA appreciates the opportunity to make the attached submission, and respectfully recommends that Saudi Arabia make several revisions to PDPL Article 28. We appreciate the opportunity to share these views and hope that they will be helpful as Saudi Arabia considers next steps. Policy makers around the world appreciate the GDA sharing best practices on data flows and we would welcome further engagement with Saudi authorities to address any questions regarding this submission.

---

[1] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, financial services, health, media and entertainment, natural resources, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org

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

[3] Indeed, the concern that Saudi personal data transfers would be blocked to all other countries without recourse pending such a formal determination is heightened by the fact that Article 28 does not recognize any of the data transfer mechanisms (standard contractual clauses, binding corporate rules, certification, interoperability frameworks, etc.) that are common in other countries' personal data protection frameworks.

[4] EU Commission website, Adequacy Decisions Webpage (2022), at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[5] *See e.g.,* Global Industry Statement, Strengthening Data Protection Through a New Trans-Atlantic Data Privacy Framework (2022), at: https://globaldataalliance.org/wp-content/uploads/2022/04/04072022gdaglltr.pdf

[6] The GDA strongly supports the accountability model for international data transfers. This model was, first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles. The accountability model provides an approach to cross-border data governance that effectively protects the privacy and consumer rights of individuals and fosters streamlined, robust data flows by requiring entities that collect personal information (often defined as personal data controllers) to be responsible for its protection no matter where or by whom it is processed.

While governments are rightfully concerned with risks to privacy and data security, these risks are not dependent on the physical location of where data is stored or processed, or the location of the infrastructure supporting it. In fact, the effectiveness of data security and personal information protection is a function of the technologies, systems, and procedures put in place by the companies handling the personal information to protect the data.

To benefit from cross-border data transfers while simultaneously ensuring the responsible processing and protection of data, the focus of privacy policy and regulation needs to be on the quality and effectiveness of the mechanisms and the controls maintained to protect the data in question. The accountability model, therefore, continues to be an important tool in increasing privacy and security by requiring entities to ensure that data will continue to be properly protected, regardless of where the data is located.

Personal data protection and privacy frameworks that are based on a common set of international consensus-based principles facilitate cross border data transfers and drive innovation and business investment in local markets by promoting international interoperable legal frameworks upon which businesses of all sizes can rely. These coordination mechanisms also help to bridge current gaps in international privacy norms while facilitating the safe and secure international transfer of personal information. Such mechanisms may include private codes of conduct, contractual arrangements such as standard contractual clauses, certifications such as the APEC Cross Border Privacy Rules (CBPR), seals or marks, and mutual recognition arrangements such as the adequacy with the European Union General Data Protection Regulation (GDPR).

[7] OECD Privacy Framework 2013 (p15), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[8] Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[9] Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/

[10] Privacy Act 2020, https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[11] Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[12] Personal Information Protection and Electronic Documents Act fair information principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[13] APEC Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[14] APEC Privacy Recognition for Processors, reference needed

[15] APEC Cross Border Privacy Rules system, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

[16] ASEAN Model Contractual Clauses (2021), at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf; *See also,* Singapore Personal Data Protection Commission, Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore (2022), at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en#:~:text=The%20ASEAN%20Model%20Contractual%20Clauses%20%28ASEAN%20MCCs%29%20are,parties%20that%20protects%20the%20data%20of%20data%20subjects.

[17] Determining whether another jurisdiction's data protection laws provide "less" protection than Saudi Arabia is an unpredictable and subjective exercise. Many methodological challenges arise. These include: (a) which benchmarks and metrics should be applied in comparing different jurisdictions; (b) what aspects of each country's law are to be examined; (c) how to treat a country that provides more detailed or specific protections in some respects but not others; (d) how to treat a country that affords greater accountability and flexibility around data transfers via data transfer mechanisms; and (e) whether to apply a quantitative, qualitative, or a hybrid analytical framework.

