GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

September 16, 2022

His Excellency Ambassador Rosan Perkasa Roeslani
Embassy of the Republic of Indonesia
2020 Massachusetts Ave NW
Washington, DC 20036

GDA Submission re IPEF "Early Harvest" on Trusted and Secure Cross-Border Data Flows

Dear Ambassador,

The Global Data Alliance[1] (GDA) congratulates the Republic of Indonesia on the conclusion of the Indo-Pacific Economic Framework (IPEF) Ministerial Meeting held on September 8-9, 2022. We introduce through this submission the GDA and our priorities for the IPEF.

I. Introduction

The GDA 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.[2] GDA member companies, which have headquarters and operations around the world, employ tens of millions of workers across the Indo-Pacific region, including in IPEF economies. GDA member companies are active in a broad array of sectors, including aerospace, agriculture, automotive, energy, electronics, finance, health, logistics, and telecommunications, among others. Data transfers and digital networks lie at the heart of the IPEF economy: They support jobs in every country, across every sector, and at every stage of the value chain in billions of transactions every day.

The GDA applauds IPEF economies for agreeing in the September 9 Ministerial Statement to "advancing inclusive digital trade by building an environment of trust and confidence in the digital economy; enhancing access to online information and use of the Internet; facilitating digital trade; addressing discriminatory practices; and advancing resilient and secure digital infrastructure and platforms." The GDA also welcomes IPEF economies' commitment to "work to promote and support, inter alia: (1) trusted and secure cross-border data flows; (2) inclusive, sustainable growth of the digital economy; and (3) the responsible development and use of emerging technologies."

The GDA also respectfully encourages IPEF economies to specifically include "trusted and secure cross-border data flows" (noted above) as part of "early harvest" negotiating outcomes – thus addressing the cross-border digital interests of all IPEF economies, their industries, and their workers, including in the automotive,[3] clean energy,[4] finance,[5] healthcare,[6] logistics,[7] telecommunications,[8] and tourism sectors.

II. Discussion

The GDA urges IPEF economies participating in the digital trade negotiations (*hereinafter "IPEF digital trade negotiators"*) to agree on an "early harvest" of cross-border data commitments.

A. Proposed Cross-Border Data Commitments in IPEF

Consistent with prior agreements among IPEF economies,[9] this "early harvest" should cover:

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

These commitments focus on the impact that data regulations may have on trade among IPEF economies, and do not prevent governments from enacting rules to promote data privacy, data security, or other policy goals. These commitments are also designed, as framed in the September 9 IPEF Ministerial Statement, to accommodate "the rapidly evolving nature of digital technology" as well as "flexibilities to achieve public policy objectives, including protecting the rights and interests of our diverse communities." This is because the commitments focus on the cross-border impacts of data regulations – rather than their substantive privacy, security, or other legal aspects.

To address the cross-border impacts of any data regulations that involve incidental restrictions on data transfers,[10] we urge IPEF digital trade negotiators to clarify that such data regulations:

- Be necessary to achieve a legitimate public policy objective;[11]
- Not be applied in a manner that would result in arbitrary or unjustifiable discrimination or a disguised restriction on trade;[12]
- Not impose restrictions on transfers that are greater than necessary;[13]
- Not improperly discriminate among different economic sectors;[14]
- Not discriminate against other IPEF-based service providers by modifying conditions of competition by treating cross-border data transfers less favorably than domestic ones;[15]
- Be designed to be interoperable with other IPEF members' legal frameworks to the greatest extent possible;[16] and
- Be developed in a transparent and accountable manner.

The bulleted list above reflects longstanding tenets of international law and practice, namely: (1) the freedom to pursue necessary public policy objectives; (2) the renunciation of discrimination against non-national persons, products, services, or technologies; (3) the commitment to minimize trade-restrictive effects; and (4) due consideration for trading partner laws.[17]

B. Other Topics that Implicate Cross-Border Data Transfers

While this submission focuses on the commitments regarding data transfers, localization, and customs duties above, several other IPEF provisions also implicate data transfers and digital trust. Among others,[18] these provisions relate to personal data protection and cybersecurity, as explained below.

- Data Transfers & Personal Data Protection: Cross-border transfer mechanisms may be necessary to ensure data is protected even if transferred across borders. Where appropriate, the IPEF could promote such mechanisms (such as standard contracts, binding corporate rules, certification mechanisms, etc.), that help ensure that data is protected even as it is transferred across borders. The IPEF could also promote cross-border interoperability among different countries' personal data protection rules through mechanisms such as the Global Cross-Border Privacy Rules Forum.

