Comments to the People's Republic of Bangladesh on
The Cross-Border Policy Implications of the Draft Data Protection Act of 2022

September 2022

The Global Data Alliance[1] ("Alliance" or "GDA") welcomes the opportunity to share its views on the Draft Data Protection Act of 2022. The GDA supports Bangladesh's goals of improving standards of data protection in Bangladesh, including by conferring on data subjects rights that align with those found in the EU General Data Protection Law. However, to avoid unintended harms, the GDA recommends that Bangladesh explore alternative approaches to the cross-border data restrictions and data localization mandates found in the Act.

In the Executive Summary, this submission contains an introduction and recommendations. In the Discussion, this submission identifies: (A) the cross-border data restrictions found in the Data Act that are of concern; (B) general concerns regarding those restrictions; and (C) specific concerns regarding those restrictions. Finally, the submission also includes two Annexes, which describe: (1) economic and policy impacts of the Act's cross-border data restrictions; and (2) the GDA cross-border data policy principles.

Executive Summary

I. Introduction

The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. 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 Bangladesh, collectively investing millions of dollars and supporting thousands of jobs. GDA member companies are active in Bangladesh in the aerospace, automotive, consumer goods, electronics, energy, financial services, health, media, supply chain, and telecommunications sectors. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output.[2]

GDA members share a deep and long-standing commitment to promoting data security and protection across technologies and business models. A forward-leaning policy on cross-border data transfers, which is interoperable with international frameworks, is a particularly effective tool to aid government efforts to support data protection, increase employment, and create other economic and societal benefits.

The GDA is concerned that the Act's data localization mandates, data transfer restrictions, and related provisions will impede Bangladesh's stated goals and will produce significant unintended consequences. We respectfully recommend that the Act be revised to adopt robust and rigorous data protection standards that promote privacy and security while allowing enterprises in Bangladesh to benefit from cross-border access to best-in-class cloud-delivered technology and while allowing citizens to benefit from economic and educational opportunities available online and across borders. In particular, we respectfully recommend that Bangladesh explore alternative approaches to the cross-border data restrictions and data localization mandates found in the Act, and to evaluate the other recommendations suggested herein.

II. Recommendations

For the reasons elaborated in this submission, GDA respectfully makes the following recommendations regarding Articles 42 and 43 of the Data Protection Act.

- Revise Article 42 to eliminate the requirements for exclusive storage ("shall only be stored in Bangladesh") of sensitive data, user generated data, and classified data. Instead, we respectfully submit that Article 42 should be revised to permit storage outside of Bangladesh, provided that the data is stored in a way that mitigates the risk of cybersecurity threats and consistent with Bangladesh legal standards.

- Amend the outright prohibition in Article 42 on "[any] other state's court, law enforcing agency or authority" having jurisdiction over, or access to, data generated in Bangladesh. As explained below, if enacted, this prohibition would disqualify Bangladesh from participating in international treaties or agreements regarding mutual legal assistance and access to evidence in civil, commercial and other matters, such as the Hague Evidence Treaty. Instead, we respectfully submit that Article 42 should permit mutual legal assistance and cross-border access to evidence by Bangladeshi and foreign authorities, consistent with international law and practice and/or specific agreements between Bangladesh and foreign authorities.

- Amend the provisions in Article 43 that only recognize consent or *ad hoc* governmental approvals as a basis for transferring certain types of data. We respectfully recommend that Article 43 be revised to recognize additional bases for international data transfers, including binding corporate rules, international trustmarks, regional certifications, and contractual arrangements. These mechanisms are incorporated in other global data protection frameworks to promote cross-border data flows, including the APEC CBPR and PRP frameworks, the EU GDPR, Japan's APPI, ASEAN Model Contractual Clauses[3] and other ongoing work under the ASEAN Cross Border Data Flows Mechanism.[4]

- Add additional provisions to Article 43 to highlight the obligations of companies (both data transferor and recipient) to protect data regardless of its location of storage and recognize that the commitments reflected in these provisions are independent bases for transferring data. As noted in the discussion below, this approach would align with the accountability principle that has been implemented in data protection laws worldwide.