[18] *See* Global Data Alliance, GDA's Comments on Draft Executive Regulation of the Saudi Personal Data Protection Law (March 2022), at: https://globaldataalliance.org/wp-content/uploads/2022/03/03292022gdasadatapro.pdf

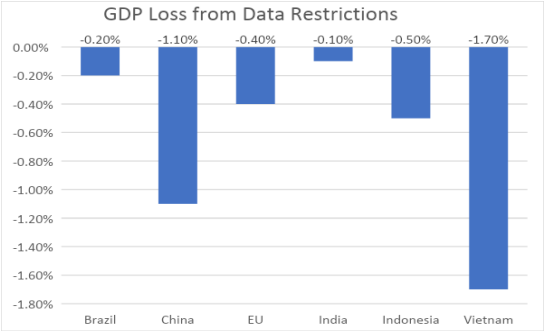
Appendix I

Economic and Policy Impacts of Data Localization Mandates and Cross-Border Data Restrictions

International organizations from the World Bank to the World Trade Organization have underscore the harms and risks that data localization mandates and cross-border data restrictions raise. Much of that evidence is directly relevant to the cross-border data restrictions proposed in Article 28 of Saudi Arabia's draft Personal Data Protection Law (PDPL). We summarize some of that evidence below, which many help inform Saudi Arabia's evaluation of the economic and policy implications of Article 28.

- **Impact on Saudi Arabia's Position as an Emerging Regional Center of Technology Services:** Saudi Arabia is an emerging regional leader in offering cloud computing and other technology services to neighboring economies. Saudi Arabia's policy positions also have broad regional influence. Saudi Arabia risks losing this position if technology providers are prohibited from providing those services to neighboring countries. Saudi Arabia's position will also be jeopardized if its neighboring economies emulate the cross-border data restrictions found in the draft Regulation – imposing their own requirements for localization of data storage and processing, and restricting cross-border data transfers to or from Saudi Arabia.

- **Impact on Saudi Arabia's Broader Economic Goals**: The World Bank's 2020 *World Development Report* found that, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies... Countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."[i]
  Cross-border data restrictions are sometimes justified as benefiting economic development. In fact, development benefits from an increase — not a decrease — in connectivity.[ii] Self-isolating cross-border data restrictions hinder economic development, reduce productivity, deprive local enterprises of commercial opportunities, and depress export competitiveness. It is estimated that such measures reduce GDP by up to 1.7 percent in implementing countries, as indicated in the table analyzing GDP impacts below.[iii]



- **Impact on Saudi Arabian Goods Exports:** Cross-border data restrictions are particularly damaging to advanced and connected industries, including in natural resources and agriculture. It has been estimated that 75% of the value of data transfers accrues to such industries.[iv] Saudi Arabia exported nearly $15 billion in goods to the United States in 2019, and exports to the EU, Asia, and other regions were even larger.[v] Data transfers are also critical to reducing the costs of reaching markets outside of Saudi Arabia. Data transfers not only enable local firms to find prospective customers in export markets; they also reduce supply chain-related transaction costs.[vi] One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.[vii]

- **Impact on Saudi Arabian Services Exports:** In 2019, Saudi Arabia exported $1.5 billion in services to the United States, in travel, financial services, and transportation services – all areas that are heavily dependent on cross-border access to technology and data transfers.[viii] The World Bank 2021 *World Development Report* has noted that measures that "restrict cross-border data flows ... [may] materially affect a country's competitive edge in the burgeoning trade of data-enabled services."[ix] A 2020 World Economic Forum study found that, "approximately half of cross-border [services] trade is enabled by digital connectivity[, which] … has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution."[x]

- **Impact on Saudi Arabian Enterprise Productivity, including in Natural Resources:** In all sectors, including natural resources, enterprises rely on data transfers to increase productivity and improve operations.[xi] Cloud-enabled software technologies (including IoT technologies) offer significant promise in making natural resource exploration and extraction more productive and carbon-efficient.[xii] Restrictions that impair the ability to deploy such technologies can undermine that potential. For example, a 2021 GSMA study indicates that data localization measures on IoT applications and M2M data could result in:
    - Loss of 59-68% of their productivity and revenue gains;
    - Investment losses ranging from $4-5 billion;
    - Job losses ranging from 182,000-372,000 jobs.[xiii]

