



## CROSS-BORDER DATA POLICY PRINCIPLES

A forward-leaning policy on cross-border data transfers is a particularly effective tool to aid policymaker efforts to drive innovation, increase employment, and rebuild economies.<sup>1</sup> Recognizing the relationship between digital connectivity and economic growth has helped drive numerous [international negotiations](#) in the area of cross-border data policy.<sup>2</sup>

However, digital protectionism and data mercantilism are also growing, often associated with measures that block the cross-border transfer of data and mandate data localization.<sup>3</sup> There remains persistent interest in these measures, even though their costs are borne primarily by the countries that adopt them.<sup>4</sup>

Building digital trust is an important factor in discouraging protectionist data policies. Governments should work toward legal frameworks that support a cross-border digital environment that is both open and secure, where [cross-border data transfers enhance online security and privacy](#), so that everyone can engage in remote interactions without fear of compromise.<sup>5</sup> And private enterprises must also do more. This may include developing or adopting codes of conduct, internal controls, or accountability mechanisms that advance data security and privacy.

For these reasons, it is of increasing importance that like-minded countries cooperate to strengthen and reinforce an international **policy consensus** that is focused on **data transfers** and built on a **foundation of trust**.<sup>6</sup> The Global Data Alliance sets out the following Cross-Border Data Policy Principles, identifying six major pillars that can strengthen this international consensus on data transfers.

### 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

“The digital economy is driven by massive cross-border information flows. Sharing data across borders allows business to access global market[s], interact with customers, communicate with suppliers and affiliates around the globe, and thereby increase efficiency and productivity.”

APEC, *Facilitating Digital Trade For Inclusive Growth* (2017)

## 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.<sup>7</sup>

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.<sup>8</sup> 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.<sup>9</sup> Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.<sup>10</sup> The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance.<sup>11</sup> Many Regional Trade Agreements (RTAs) reflect this presumption.<sup>12</sup>

#### Growing the Global Economy

**2.5 quintillion** data bytes  
are generated every day<sup>1</sup>

Data transfers contributed  
**\$2.8 trillion** to global GDP,  
growing 45x every ten years<sup>2</sup>

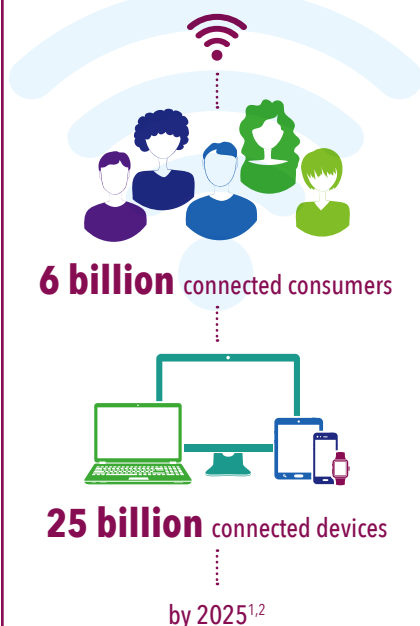
**60% of global GDP will be  
digitized** by 2022, with growth in  
every industry driven by data flows  
and digital technology<sup>3</sup>

<sup>1</sup> *World's Top Global Mega Trends to 2025 and Implications to Business, Society, and Cultures*, Frost & Sullivan, 2014.

<sup>2</sup> *Trade and Cross-Border Data Flows*, OECD, 2019.

<sup>3</sup> *FutureScape—Worldwide IT Industry 2019 Predictions*, IDC, 2018.

#### Connecting People to Economic Opportunities



<sup>1</sup> *The Mobile Economy 2020*, GSMA, 2020.

<sup>2</sup> *The Digitization of the World From Edge to Core*, IDC, 2018.

#### Benefitting All Sectors

**75% of the value of data  
transfers** accrues to traditional  
industries like agriculture,  
logistics, and manufacturing<sup>1</sup>



For SMEs in Asia—digital tools **reduce  
export costs by 82%, and  
transaction times by 29%**<sup>2</sup>

<sup>1</sup> *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*, McKinsey Global Institute, 2011.

<sup>2</sup> *Micro-Revolution: The New Stakeholders of Trade in APAC*, Alphabet, 2019.

“Cross-border data flows are especially important for micro, small and medium-sized enterprises (MSMEs), enabling a new breed of ‘micro multinationals’ which is ‘born global’ and is constantly connected. ... Better and faster access to critical knowledge and information also helps MSMEs overcome informational disadvantages, notably with respect to larger firms, reducing barriers to engaging in international trade and allowing them more readily to compete with larger firms.”