- Narrow the scope and categories of data types that are covered by the Act. The Act currently covers a wide range of personal and non-personal data, including user-generated data, sensitive data, and classified data. We respectfully recommend that the Act be revised to focus specifically on personal data, rather than including such a wide scope of non-personal data.

Discussion

In the following discussion, we introduce: (A) the cross-border data restrictions of concern; (B) general concerns; and (C) specific concerns. We also include two Annexes, which address: (1) economic and policy impacts; and (2) the GDA cross-border data policy principles.

I. Cross-Border Data Restrictions in the Act

Under the heading, "Data Storage and Transfer Related Provisions," Chapter X of the Act states as follows:

> **42. Storage of sensitive data, user generated data and classified data.** (1) Sensitive data, user generated data and classified data shall only be stored in Bangladesh and no other state's court, law enforcing agency or authority other than the courts, law enforcing agencies or authorities of Bangladesh shall have jurisdiction over such data.
>
> **43**. **Provision regarding data transfer mentioned in section 42**. (1) Any data under section 42 that is specified, from time to time by general or special order, by the Government as classified data, shall not be transferred to a place or system outside Bangladesh without prior authorisation of the Government.
>
> (2) Notwithstanding anything contained in sub-section (1) or any other provisions of this Act-
>
> (a) the sensitive data of a data-subject and any other data, including user-generated data, with his consent,
>
> (b) for the purpose of maintaining international relations, cross-border business, immigration or any other data as specified, from time to time, by the Government, may be transferred to any state or organisation outside Bangladesh or any international organisation.
>
> (3) The Director General shall be notified in a manner, as may be prescribed by the rules, regarding any data transfer under this section to any other state or international organisation outside of Bangladesh

II. General Comments on Cross-Border Restrictions in the Act

The GDA has several general and specific concerns regarding Chapter X of the Act. The GDA offers the following general comments:

(1) The Chapter X cross-border restrictions would threaten Bangladesh' ecosystem for software and technology start-ups, and its ability to attract investment and to compete with or keep abreast of peer nations. For example, based in part on concerns voiced by India's indigenous technology start-up community, the Indian government has withdrawn its own plans to mandate data localization and data transfer restrictions for non-personal data. This policy change will benefit Indian enterprises and promote ongoing investment in India's software and technology sector. Conversely, by imposing restrictions that make it more difficult to engage in Bangladesh in cross-border software development and technology transfer, Bangladesh risks hobbling its own indigenous enterprises and making itself less attractive (in both absolute and relative terms) to foreign investment in software development and other emerging technologies. Avoiding the restrictions outlined in Chapter X of the Act would help Bangladesh avoid this negative outcome.

(2) The Chapter X restrictions would threaten to isolate Bangladesh economically from its regional and global partners. Data transfers support shared economic prosperity. Cross-border access to marketplaces, purchasers, suppliers, and other commercial partners allow Bangladesh enterprises in all sectors to engage in mutually beneficial international transactions with

foreign enterprises. The restrictions found in Chapter X of the Act jeopardize these benefits by exacerbating so-called "digital fragmentation" – impeding access to knowledge, digital tools, and commercial opportunities. 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." [5]

However, by avoiding the restrictions outlined in Chapter X of the Act, Bangladesh would be better able to secure the benefits of cross-border innovation and economic development.[6]

(3) The Chapter X restrictions would also threaten Bangladesh' ability to participate in and benefit from regional trade initiatives, such as the Indo-Pacific Economic Framework (IPEF). Provisions on cross-border data transfers, data localization, digital customs duties, cybersecurity, and personal data protection are core pillars of the IPEF trade pillar. Those provisions will be based on standards found in the US-Japan Digital Trade Agreement (USJDTA), the Australia-Singapore Digital Economy Agreement (DEA), the Singapore-Korea Digital Partnership Agreement (DPA), the Digital Economic Partnership Agreement (DEPA), the US-Mexico-Canada Agreement, and the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP), among others. Unfortunately, the restrictions outlined in Bangladesh Data Protection Act would be incompatible with the aforementioned provisions in each of the named agreements. By avoiding the restrictions outlined in Chapter X of the Act, Bangladesh would also avoid disqualifying itself *ab initio* from participating in the IPEF trade pillar negotiations on cross-border data matters.

