GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

2 February 2023

**Comments to the United Kingdom on**
**Cross-Border Data Provisions in UK-Korea Trade Negotiations**

The Global Data Alliance[1] (GDA) congratulates the United Kingdom (UK) on its trade negotiations with the Republic of Korea (Korea). The GDA welcomes the forward-looking and innovative approach to cross-border data negotiating priorities reflected in the work of the UK Department for International Trade (DIT) and the UK Department of Culture, Media, and Sport (DCMS).[2] This submission urges the UK to continue providing for strong cross-border data commitments in its negotiations with Korea.

Among other things, we specifically urge the UK to secure robust commitments on data localization and cross-border data transfers of financial data, as recent Korean agreements (including the Korea-Singapore Digital Partnership Agreement) have fallen short of prevailing digital trade outcomes in comparable agreements such as the Australia-Singapore Digital Economy Agreement, the Japan-UK Comprehensive Economic Partnership Agreement, the Singapore-UK Digital Economy Agreement, and the Australia-UK Free Trade Agreement. The GDA will convey these same priorities to Korea's Ministry of Trade, Industry, and Energy (MOTIE).

## I. Introduction

The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA member companies employ tens of thousands of workers across the UK in digitally intensive industries. GDA member companies are active in a broad array of sectors, including aerospace, agriculture, automotive, energy, electronics, film, music, finance, health, logistics, retail and consumer goods, technology, and telecommunications, among others.

GDA members welcome the UK's proactive approach in working to ensure that the UK's FTA negotiations address the cross-border digital interests of all UK industries and their workers, including in the agriculture, automotive, clean energy, finance, healthcare and medical technology, logistics, media (including film, music and publishing), pharmaceutical, software, semiconductor, and telecommunications sectors. Digital networks lie at the heart of today's interconnected global economy: they support jobs across the UK in every sector, and at every stage of the value chain in millions of transactions every day.[3]

## II. Importance of Cross-Border Data in the UK-Korea Trade Negotiations

Developing strong cross-border data disciplines will be critical to the success of forthcoming UK-Korea trade negotiations.

Digitally delivered services, which depend upon cross-border data transfers, account for a high share of UK trade with around 79% of UK services exports to Korea, and 80% of services imports, being digitally delivered in 2020. A significant proportion of UK-Korea services trade Korea related specifically to the financial services sector.[4]

Similarly, cross-border data transfers play a crucial role in connection with bilateral investment flows. From 2011-2021, UK outward foreign direct investment (FDI) projects in Korea were concentrated (at 39% of all UK FDI in Korea) on "creative industries", "retail trade" and "ICT & electronics". Korean investment into the

UK is also dependent on cross-border data transfers, with 42 percent of Korea's FDI projects in the UK concentrated in "ICT & electronics", "financial services" and "environmental technology."[5] Notably, Korea itself has a strong interest in avoiding restrictions on financial data transfers, given the level of its investment in the UK financial sector.

As the UK has stated in connection with its trade negotiations with Korea's regional partners, such as Australia, Japan, and Singapore, critical priorities in these agreements include:

- Free and trusted cross-border data flows. Data flows are vital for the modern global economy, enabling everything from more efficient manufacturing and supply chains to effective maintenance of jet engines.
- Strengthening the UK's … financial services [sector] by ensuring data can flow freely without unjustified barriers and enhanced cooperation for innovative financial services.

## III. Proposed Commitments on Cross-Border Data and Digital Trust

As reflected in the attached Appendix, the GDA supports the UK working to ensure cross-border data outcomes in the Korea trade negotiations that are consistent with prior UK digital trade agreements, such as the UK-Singapore Digital Economy Agreement, including:

- Cross-Border Transfer of Information by Electronic Means: Across all sectors, including financial services, Parties shall not prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for business purposes.
- Location of Computing Facilities: Across all sectors, including financial services, Parties shall not impose requirements to use or locate computing facilities in their own territory as a condition for conducting business. GDA's draft provisions include illustrative examples of several types of localization measures that would breach this broader obligation.
- Custom Duties: Parties shall not impose customs duties on electronic transmissions.
- Cybersecurity Risk Management: Parties shall adopt frameworks to manage cybersecurity risk. In connection with certification requirements for cybersecurity, Parties shall refrain from data localization mandates or other measures that undermine cybersecurity.
- Personal Data Protection: Parties shall adopt a framework to protect personal information. Parties shall promote mechanisms to ensure interoperability of such legal frameworks, and to ensure that data can be transferred across borders.