- Data Transfers & Cybersecurity: Data transfers help improve cybersecurity because they 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. Given the role of data transfers in promoting timely visibility and response to emergent cyberthreats, the IPEF could helpfully promote risk-based approaches that rely on internationally recognized standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.[19]

III. Conclusion

For the reasons explained above, we respectfully urge all IPEF digital trade negotiators to include the "trusted and secure cross-border data flow" priorities from the September 9 IPEF Ministerial Statement among a package of "early harvest" digital outcomes. These "early harvest" outcomes should address, at a minimum, data transfers, localization mandates, and customs duties on electronic transmissions. Permitting unnecessary cross-border data restrictions to persist and proliferate across the Indo-Pacific region is incompatible with the potential of the IPEF framework to bind Indo-Pacific economies more closely together. Such restrictions impose significant costs on IPEF governments, workers, consumers, and enterprises – exacerbating digital fragmentation and the digital divide. Failing to address this economic and policy challenge would be a significant missed opportunity and would result in an agreement that would likely lack commercial significance or support from many industry and stakeholder groups.

The Global Data Alliance welcomes the opportunity to provide this submission and we look forward to continuing to work with you. Please let us know if you have any questions or comments.

Sincerely yours,

Joseph Whitlock

Joseph P. Whitlock
Executive Director
Global Data Alliance
josephw@bsa.org

[1] For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org/

[2] While Alliance member companies have a range of interests in the IPEF negotiations, this submission focuses exclusively on the cross-border data aspects of the negotiations.

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

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

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

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

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

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

[9] These commitments should be built on prior agreements involving IPEF Parties. These agreements include the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the Australia-Singapore Digital Economy Agreement (DEA), the Digital Economy Partnership Agreement (DEPA), the UK-Japan Economic Partnership Agreement, as well as the United States-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement, which contain the most advanced cross-border data provisions in any agreement.

[10] As connectivity and data have become integrated into every aspect of our lives, data-related regulation has become common in many areas: data privacy, cybersecurity, intellectual property, online health services – to name a few. Globally, the number of data regulations grew by over 800% between 1995 and 2015, and exceeds 250 today. *See* OECD, Trade and Cross-Border Data Flows, OECD Trade Policy Papers (2019), at: https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1636811939&id=id&accname=guest&checksum=4D81CCF1C6E59168A9C5AE0E43F3F9FB

[11] *See e.g.,* US-Japan DTA Art. 11.2; USMCA Art. 19.11.2.
[12] *See e.g.,* US-Japan DTA Art. 11.2(a); USMCA Art. 19.11.2(a).
[13] *See e.g.,* US-Japan DTA Art. 11.2(b); USMCA Art. 19.11.2(b).
[14] *See e.g.,* US-Japan DTA Art. 12-13; USMCA Chapter 17.
[15] *See e.g.,* US-Japan DTA Art. 11, footnote 9; USMCA Art. 19.11, footnote 5.
[16] *See e.g.,* US-Japan DTA Art. 15.3; USMCA Art. 19.8.4, 19.8.6.

[17] In the WTO context, these tenets – which trace back to the 1947 General Agreement on Tariffs and Trade – now apply to all multilateral trade rules, including those relating to goods, services, investment, technical regulations, and customs procedures. In the same spirit, IPEF digital trade negotiators should explicitly extend these core tenets to trade rules relating to the cross-border movement of data.

[18] Other topics that implicate data transfers and digital trust include:

- Data Transfers & Mandates to Force Technology Transfer or Source Code Disclosure: Data transfers enabled by software are critical to economic development. Unfortunately, some countries mandate involuntary access, transfer, or disclosure of proprietary source code as a condition of market access or for other improper purposes. While a regulatory body should be free to require an entity to make available source code for a specific investigation, enforcement action, or judicial proceeding, governments should not force technology transfer or source code disclosure for industrial policy, industrial espionage, cyber-exfiltration, or other improper purposes. Such measures not only increase the risk of malicious cyberactivity, but also discourage companies from providing cross-border access to their technologies or engaging in beneficial data transfers. By prohibiting such mandates, IPEF can continue to encourage cross-border access to technology.

- Data Transfers & Data Analytics: Recognizing that data transfers and the consolidation of data sets across borders are critical to data analytics and AI tools, IPEF provisions could helpfully promote AI risk management best practices, which are more compatible with the responsible application of these tools to data sets consolidated across borders than top-down restrictions that fail to acknowledge the rapidly

evolving nature of digital technology. Data transfers are integral to every stage of the AI life cycle, from the development of predictive models to the deployment and use of AI systems. The data used in AI systems often originates from many geographically dispersed sources, making it imperative that data can move freely and securely across borders. To secure for themselves the insights and other benefits that AI systems can provide, IPEF economies should agree to the responsible and secure cross-border movement of data for analytics and AI purposes.