(4) The Chapter X restrictions do not account for prevailing international legal practice relating to the cross-border movement of data under the so-called "accountability principle." 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] By reflecting this foundational international principle in the Data Protection Act, Bangladesh will avoid unintended harms that would isolate and disconnect it from the legal frameworks of regional and global partners.

(5) The Chapter X restrictions do not advance – and would even undermine – the Act's stated objectives of improving data security and protection in Bangladesh. Cross-border data transfers help improve data security, allowing for real-time visibility and response to emergent cyberthreats, including malware, online fraud, and other criminal activity online. Imposing the restrictions found in Chapter X of the Act will impede the ability to respond to these threats to data protection – creating unintended data security vulnerabilities for Bangladesh.

III. Specific Comments on Cross-Border Restrictions in the Act

The GDA also offers the following specific comments on the restrictions found in Chapter X of the Act:

(6) The subject data categories ("sensitive," "classified," and "user-generated") go far beyond personal data, significantly expanding the scope of these provisions to non-various personal data types. The GDA is unaware of any other national law that imposes such restrictions on such a broader universe of data types. Bangladesh' departure from prevailing international practice creates significant risk of unintended consequences;[17]

(7) It would likely be technically impracticable or impossible to segregate the broadly construed data types identified in Chapter X from other data types, with the result that other data types (e.g., non-sensitive data, non-classified data, non-personal data, etc.) would also need to be localized. Again, the risk of unintended consequences is high.

(8) The strict localization requirements and transfer restrictions are contrary to prevailing international practice – and indeed appear to be significantly stricter than any other country's law, including China. For example, the *ad hoc* government authorization mechanism for transfers is unworkable and contrary to prevailing international practice, which provides for a range of transfer mechanisms including contractual arrangements, binding corporate rules, certification mechanisms, and so forth.[18] The exclusive reliance on *ad hoc* government approvals or consent as a basis for transfer under Article 43(2) also fails to reflect the range of alternative bases for processing and transfer; and

(9) The strict prohibition on foreign jurisdictional reach for any data generated in Bangladesh would also undermine the ability of Bangladesh to accede in the future to various international treaties relating to cross-border mutual judicial assistance, such as the *Convention on the Taking of Evidence Abroad in Civil or Commercial Matters*.[19] By disqualifying itself from participating in such treaties, Bangladesh would also make it more difficult for judicial or other governmental authorities in Bangladesh to gain access to relevant evidence or data in other countries.

The GDA elaborates on these and other points in Annex I, which details the unintended economic and policy risks created by Chapter X of the Act. The GDA urges Bangladesh to reconsider these problematic aspects of Chapter X, and respectfully submits that the GDA's Cross-Border Data Policy Principles may offer a more suitable policy approach that promotes data security and protection without sacrificing Bangladesh' economic and technological development. Reflecting the emerging international policy consensus focused on data transfers and built on a foundation of trust,[20] the GDA Policy Principles comprise six major pillars.

- Principle 1: Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders
- Principle 2: Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices
- Principle 3: Any rules impacting cross-border data transfers should be non-discriminatory
- Principle 4: Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary
- Principle 5: Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices
- Principle 6: Countries should work together to create trust-based frameworks that are interoperable and support the seamless and responsible movement of information across borders

IV. Conclusion

In conclusion, we respectfully recommend that Bangladesh remove the Act's data localization mandates and cross-border data transfer restrictions, and address other recommendations set forth in these comments. We appreciate the opportunity to share these views and hope that they will be helpful as Bangladesh considers its next steps on the Data Protection Act of 2022. Please do not hesitate to contact us with any questions regarding this submission.