OECD, *Mapping Approaches to Data and Data Flows* (2020)

## 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;<sup>13</sup>
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;<sup>14</sup>
- 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;<sup>15</sup> and
- Include other procedural safeguards and due process.<sup>16</sup>

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.<sup>17</sup>

“Digital technologies and data profoundly affect international trade by reducing trade costs; facilitating the co-ordination of global value chains; diffusing ideas and technologies across borders; and connecting greater numbers of businesses and consumers globally. In particular, goods are increasingly bundled with services, and new and previously non-tradeable services are now traded across borders.”

OECD, *Digital Economy Outlook* (2020)

“ [A]pproximately 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.

WEF, *Paths Towards Free and Trusted Data Flows* (2020)

### 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.<sup>18</sup>

“ [F]or data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies. This may, at least in part, explain why binding rules on cross-border data transfers and localization restrictions have been introduced in a number of RTAs and have been discussed [at the WTO].”

WTO, *Government Policies to Promote Innovation in the Digital Age*, 2020 World Trade Report (2020)

## 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<sup>19</sup> 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.<sup>20</sup>

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.

“[C]ross-border data flows... allow companies not only to sell their goods and services, but also to coordinate their logistics and the activities of their subsidiaries and partner offices across the globe.... Indeed, the internet is now one of the most important business platforms for companies, domestically and internationally.”

WTO, *Towards a New Digital Era*, 2018 World Trade Report (2018)

Data transfers are critical to economic opportunity for all. For example:

Farmers rely on cross-border access to meteorological and market data to plant and harvest crops, and to find buyers for those crops in global markets

Workers and citizens depend upon data transfers for remote work, online education, and remote services (e.g., telemedicine)

Employers and employees rely on data transfers to collaborate in the research, design, engineering, manufacturing, marketing, and post-sale service of new products

Governments and enterprises rely on data transfers to manage risks relating to health, consumer protection, cybersecurity, anti-money laundering, and other policy priorities

GDA, *Jobs in All Sectors Depend On Data Flows* (2020); GDA, *Creating Jobs and Trust Across Borders in Every Sector* (2020)

## 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.<sup>21</sup> 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.

“Countries that impose local data storage and retention requirements to secure better [data] access for themselves can expect multinational businesses to stay away and other countries to retaliate. Similarly, countries that regulate data processing too rigidly and with specific restrictions on cross-border data transfers provoke reciprocal restrictions by other countries, resulting in reduced access to global data and technology, pressures for compromises in bilateral trade negotiations, and accumulating complexities. Cross-border data transfers require give and take.”

WEF, *A Roadmap for Cross-Border Data Flows* (2020)



“Data localization requirements can increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information. Data mobility in financial services supports economic growth and the development of innovative financial services and benefits risk management and compliance programs, including by making it easier to detect cross-border money laundering and terrorist financing patterns, defend against cyberattacks, and manage and assess risk on a global basis.”

*US-Singapore Joint Statement (2020)*

## 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,<sup>22</sup> security,<sup>23</sup> and safety.<sup>24</sup> 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.<sup>25</sup>

“A study conducted on three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on IoT applications and M2M data could cut 59-68% of their productivity and revenue gains. Such losses of competitiveness also lead to reductions of \$4-5 billion in investments and 182,000-372,000 jobs...”