The cross-border data restrictions in the PDPL may also undermine public policy goals relating to the privacy, security, health, and welfare of persons in Saudi Arabia. We address these topics below.[xiv]

- **Impact on Privacy**: Some argue that data localization requirements and cross-border data restrictions are necessary for privacy reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. This argument is incorrect. Cross-border restrictions are not necessary to protect privacy and can undermine data security. In lieu of such restrictive policies, countries with robust data protection frameworks often adhere to the accountability principle and interoperable legal frameworks that protect data consistent with national standards, even as the data is transferred across borders. Organizations that transfer data globally typically adopt a set of best practices and internal controls to ensure that the data is protected even when transferred outside of the country. To that end, organizations often rely on various approved data transfer mechanisms.[xv]

- **Impact on Cybersecurity**: Some argue that cross-border data restrictions are necessary to ensure cybersecurity. However, *how* data is protected is more important to security than *where* it is stored, and transfer restrictions often result in *weaker*, not *stronger*, cybersecurity. Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Stronger cybersecurity is enabled by cross-border data analytics an assertive cyber-defense posture coordinated across IT networks and national boundaries.[xvi] When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.[xvii]

- **Impact on Regulatory Compliance**: Some claim that cross-border data restrictions ensure governmental access to data for regulatory or investigatory purposes. The location of the data, however, is not the determining factor. On the contrary, "data localization requirements can increase … operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information."[xviii] Accordingly, regulatory authorities in many countries actually encourage the responsible transfer of data across borders.[xix] Likewise, data

transfers are critical to other public policy priorities, including financial fraud monitoring and prevention; anti-money laundering; anti-corruption; and other legal compliance objectives.

- **Impact on Innovation:** Some claim that cross-border data restrictions promote innovation. On the contrary, data localization mandates and data transfer restrictions undermine beneficial innovation processes—from accessing global scientific and technical research databases, to engaging in cross-border research and development (R&D), to securing intellectual property rights for new inventions, and regulatory product approvals for new products and services.[xx]

- **Impact on ICT Policies:** From artificial intelligence to 5G to the cloud, governmental ICT policies can help coordinate public-private dialogue, support investment, and maximize the benefits of ICT technologies across the economy. Cross-border data restrictions often undermine these polices. For example, the benefits of a "cloud first" policy are most likely to arise in a cross-border context that allows for elastic and scalable delivery of computing resources, rapid load balancing, and ready access to best-in-class technology from all over the world. Using data localization mandates and transfer restrictions to ban cross-border access to cloud computing infrastructure and technology would deprive local enterprises (including MSMEs) and users of:
    - Cross-border access to IT resources hosted abroad;
    - Cross-border collaboration and communication with foreign business partners;
    - Foreign transactions and business opportunities; and
    - Improved resiliency resulting from data storage across multiple geographical locations.[xxi]

- **Impact on Prevention of Fraud, Money laundering, or Other Financial Crimes**: If financial data is categorised as "classified data", the prohibition on cross-border data transfers without government approval in respect of financial data would have significant negative impacts on the effectiveness of efforts to prevent fraud, money laundering, terrorist financing, or other financial crimes. For example, effective fraud mitigation as provided by banks, card networks and other players in the financial services sector demands sophisticated monitoring and rapid detection at the time of transaction to interpret and weigh the risk of fraud of each payment transaction as weighed by the facts of that payment transaction as against norms for all payment transactions and that account. Fraud detection models are typically built on global transaction data or transaction data collected from multiple countries since fraud patterns are not limited by national boundaries. Fraud trends which appear in one region or country may apply in others as cardholders travel to different countries, cardholders transact online with merchants in different countries, and the perpetrators of fraud do not respect any national boundary lines. Thus, to build effective fraud models and to gain the necessary insights into fraudulent activity in order to help prevent them, these models must be built off of global or multi-country data sets, based both on the location of the merchant and the location of the cardholder. Similar technologies and techniques are used to track and prevent other financial crimes. The restrictions proposed in the PDPL may undermine the ability to prevent such activity in Saudi Arabia and beyond.