- Data Transfers & Technical Barriers to Digital Trade: International standards development organizations (SDOs) convene companies from across the region to voluntarily contribute their innovations to the development of new international technology standards. Cross-border data transfers and technology access lie at the heart of this beneficial process. Unfortunately, technical regulations and mandatory national standards are sometimes misused (often in conjunction with data restrictions) to discriminate against non-national persons and technologies. By supporting the development and adoption of voluntary, internationally recognized standards, IPEF could help avoid the creation of new cross-border digital barriers.

[19] 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. When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities. *See generally,* BSA, *Moving to the Cloud – A Primer on Cloud Computing* (2018), at https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf

Annex I

Evidentiary Support for IPEF Cross-Border Data Commitments

To deliver on IPEF's promise of shared Indo-Pacific prosperity and economic opportunity, it is critical that the IPEF contain cross-border data commitments that can help all Parties benefit from cross-border access to information, knowledge, and digital tools. There is widespread evidence of these benefits, some of which is summarized below.

Data Transfers & Economic Growth: Cross-border data transfers – valued in the trillions of dollars[1] – benefit regional economic growth. The World Bank's 2020 *World Development Report* found that, "[c]ountries 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."[2] Local enterprises rely on data flows to drive quality, reach international customers, achieve economies of scale, and improve output,[3] often benefiting from cross-border access to tailored data-enhanced analytics and insights.[4] Cross-border data commitments can promote economic growth and job creation among IPEF economies.

Data Transfers & Manufacturing: Cross-border data transfers are especially beneficial to manufacturing industries, which depend on access to international supply chains, and which increasingly integrate Internet-of-Things (IoT) technologies on the shop floor and across assembly lines. It has been estimated that 75% of the value of data transfers accrues to manufacturing and other industries.[5] Conversely, data restrictions are harmful in this area. For example, a 2021 GSMA study conducted in three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on IoT applications and machine-to-machine (M2M) data processing could result in: (a) loss of 59-68% of their productivity and revenue gains; (b) investment losses ranging from $4-5 billion; and (c) job losses ranging from 182,000-372,000 jobs.[6] Cross-border data commitments can promote manufacturing across the IPEF region.

Data Transfers & Services: As services are increasingly enabled by digital means, cross-border data transfers have increased in importance. 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. … Developing countries ... accounted for 29.7% of services exports in 2019."[7] Cross-border data commitments can help support the growth of services across the region.

Data Transfers & Trade Facilitation: Cross-border technology access and data transfers also reduce supply chain-related transaction costs.[8] One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.[9] 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%.[10] Cross-border data commitments in IPEF can help promote these efficiencies.

Data Transfers & Sustainable Agriculture: Cross-border access to green technologies, satellite-based data, and other information helps small-scale agricultural producers improve crop yields; mitigate crop risks (including losses from pests, disease, and weather-related events); reduce arbitrage by middlemen (up to 70 percent of smallholder production value is captured by intermediaries); and promote sustainability (agriculture accounts for 70 percent of water use, while one third of global food production is either lost or wasted).[11] Cross-border data commitments can help promote uptake of sustainable agricultural practices and technologies across the region.

Data Transfers & Sustainable Economic Development: Analyses by development banks consistently show that cross-border access to technology and data transfers promote sustainable economic growth. For example, there remain over 2.5 billion unbanked people worldwide, many living in remote locations lacking physical banking infrastructure.[12] The US Agency for International Development (USAID) estimates that, by enabling digital financial services that leverage cross-border data, the GDP of emerging economies could increase by more than $3.5 trillion, or 6 percent, by 2025.[13]

Unfortunately, some Indo-Pacific economies are erecting costly data transfer restrictions vis-à-vis one another.[14] As UNCTAD has explained, such "digital fragmentation":

> reduces market opportunities for domestic MSMEs to reach worldwide markets, [and] ... reduces opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation. ... [M]ost small, developing economies will lose opportunities for raising their digital competitiveness.[15]

Economic development depends upon cross-border access to knowledge, digital tools, and commercial opportunities. Cross-border data commitments in IPEF can help promote such access.