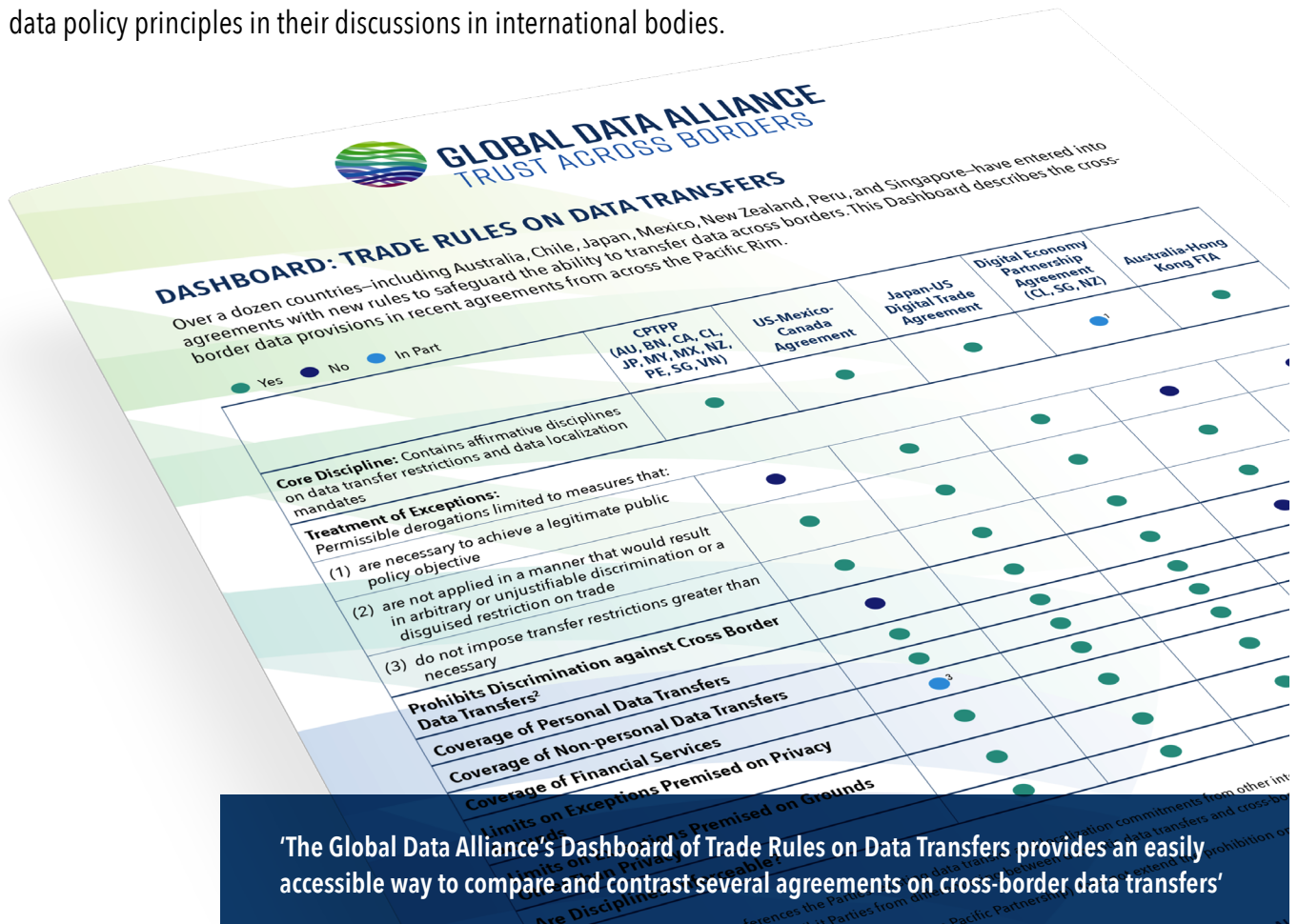
WEF, *Paths Towards Free and Trusted Data Flows* (2020)

“Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development. At the same time, we recognize that the free flow of data raises certain challenges. By continuing to address [these] challenges..., we can further facilitate data free flow and strengthen consumer and business trust.”

[G20 Ministerial Statement on Trade and Digital Economy \(2019\)](#)

## Conclusion

It is of increasing importance that like-minded countries cooperate to strengthen the pillars of an international **policy consensus** that is focused on **data transfers** and built on a **foundation of trust**. Advancing international policies on cross-border data transfers offer policymakers an effective tool to build digital trust and drive innovation, increase employment, and rebuild economies. We encourage policymakers to consider the foregoing cross-border data policy principles in their discussions in international bodies.



“Any future WTO JSI e-commerce” agreement should discipline unnecessary or discriminatory data localization mandates and data transfer restrictions. Any agreement should also be guided by principles of transparency and interoperability among legal frameworks; should apply across all economic sectors; and should require all countries to adopt or maintain legal frameworks to protect personal information.”

[Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in WTO Negotiations on E-Commerce, Statement by 78 Associations from Africa, Asia, Australia, Europe, and the Americas \(Jan. 26, 2021\)](#)



## ENDNOTES

- <sup>1</sup> The Global Data Alliance ([globaldataalliance.org](https://globaldataalliance.org)) 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 include BSA members and American Express, Amgen, AT&T, Citi, ITB, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, RELX, Roche, UDS, United Airlines, Verizon, Visa, and WD-40 Company. These companies are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. See Global Data Alliance, *About the Global Data Alliance* (2020), <https://www.globaldataalliance.org/downloads/aboutgda.pdf>.
- <sup>2</sup> See Global Data Alliance, *International Negotiations on Cross-Border Data Transfers & Data Localization* (2020), <https://www.globaldataalliance.org/downloads/06022020GDAlnternationalNegotiations.pdf>.
- <sup>3</sup> See e.g., Global Data Alliance, *Submission to USTR on National Trade Estimate of Foreign Trade Barriers* (2020), <https://www.globaldataalliance.org/downloads/10292020GDA2020NTESubmission.pdf>.
- <sup>4</sup> Severing or limiting connections to foreign markets through such self-imposed restrictions tends to hinder economic development, reduce innovation and productivity growth, and depress export competitiveness. Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, et al, *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE (2014), [https://ecipe.org/wp-content/uploads/2014/12/OCC32014\\_1.pdf](https://ecipe.org/wp-content/uploads/2014/12/OCC32014_1.pdf); Martina F. Ferracane, Janez Kren, and Erik van der Marel, *The Costs of Data Protectionism*, VOX (2018), <https://voxeu.org/article/cost-data-protectionism>; Martina F. Ferracane and Erik van der Marel, *Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?* ECIPE (2019), <https://ecipe.org/publications/do-data-policy-restrictions-impact-the-productivity-performance-of-firms-and-industries/>; Susan Lund and James Manyika, *Defending Digital Globalization*, McKinsey Global Institute (2017), <https://www.mckinsey.com/mgi/overview/in-the-news/defending-digital-globalization>; Anupam Chander and Uyên P. Lê, *Data Nationalism*, Emory Law Journal 64, No. 3 (2015), <https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/>.
- <sup>5</sup> See Global Data Alliance, *Position Paper on Cross-Border Data Transfers & Data Localization* (2020) <https://www.globaldataalliance.org/downloads/02112020GDACrossborderdata.pdf> (Cross-border data transfers foster online security and privacy by enabling cybersecurity tools to identify anomalies, divert potential threats, and patch vulnerabilities through global, real-time monitoring of traffic patterns and data exceptions. When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended security gaps and blind spots that criminals can exploit. Cross-border data transfers also foster compliance with regulatory requirements by firms engaged in services including transportation, logistics, and financial services).
- <sup>6</sup> See Global Data Alliance, *Trends in International Negotiations regarding Cross-Border Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/06022020GDAlnternationalNegotiations.pdf>.
- <sup>7</sup> 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>.
- <sup>8</sup> See Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), <https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf>.
- <sup>9</sup> *Ibid.*
- <sup>10</sup> *Ibid.*
- <sup>11</sup> 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).
- <sup>12</sup> Global Data Alliance, *Dashboard—Trade Rules on Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/gdadashboard.pdf>.
- <sup>13</sup> 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.
- <sup>14</sup> 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.
- <sup>15</sup> 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.
- <sup>16</sup> 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.
- <sup>17</sup> Commentary on good regulatory practices in relation to cross-border data policy includes: OECD, *Principles for Market Openness in the Digital Age*, Working Party Report, TAD/TC/WP(2018)17/FINAL (2018), [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP\(2018\)17/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)17/FINAL&docLanguage=En); Joshua Meltzer, *How APEC can address restrictions on cross-border data flows* (2021), [https://ab46bb92-a539-4d61-9a28-f77eb5f41c00.usfiles.com/ugd/ab46bb\\_830a70b4f8dc4508a38d3e480ffa9cb2.pdf](https://ab46bb92-a539-4d61-9a28-f77eb5f41c00.usfiles.com/ugd/ab46bb_830a70b4f8dc4508a38d3e480ffa9cb2.pdf); 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](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/dtstict2016d1\\_summary\\_en.pdf](https://unctad.org/system/files/official-document/dtstict2016d1_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).
- <sup>18</sup> Global Data Alliance, *Dashboard—Trade Rules on Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/gdadashboard.pdf>.

- <sup>19</sup> Global Data Alliance, *Dashboard—Trade Rules on Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/gdadashboard.pdf>.
- <sup>20</sup> 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](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.")
- <sup>21</sup> 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](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf).
- <sup>22</sup> 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.
- <sup>23</sup> 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.
- <sup>24</sup> 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.
- <sup>25</sup> 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 (CPTPP), 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.

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. BSA | The Software Alliance administers the Global Data Alliance.