- **Impact on Healthcare:** Healthcare R&D, the submission of health-technology-assessment and regulatory filings, and the provision of services in the life-science industries are increasingly cross-border endeavors which rely on the responsible and secure flow of large volumes of data. These transfers can support the adoption of data analytics and machine-learning technologies, and processing of data from multi-country clinical studies and other research activities. Supporting cross-border data transfers, in a way that is compatible with the best practices in ensuring patient and customer privacy, is essential for the innovation of healthcare products and services, collaboration across multiple public and private research organizations, and the early detection of regional or global health risks. Restricting such data transfers will undermine the ability to identify new treatments and improve healthcare delivery, to the ultimate detriment of patients in those countries that restrict transfers.

- **Impact on COVID-19 Recovery:** As governments seek to limit the spread of COVID-19, cross-border access to technology and data transfers have become essential for countries seeking to

sustain jobs, health, and education. This is particularly true for the remote work, remote health, supply chain management, and innovation-related technologies that depend on cross-border access to cloud computing resources.[xxii]

Annex II

GDA Cross-Border Data Principles (excerpts)

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

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

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

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

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

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

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

- Be transparent;[xxix]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[xxx]
- Analyze that evidence according to sound, objective, and verifiable methods (including regulatory impact assessments—as discussed further under Principle 4 below);
- Provide opportunity for input from the public, experts, and interested stakeholders;[xxxi] and
- Include other procedural safeguards and due process.[xxxii]

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

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

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

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

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

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

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

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

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

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

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

This analysis is important because **how** data is protected is typically more salient than **where** it is stored.

As outlined above and in many RTAs negotiated to date, rules impacting cross-border data transfers should be necessary to achieve a legitimate and justified public policy objective and impose no more restrictions on data transfers than necessary.

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

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

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

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

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

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

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

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

- **International Frameworks Regarding Regulation of Data Transfers and Localization:** Another trust-building mechanism involves negotiating agreements to prohibit unnecessary data transfer restrictions and data localization mandates. Thus, these agreements reaffirm the core principle that the seamless and responsible movement of information across digital networks is foundational to a healthy, integrated global economy. These agreements also can more precisely define the relationship between rules impacting data transfers and specific policy objectives. Overall, these agreements support legal certainty, helping grow digital trust, economic development, and technological innovation.[xli]

---

[i] World Bank, World Development Report (2020), at: https://www.worldbank.org/en/publication/wdr2020

[ii] *See e.g.,* Ferracane et al., *The Costs of Data Protectionism,* VOX (2018); Ferracane et al., *Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?* ECIPE Digital Trade Estimates Working Paper No. 1 (2019); Lund et al., Defending Digital Globalization, McKinsey Global Institute (2017). Access to foreign markets, innovation, education, and economic growth are all jeopardized by governmental measures that: (1) block cross-border access to information; (2) interfere with the circulation of technology, knowledge, and commercial data; (3) restrict connectivity to the Internet; (4) deny MSMEs and other local enterprises or citizens opportunities to engage with the technologies they need to engage with the economy. *See* https://hbr.org/2017/07/60-countries-digital-competitiveness-indexed

[iii] *See* Lee-Makiyama et al., *The Costs of Data Localization*, ECIPE Occasional Paper (2014), at: https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf

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

[v] USTR website, US-Saudi Arabia Bilateral Trade (2022), at: https://ustr.gov/countries-regions/europe-middle-east/middle-eastnorth-africa/saudi-arabia

[vi] Global Data Alliance, *Cross-Border Data Transfers and Supply Chain Management* (2021), at https://globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf

[vii] Micro-Revolution: The New Stakeholders of Trade in APAC, Alphabeta, 2019. Likewise, the Asia Development Bank Institute estimates that electronic commerce platforms, which operate on the basis of cross-border data transfers, have helped some local firms reduce the cost of distance in trade by 60%. Asia Development Bank Institute, *The Development Dimension of E-Commerce in Asia: Opportunities and Challenges* (2016), at: https://www.adb.org/sites/default/files/publication/185050/adbi-pb2016-2.pdf

[viii] USTR website, US-Saudi Arabia Bilateral Trade (2022), at: https://ustr.gov/countries-regions/europe-middle-east/middle-eastnorth-africa/saudi-arabia

[ix] World Bank, *World Development Report – Data For Better Lives* (2021), at: https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf

[x] World Economic Forum, Paths Towards Free and Trusted Data Flows (2020).