Sincerely yours,

Joseph Whitlock

Joseph Whitlock
josephw@bsa.org

[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] The seamless transfer of data across international borders enables the deployment of modern and emerging technologies and services that underpin the economy, across all sectors and at the local, national, and international level. This includes technologies and services enabled by data transfers, such as AI-related data analytics and machine learning technologies, as well as cloud computing, blockchain, and new privacy-enhancing technologies. These technologies and services, which are often accessed across borders or rely on data transferred across borders (or both), support many important economic activities and priorities, including remote work and virtual collaboration, distance education, telemedicine, cybersecurity, fraud monitoring and prevention, anti-money laundering, investigation of dangerous counterfeit products, and a broad range of other activities relating to the protection of health, privacy, security, and intellectual property.

[3] ASEAN Model Contractual Clauses, https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

[4] ASEAN Cross Border Data Flows Mechanism, https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf

[5] UNCTAD, *Digital Economy Report* (2021), at: https://unctad.org/system/files/official-document/der2021_en.pdf
[6] As the WTO has stated, "for data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies." WTO, Government Policies to Promote Innovation in the Digital Age, 2020 World Trade Report (2020), at: https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20-0_e.pdf
[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] While the processing and transfer of sensitive information across borders may require enhanced data protection measures, a broad-brush approach to restrict the data transfers of sensitive information would disrupt services and manufacturing operations in Bangladesh, including for local enterprises seeking to reach overseas markets. The GDA is also concerned regarding the lack of clear definitions for restricted data categories ("sensitive data", "user generated data", "classified data"), and the lack of any clear relationship between the Act's purported data protection

objectives and these broad data categories. As a result, regulated entities will likely end up overclassifying non-personal and non-sensitive personal data as being covered by the Act, restricting cross-border commercial, innovation, and scientific opportunities.

[18] Many companies that operate internationally adhere to robust and secure data transfer mechanisms, which may include, where relevant, adequacy decisions, certifications, codes of conduct, binding corporate rules (BCRs), and standard contractual clauses (SCCs). Assuming that such working mechanisms have not already been established in Bangladesh law, we would recommend eliminating the data localization mandates and data transfer restrictions from the Act.

[19] *See e.g., Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters* (1970) at https://www.hcch.net/en/instruments/conventions/specialised-sections/evidence

[20] *See* Global Data Alliance, *Trends in International Negotiations regarding Cross-Border Data Transfers* (2020), https://www.globaldataalliance.org/downloads/06022020GDAInternationalNegotiations.pdf.

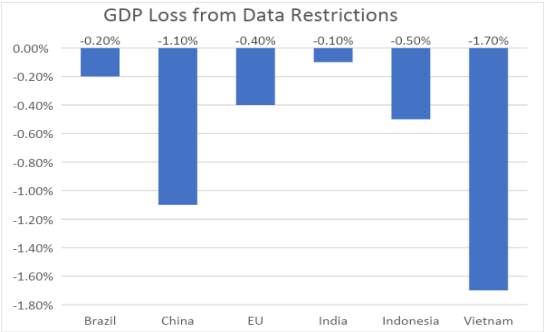
Annex I

Economic and Policy Impacts of the Act's Data Localization Requirements and Cross-Border Data Restrictions

The data localization requirements and cross-border data restrictions found in Chapter X of the Data Protection Act of 2022 will increase economic risks to Bangladesh, as outlined below.

- **Impact on Broader Economic Policy 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."[1]

  Cross-border data restrictions are sometimes justified as benefiting economic development. In fact, development benefits from an increase — not a decrease — in connectivity.[2] Self-isolating cross-border data restrictions hinder economic development, reduce productivity, deprive local enterprises of commercial opportunities, and depress export competitiveness, as reflected in the table analyzing GDP impacts below.[3]



- **Impact on Manufacturing Sector:** Cross-border data restrictions are particularly damaging to industries upon which Bangladesh depends, including manufacturing (e.g., textiles), agriculture, and logistics. It has been estimated that 75% of the value of data transfers accrues to such industries.[4] Bangladesh-origin textiles comprise nearly $7 billion in annual exports to the United States and nearly €15 billion in exports to the EU.[5]

- **Impact on Services Sector:** 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."[6] 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]