In connection with the foregoing articles, the GDA seeks to reflect longstanding tenets of international law and practice, including: (1) the freedom of governments to pursue necessary public policy objectives; (2) the renunciation of discrimination against non-national persons, products, services, or technologies; (3) the commitment to minimize trade-restrictive effects; and (4) due consideration to principles of compatibility and interoperability with trading partner laws. We support the efforts of UK digital trade negotiators to explicitly clarify that these same core tenets apply to trade rules relating to the cross-border movement of data, including in the financial sector.

We address two specific issues in greater detail below – namely financial services data and cybersecurity certification mechanisms.

## IV. Financial Data Disciplines

Given that Korea's recent digital economy agreements not covered financial services data mobility as fully as other digital economy agreements involving the UK and the countries above, we stand ready to support both the UK and Korea in helping build a strong case for more ambitious outcomes on financial services data transfers and localization norms in the UK-Korea trade negotiations.

We are concerned that the Korea-Singapore Digital Partnership Agreement (KSDPA), which went into effect in late December 2022, excludes the financial sector from its prohibitions on computing facility localization does not apply with respect to a "financial institution" or a "financial service supplier of a Party."[6] This provision means that financial institutions and service suppliers from Singapore may be required to use or locate their computing facilities in Korea as a condition for conducting business in Korea, and vice versa.

Below we discuss the costs and risks associated with such an exclusion of the financial sector. We also discuss the lack of any demonstrated need for such an exclusion.

### A. Risks Associated with any Exclusion of the Financial Sector from Cross-Border Data and Data Localization Rules in the UK-Korea Negotiations

Excluding the financial sector from the data transfer and data localization rules in the UK-Korea negotiations would be highly disruptive, distortive, and costly.

Requiring financial institutions/service suppliers to localize their computing facilities and data may increase security and financial fraud risks. As the capabilities of malicious actors in cyberspace continue to evolve, investments in data security have increased. This is especially so for the financial sector, where the effects of a cyberattack can be devastating.

However, localization measures often compel financial institutions and service suppliers to use local data storage service providers in the country the imposes such measures. This by definition limits the options of such financial institutions and service providers when deciding where and with what entities they wish to entrust their data, including the option of using their own centralized data storage and processing centers, or those provided by third party service providers that may not have data centers in country. Local data storage service providers may not have the same security capabilities as global counterparts, many which invest enormous amounts of resources in their cybersecurity capabilities and constantly upgrade their security programs and controls to deal with the latest cyber threats.

Delays in uploading threat incident information to cybersecurity companies' global networks due to regional data restrictions could also expose customers in that region to new threats spreading from other parts of the world, reducing information privacy and security for those customers. For example, effective fraud mitigation as provided by banks, card networks and other players in the financial services sector demands sophisticated monitoring and rapid detection at the time of transaction to interpret and weigh the risk of fraud of each payment transaction as weighed by the facts of that payment transaction as against norms for all payment transactions and that account.

Fraud detection models are typically built on global transaction data or transaction data collected from multiple countries since fraud patterns are not limited by national boundaries. Fraud trends which appear in one region or country may apply in others as cardholders travel to different countries, cardholders transact online with merchants in different countries, and the perpetrators of fraud do not respect any national boundary lines. Thus, to build effective fraud models and to gain the necessary insights into fraudulent activity in order to help prevent them, these models must be built off of global or multi-country data sets, based both on the location of the merchant and the location of the cardholder.

Likewise, excluding the financial sector from cross-border data transfer and data localization disciplines would also limit the scope of information sharing across jurisdictions, undermining efforts from both financial institutions/service suppliers and regulatory authorities to combat money-laundering and financing of terrorism.

### B. Lack of Any Demonstrated Justification for Excluding the Financial Sector from Cross-Border Data and Data Localization Rules in the UK-Korea Negotiations

Excluding the financial from cross-border data transfer and data localization disciplines also appears to be unnecessary, given that numerous other agreements have allow for disciplines on data transfers and data localization, provided that financial regulatory authorities can be guaranteed immediate and ongoing access

to information of financial institutions and service suppliers, including information underlying their transactions and operations, to discharge their supervisory and monitoring duties.

Localization requirements in the financial sector are not necessary for regulatory oversight for several reasons. In a globalized economy, financial institutions and service suppliers often must provide services internationally to their customers in other countries, requiring the international transfer of significant amounts of financial data daily. Regulators have several mechanisms to ensure that they may maintain access to necessary data from financial institutions and service suppliers regardless of where the data may be stored, such as entering contractual agreements with financial institutions/service suppliers to have immediate and ongoing access to information processed or stored on computing facilities out of the country.