[xi] Data localization mandates and unnecessary data transfer restrictions hurt local innovation because a country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are critical to growth and innovation, business operations, and the transfer of technology. These include: (a) productivity-enhancing

software solutions; (b) scientific, research, and other publications; and (c) manufacturing data, blueprints, and other operational information. Faced with higher software costs and an unpredictable environment for R&D investments, local industries face challenges keeping technological pace with foreign competitors — threatening both domestic and export market sales. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for investment and R&D.

[xii] *See e.g.,* World Economic Forum, Digital Transformation Initiative: Oil and Gas Industry (January 2017), available at http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-oil-and-gas-industry-white-paper.pdf; IBM, Tapping the Power of Big Data for the Oil and Gas Industry, White Paper, available at https://www-935.ibm.com/services/multimedia/Tapping_the_power_for_the_big_data_for_the_oil_and_gas_industry.pdf ; Tom DiChristopher, Oil Firms Are Swimming in Data They Don't Use, CNBC (March 5, 2015), available at https://www.cnbc.com/2015/03/05/us-energy-industry-collects-a-lot-ofoperational-data-but-doesnt-use-it.html; Ed Crooks, "Drillers Turn to Big Data in the Hunt for More, Cheaper Oil," Financial Times (February 12, 2018), available at https://www.ft.com/content/19234982-0cbb-11e8-8eb7-42f857ea9f09; Chevron Partners With Microsoft to Fuel Digital Transformation From the Reservoir to the Retail Pump (October 30, 2017), available at https://www.chevron.com/stories/chevron-partners-with-microsoft

[xiii] GSMA, Cross-border Data Flows – The Impact of Localization on IOT (2021).

[xiv] For additional information, *see* https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf

[xv] *See generally* footnote 8, *infra.* These data transfer mechanisms may include adequacy decisions, certifications, codes of conduct, Binding Corporate Rules (BCRs), and Standard Contractual Clauses (SCCs) that contain built-in data protection safeguards.

[xvi] *See id.* Cloud services delivered across-borders provide security advantages over alternative IT delivery approaches (on-premises or local cloud services):

- Physical Security: Certified personnel can carefully monitor servers 24/7 to prevent physical breaches, and can apply consistent protocols over a small number of locations.
- Data Security: CSPs can ensure data integrity through use of state-of-the-art encryption protocols for data at-rest and in-transit. CSPs can establish redundant backups of data in geographically dispersed data centers, mitigating risk of loss in the event of power outages or natural or manmade disasters.
- Advanced Threat Detection: CSPs leverage state-of-the-art enhanced security intelligence They use regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- Automated Patch Deployment: Automated and centralized patch deployment and realtime updates to network security protocols work to protect systems from newly identified vulnerabilities.
- Incident Management and Response: CSPs maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- Certification: CSPs are typically certified to international security standards, and go through regular audits to maintain their certifications.

[xvii] *See id.,* p. 1.

[xviii] *See e.g.,* United States-Singapore Joint Statement on Financial Services Data Connectivity, at: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity;

[xix] *See id.,* USMCA Art. 17.2.1; US-Japan FTA Art. (PPC).

[xx] *See* Global Data Alliance, *Cross-Border Data Transfers and Innovation* (2021), at https://globaldataalliance.org/downloads/04012021cbdtinnovation.pdf

[xxi] *See generally,* BSA, *Moving to the Cloud – A Primer on Cloud Computing* (2018), at https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf.