- **Impact on Global Market Access:** Data transfers are also critical to reducing the costs of reaching markets outside of Bangladesh. Data transfers not only enable local firms to find prospective customers in export markets; they 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]

- **Impact on IoT Economics:** 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 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.[11]

- **Impact on Enterprise Productivity:** Local enterprises rely on data flows to increase productivity, drive quality, and improve output in other ways.[12] Among other things, cross-border data restrictions impede access to tailored data-enhanced analytics and insights that help these firms compete.[13]

The cross-border data restrictions in the Act may also undermine public policy goals relating to the privacy, security, health, and welfare of persons in Bangladesh. We address these topics below.[14]

- **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.[15]

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

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

- **Impact on Fraud Prevention**: 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 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.

- **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.[20]

- **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 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.[21]

- **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.[22]

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.[23]

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.[24] 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.[25] Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.[26] The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance.[27] Many Regional Trade Agreements (RTAs) reflect this presumption.[28]

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;[29]
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;[30]
- 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;[31] and
- Include other procedural safeguards and due process.[32]

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.[33]

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.[34]

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[35] 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.[36]

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.[37] 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,[38] security,[39] and safety.[40] 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.[41]

---

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

[2] *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

[3] *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

[4] *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

[5] *See e.g.,* Office of the US Trade Representative, *US-Bangladesh Trade Relationship* (2019), at: https://ustr.gov/countries-regions/south-central-asia/bangladesh Top US imports from Bangladesh in 2019 were: woven apparel ($4.1 billion), knit apparel ($1.6 billion), headgear ($208 million), miscellaneous textile articles ($202 million), and footwear ($156 million); European Commission, *Bangladesh Trade Relationship*, at: https://ec.europa.eu/trade/policy/countries-and-regions/countries/bangladesh/

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

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

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

[12] 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.

[13] 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

[14] In addition to those topics discussed in the main text, A few other examples of unintended consequences resulting from extra-territorial effects and the scope of the DPA combined with the restrictions on cross-border transfers are discussed below:

- The current formulation of the restrictions on cross-border transfers read together with the wide jurisdiction of the DPA would mean that if an employee in the Bangladeshi operations of a global group of companies has remote view or edit access to data which is stored in a database offshore, that act of remote viewing or editing would then bring that offshore dataset within the scope of the DPA and trigger the requirement of on-soil storage of data. This is because the DPA applies to the processing (which includes retrieval and disclosure by transmission) of data within Bangladesh.
- It would be untenable to suggest that multinational companies store a copy of data of their offshore employees just because these companies are using support teams to process the data in Bangladesh. For example, if the employee in Bangladesh is working on back-office global HR data processing for all employees, the DPA would require the company to store all its global employees' data in Bangladesh. The DPA would also require a multi-national healthcare company which uses back-office IT or customer support teams to process health insurance claims of persons outside of Bangladesh, to store all records of insured persons in Bangladesh just because of the act of processing by those teams.
- It is uncertain whether the restrictions on cross-border transfers would apply to the local processing of classified data of foreign data subjects where the processing is done in Bangladesh or by a data controller in Bangladesh.
- For example, a data controller may utilise Bangladeshi operations to process health data or financial data of its foreign employees or customers (e.g., for internal back-office functions, customer support, documentation management purposes), and may need to process the data overseas to comply with legal requirements in a foreign country. As another example, account information for crediting salaries is needed for audit reasons in the country where the foreign employee is based. Such legal reporting requirements would require that financial data be transferred and processed offshore.
- A categorisation of financial data or health data as classified data would effectively prevent access to that data offshore for these purposes or requirements, even if measures may have been put in place to ensure such processing of data offshore has adequate safeguards.

Cross-border transactions by their very nature would involve offshore transfers of data, and the data would need to be processed for a range of legitimate reasons including accounting, tax, and audit reasons. For additional information, *see* https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf

[15] 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.

[16] *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.

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

[18] *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;

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

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

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

[22] *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

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

[32] 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.

[33] 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)

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

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

[36] *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.")

[37] *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

[38] 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.

[39] 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.

[40] 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.

[41] 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.