As a general principle, there is no reason to impose localization requirements on financial institutions/service suppliers if regulatory authorities have immediate and ongoing access to their data. This is the approach taken in prior UK agreements with other regional partners, which GDA strongly supports:

- These provisions typically state that neither Party shall require a financial institution/services supplier to localize their computing facilities and data, so long as financial regulatory authorities "have immediate, direct, complete and ongoing access" to the information processed or stored on computing facilities used by the financial institution/service supplier located out of the country.

- These provisions have also stated in the past that a Party may only impose localization measures on a financial service supplier if it is "not able to ensure appropriate access to information required for the purposes of financial regulation and supervision". The Article further requires the Party imposing the localization measure to: (1) provide the financial service supplier "a reasonable opportunity to remediate any lack of access to information"; and (2) to consult with the other Party's regulatory authorities before imposing the localization measure.

The United States-Singapore Joint Statement on Financial Services Data Connectivity[7] is also a useful reference point. While non-binding in nature, both countries agreed to:

- Ensure that financial service suppliers can transfer data, including personal information, across borders by electronic means if the activity is for the business of a financial service supplier.

- Oppose measures that restrict where financial data can be stored and processed as long as regulators have full and timely access to data needed for their regulatory and supervisory mandate.

- Ensure that financial service suppliers have the opportunity to remediate the lack of access to such data before being required to use or locate computing facilities locally.

## V. Cybersecurity Certification Disciplines

We also urge the UK to propose a slight expansion of the cybersecurity provision found in prior digital economy agreements. Specifically, we would propose that the UK include text prohibiting the inclusion in cybersecurity certification frameworks of data localization mandates, data transfer restrictions, corporate residency requirements or other restrictions that are often contrary to good cybersecurity practices. Cybersecurity certification requirements may increase risk when they contain elements that impair cross-border coordination or access to cybersecurity technologies, as well as cross-border visibility of the cybersecurity landscape generally and specific cybersecurity threats. Accordingly, we urge the UK and Korea to jointly commit that any cybersecurity certification standards and other measures shall treat service suppliers from other Parties no less favorably than domestic service suppliers, including in respect of the domicile, nationality, or degree of foreign affiliation or ownership of the service supplier; in respect of the country of origin of the technology; and in respect of the location of computing facilities and the cross-border transfer of information

## VI. Conclusion

We appreciate the opportunity to comment, and include with this submission two Appendices that are consistent with the positions outlined above:

- **Appendix I: Proposed Provisions on Cross-Border Data** and **Digital Trust**;
- **Appendix II: Economic Importance of Cross-Border Data in the UK-Korea Agreement**

We thank you for the opportunity to share these views. Please do not hesitate to contact us with any questions.

Sincerely yours,

*Joseph Whitlock*

Joseph Whitlock
Executive Director
Global Data Alliance

## Appendix I

## Provisions re Cross-Border Access to Information

**Article __: Supporting Cross-Border Access to Information**

The Parties recognize that the ability to access, store, process, and transmit information across borders supports:

(a) The legitimate policy objectives of Parties, including those relating to the protection of the environment, health, privacy, safety, security, and regulatory compliance;
(b) Sustainable economic development and shared economic prosperity, including through greater cross-border connectivity, including for Micro-, Small-, and Medium-Sized Enterprises;
(c) Financial inclusion and security, including for those lacking access to banking resources, as well as fraud prevention, anti-money laundering, and financial transparency;
(d) Healthcare delivery, research and development of new healthcare treatments, cross-border healthcare regulatory collaboration, and global medical humanitarian assistance;
(e) Scientific progress, including through cross-border access to knowledge and information, cross-border data analytics, and cross-border research and development (R&D) needed to develop technological solutions to meet global challenges;
(f) Cybersecurity, including through an enhanced ability to detect cybersecurity risks, respond to cybersecurity threats, and recover from cybersecurity incidents through real-time cross-border data access and visibility; and
(g) Climate change response, including through improved cross-border carbon emissions tracking and predictive climate modeling based on multi-regional data sets that can help communities to prepare for climate-related risks and identify mitigation and remediation strategies.

**Article ___: Cross-Border Transfer of Information by Electronic Means**

1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.