[xxii] *See id.,* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (2020), at https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf; *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (2020), at https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf
Global Data Alliance, *Cross-Border Data Transfers and Supply Chain Management* (2021), at https://globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf

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

[xxiv] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.
[xxv] *Ibid.*
[xxvi] *Ibid.*
[xxvii] With COVID-19, these trends have become even more pronounced. *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf (showing that before COVID-19, 5–15 percent of US employees worked remotely; as of mid-2020, more than 50 percent of US employees do); Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (Sept. 2020), https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf (showing that remote health services are expected to grow by 700 percent by 2025, and some regions have seen even more rapid growth—up to 40-fold—for non-urgent telemedicine visits).
[xxviii] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[xxix] For example, governments should adopt pre-publication and final publication processes that specify implementation timelines, how various substantive concerns are addressed, the evaluation of evidence and expert input, and alternatives or other steps taken to mitigate negative impacts of the measure. *See e.g.,* USMCA Arts. 28.9 and 28.11.
[xxx] For example, governments should seek out the best reasonably obtainable information relevant to the proposed policy, be transparent regarding information sources and any significant assumptions, and use sound statistical methodologies in analyzing that information. *See e.g.,* USMCA Art. 28.5.
[xxxi] For example, governments should adopt procedural safeguards to ensure that any proposed measure that would impact cross-border data transfers is well-informed through input from experts, interested stakeholders, and the public. Such safeguards include:

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

See e.g., USMCA Arts. 28.7, 28.9, and 28.10.
[xxxii] For example, governments should offer a retrospective review mechanism that allows for future enhancements or revisions of the measure, including from the perspective of cross-border data policy. The mechanism should permit the government to evaluate:

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

See e.g., USMCA Art. 28.13.
[xxxiii] Commentary on good regulatory practices in relation to cross-border data policy includes: OECD, *Trade in the Digital Era* (2019), http://www.oecd.org/going-digital/trade-in-the-digital-era.pdf; World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, White Paper (2020), p. 18 https://www.jmfrri.gr.jp/content/files/Open/Related%20Information%20/WEF_May2020.pdf ("[P]olicy-makers should ensure that domestic measures affecting data are enacted in a transparent manner that allows opportunities for broad stakeholder input; are evidence-based and consider the technical and economic feasibility of requirements; require the publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and are targeted and proportionate, and restrict trade as little as possible."); UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (2016), at: https://unctad.org/system/files/official-document/dtlstict2016d1_summary_en.pdf (recommending that the impact on smaller businesses be assessed with respect to proposed data protection legislation and data flow restrictions); Indian Council for Research on International Economic *Relations, Regulatory Burden on Micro, Small and Medium Businesses Due to Data Localisation Policies*, (Sept. 2019), at http://icrier.org/pdf/Regulatory-Burden.pdf; OECD, *Going Digital: Shaping Policies, Improving Lives* (2019), Molinuevo & Saez, Regulatory Impact Assessment Toolkit, The World Bank (2014), at: https://openknowledge.worldbank.org/bitstream/handle/10986/17255/9781464800573.pdf?sequence=1; ICTSD, Advancing Sustainable Development Through Services Regulation (2017)
[xxxiv] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[xxxv] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf

[xxxvi] *See e.g.,* OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Art. 12 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf ("Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.")
[xxxvii] *See* OECD, *Guidelines governing the protection of privacy and transborder flows of personal data*, Arts. 14-18 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[xxxviii] Ensuring continued benefits from cross-border data transfers depends on users' faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of cloud-based technologies, providers must be free to move data across borders in an efficient and commercially viable manner.
[xxxix] Users must be assured that governments and enterprises understand and properly manage the risks inherent in storing and running applications in the cloud. This requires implementing cutting-edge cybersecurity solutions without being required to use specific technologies.
[xl] Laws online must provide meaningful deterrence and clear causes of action to deal with online threats and cybercrime. Legal systems should provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud.
[xli] To date, many countries have made, or are negotiating, such commitments under international agreements, including under the United States-Mexico-Canada Agreement (USMCA), the US-Japan Digital Trade Agreement, the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CP-TPP), the Digital Economy Partnership Agreement (DEPA), the Australia-Singapore Digital Economy Agreement (DEA), the UK-Japan Comprehensive Economic Partnership Agreement, the US-Japan Digital Trade Agreement, and the WTO Joint Statement Initiative digital trade negotiations. This positive trend should continue.