Data Transfers & 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, as discussed above.[16]

Data Transfers & 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.[17] When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.[18]

Data Transfers & 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." Accordingly, regulatory authorities in many countries actually encourage the responsible transfer of data across borders. Likewise, data transfers are critical to other public policy priorities, including anti-money laundering; anti-corruption; and other legal compliance objectives.[19]

Data Transfers & Fraud Prevention: Prohibitions on cross-border data transfers in respect of financial data can have significant negative impacts on the effectiveness of fraud prevention and mitigation tools. 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.

Data Transfers & 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.[20]

Data Transfers & 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.[21]

Data Transfers & 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

Data Transfers & 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.

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.[22]

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.[23] 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.[24] Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.[25] The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance.[26] Many Regional Trade Agreements (RTAs) reflect this presumption.[27]

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;[28]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[29]
- 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;[30] and
- Include other procedural safeguards and due process.[31]

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.[32]

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.[33]

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[34] 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.[35]

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.[36] 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,[37] security,[38] and safety.[39] 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.[40]

---

[1] Global Data Alliance, *Cross-Border Data Transfers - Facts and Figures* (2020), at: https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf

[2] World Bank, World Development Report (2020), at: https://www.worldbank.org/en/publication/wdr2020 . Conversely, the World Bank also found that, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies..."

[3] 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) growth-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.

[4] Local enterprises face competitive harm if they are deprived of the insights that come from consolidating local data sets within larger regional or global data sets for purposes of data analysis. *See generally,* BSA, *Understanding Artificial Intelligence* (2017), at: https://www.bsa.org/sites/default/files/2019-03/BSA_2017UnderstandingAI.pdf ; BSA, *What's the Big Deal with Data* (2017), at: https://data.bsa.org/; BSA, *Artificial Intelligence in Every Sector* (2019), at:

https://www.bsa.org/sites/default/files/2019-03/BSA_2018_AI_Examples.pdf

[5] *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

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

[7] World Economic Forum, Paths Towards Free and Trusted Data Flows (2020). Conversely, 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." World Bank, *World Development Report – Data For Better Lives* (2021), at: https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf

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

[9] Micro-Revolution: The New Stakeholders of Trade in APAC, Alphabeta, 2019.

[10] 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

[11] *See e.g.,* Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021); Every Sector Is a Software Sector: Agriculture, https://software.org/wp-content/uploads/Every_Sector_Software_Agriculture.pdf; World Bank, *Agriculture and Food* (2020), https://www.worldbank.org/en/topic/agriculture/overview; IDB Climate Smart Agriculture, *Thematic Paper: Climate-Smart Agriculture* (Revised Version), p. 5, http://www.iadb.org/document.cfm?id=EZSHARE-1914875107-52. The IDB explains the underlying challenge that cross-border access to technologies and export markets can help ameliorate: "Smallholders typically capture a low share of the final value of its products and encounter non-transparent commercialization markets and difficulties in buying inputs and selling their products at fair prices. On top of that, small farm holders typically face limited access to export to new markets and unfavorable prices in international trade, and they are particularly vulnerable to volatility in commodity prices."

[12] USAID, US Global Development Lab website, available at: https://www.usaid.gov/digital-development/digital-finance

[13] *See* US Agency for International Development, Digital Strategy 2020-2024 (2020), at: https://www.usaid.gov/sites/default/files/documents/15396/USAID_Digital_Strategy.pdf; *see also See* Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021). Technologies that leverage data transfers help increase access – particularly as 95% of the world's population is already covered by mobile broadband networks and as new low-earth orbit satellite technologies bring connectivity to previously unserved communities. *See e.g.,* Ericsson, *Ericsson Mobility Report* (November 2019), at: https://www.ericsson.com/en/mobility-report/reports/november-2019; Global Data Alliance, *Cross-Border Data Transfers & Telecommunication Network Technologies* (2021), at: https://globaldataalliance.org/wp-content/uploads/2021/10/10042021cbdttelecom.pdf

[14] *See e.g.,* USTR, *2021 National Trade Estimate Report on Foreign Trade Barriers* (March 2021), at: https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf

[15] UNCTAD, *Digital Economy Report* (2021), at: https://unctad.org/system/files/official-document/der2021_en.pdf

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

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

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

[19] *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

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

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

[22] *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
[23] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.
[24] *Ibid.*
[25] *Ibid.*
[26] 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).
[27] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf
[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] 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)

[33] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf

[34] Global Data Alliance, *Dashboard - Trade Rules on Data Transfers* (2020), https://www.globaldataalliance.org/downloads/gdadashboard.pdf

[35] *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.")

[36] *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

[37] 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.

[38] 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.

[39] 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.

[40] 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.