2. In the case of transfers of financial information, no Party shall prevent a covered person from transferring information, including personal information, into and out of the Party's territory by electronic or other means when this activity is for the conduct of business within the scope of the license, authorization, or registration of that covered person.

3. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade;[8] and
(b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.

**Article ___: Location of Computing Facilities**

1. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

2. In the case of financial information, no Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory.[9]

3. Examples of measures that would breach paragraphs 1 and 2 include those that:

(a) require the use of computing facilities or network elements in the territory of a Party;

(b) require the use of computing facilities or network elements that are certified or approved in the territory of a Party;

(c) require the localization of information in the territory of a Party;

(d) prohibit storage, access, or processing of information outside of the territory of the Party;

(e) provide that the use of computing facilities or network elements in its territory, or the storage or processing of information in its territory, is a condition of eligibility relating to:

(i) technical regulations, standards, or conformity assessment procedures;[10]

(ii) licensing requirements and procedures;[11]

(iii) qualification requirements and procedures;[12] or

(iv) other governmental measures that affect trade; or

(f) condition market access upon the use of computing facilities or network elements in its territory or upon requirements to store or process information in its territory.

4. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade;[13] and

(b) does not impose requirements that are greater than are necessary to achieve the objective.

**Article __: Customs Duties**

No Party shall impose customs duties[14] on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.

## Provisions re Digital Trust

**Article __ : Supporting Digital Trust**

The Parties place a high value on building and strengthening public trust in the digital environment, and in that regard, recognize that:

1. Promoting personal information protection can help enhance confidence in digital trade and can facilitate the delivery of economic and social benefits to citizens;
2. Promoting interoperability among legal frameworks for personal information protection is important to facilitate cross-border information transfer while protecting digital trust;
3. Protecting cybersecurity through cyber-incident detection, response, and recovery depends in part upon effective cybersecurity risk management and real-time cross-border access to cybersecurity-related technologies and cyber threat indicators; and

**Article __: Protecting Personal Information**

1. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade.[15] In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

2. The Parties recognize that pursuant to paragraph 1, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.

3. Each Party shall adopt or maintain non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.

4. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:

    (a) a natural person can pursue a remedy; and

    (b) an enterprise can comply with legal requirements.

5. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development of mechanisms to promote compatibility and interoperability between these different approaches. These mechanisms include:

    (a) broader international and regional frameworks, such as the APEC Cross Border Privacy Rules;

    (b) mutual recognition of comparable protection afforded by their respective legal frameworks, national trustmarks or certification frameworks; or

    (c) other avenues of transfer of personal information between the Parties.

6. The Parties shall endeavor to exchange information on how the mechanisms in paragraph 6 are applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.

7. The Parties recognize that the APEC Cross Border Privacy Rules System and/or APEC Privacy Recognition for Processors System are valid mechanisms to facilitate cross-border information transfers while protecting personal information.

8. The Parties shall endeavor to jointly promote the adoption of common cross-border information transfer mechanisms, such as those found in the Global Cross Border Privacy Rules Forum.

**Article ___: Managing Cybersecurity Risk**

1. The Parties shall endeavor to:

    (a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and

    (b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity incidents.

3. Given that cybersecurity certification requirements and other measures may increase risk when they contain elements that impair cross-border coordination or access to cybersecurity technologies, each

Party's cybersecurity certification standards and other measures shall treat service suppliers from other Parties no less favorably than domestic service suppliers, including in respect of the domicile, nationality, or degree of foreign affiliation or ownership of the service supplier; in respect of the country of origin of the technology; and in respect of the location of computing facilities and the cross-border transfer of information.

## Appendix II

## Evidentiary Support for UK-Korea Cross-Border Data Commitments

To deliver prosperity and economic opportunity for the UK and Korea alike, it is critical that the revised UK-Korea trade agreement contain cross-border data commitments that can help all Parties benefit from cross-border access to information, knowledge, and digital tools. There is widespread evidence of these benefits, some of which is summarized below.

**Data Transfers & Economic Growth**: Cross-border data transfers — valued in the trillions of dollars[1] — benefit regional economic growth. The World Bank's 2020 *World Development Report* found that, "[c]ountries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."[2] Local enterprises rely on data flows to drive quality, reach international customers, achieve economies of scale, and improve output,[3] often benefiting from cross-border access to tailored data-enhanced analytics and insights.[4] Cross-border data commitments can promote economic growth and job creation in the UK and Korea.

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

**Data Transfers & Services**: As services are increasingly enabled by digital means, cross-border data transfers have increased in importance. A 2020 World Economic Forum study found that, "approximately half of cross-border [services] trade is enabled by digital connectivity[, which] … has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution. … Developing countries ... accounted for 29.7% of

---

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

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

[3] Data localisation mandates and unnecessary data transfer restrictions hurt local innovation because a country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are critical to growth and innovation, business operations, and the transfer of technology. These include: (a) growth-enhancing software solutions; (b) scientific, research, and other publications; and (c) manufacturing data, blueprints, and other operational information. Faced with higher software costs and an unpredictable environment for R&D investments, local industries face challenges keeping technological pace with foreign competitors — threatening both domestic and export market sales. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for investment and R&D.

[4] Local enterprises face competitive harm if they are deprived of the insights that come from consolidating local data sets within larger regional or global data sets for purposes of data analysis. *See generally,* BSA, *Understanding Artificial Intelligence* (2017), at: https://www.bsa.org/sites/default/files/2019-03/BSA_2017UnderstandingAI.pdf ; BSA, *What's the Big Deal with Data* (2017), at: https://data.bsa.org/; BSA, *Artificial Intelligence in Every Sector* (2019), at: https://www.bsa.org/sites/default/files/2019-03/BSA_2018_AI_Examples.pdf.

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

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

services exports in 2019."[7] Cross-border data commitments can help support the growth of services in the UK and Korea.

**Data Transfers & Trade Facilitation**: Cross-border technology access and data transfers also reduce supply chain-related transaction costs.[8] One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.[9] Likewise, the Asia Development Bank Institute estimates that electronic commerce platforms, which operate on the basis of cross-border data transfers, have helped some local firms reduce the cost of distance in trade by 60%.[10] Cross-border data commitments in the UK-Korea FTA can help promote these efficiencies.

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

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

---

[7] World Economic Forum, Paths Towards Free and Trusted Data Flows (2020). Conversely, the World Bank 2021 *World Development Report* has noted that measures that "restrict cross-border data flows ... [may] materially affect a country's competitive edge in the burgeoning trade of data-enabled services." World Bank, *World Development Report – Data For Better Lives* (2021), at: https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf

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

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

[10] Asia Development Bank Institute, *The Development Dimension of E-Commerce in Asia: Opportunities and Challenges* (2016), at: https://www.adb.org/sites/default/files/publication/185050/adbi-pb2016-2.pdf

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

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

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

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

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

Economic development depends upon cross-border access to knowledge, digital tools, and commercial opportunities. Cross-border data commitments in the UK-Korea trade agreement can help both the UK and Korea support access and development in emerging economies, consistent with the UN's Sustainable Development Goals.

**Data Transfers & Privacy**: Some argue that data localisation requirements and cross-border data restrictions are necessary for privacy reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. This argument is incorrect. Cross-border restrictions are not necessary to protect privacy and can undermine data security. In lieu of such restrictive policies, countries with robust data protection frameworks often adhere to the accountability principle and interoperable legal frameworks that protect data consistent with national standards, even as the data is transferred across borders. Organizations that transfer data globally typically adopt a set of best practices and internal controls to ensure that the data is protected even when transferred outside of the country. To that end, organizations often rely on various approved data transfer mechanisms, as discussed above.[16]

**Data Transfers & Cybersecurity**: Some argue that cross-border data restrictions are necessary to ensure cybersecurity. However, *how* data is protected is more important to security than *where* it is stored, and transfer restrictions often result in *weaker*, not *stronger*, cybersecurity. Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Stronger cybersecurity is enabled by cross-border data analytics an assertive cyber-defense posture coordinated across IT networks and national boundaries.[17] When governments mandate localisation or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.

**Data Transfers & Regulatory Compliance**: Some claim that cross-border data restrictions ensure government access to data for regulatory or investigatory purposes. The location of the data, however, is not the determining factor. On the contrary, "data localisation requirements can increase … operational

---

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

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

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

[17] See generally, BSA, *Moving to the Cloud – A Primer on Cloud Computing* (2018), at https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf. Cloud services delivered across-borders provide security advantages over alternative IT delivery approaches (on-premises or local cloud services):

- Physical Security: Certified personnel can carefully monitor servers 24/7 to prevent physical breaches and can apply consistent protocols over a small number of locations.
- Data Security: CSPs can ensure data integrity through use of state-of-the-art encryption protocols for data at-rest and in-transit. CSPs can establish redundant backups of data in geographically dispersed data centers, mitigating risk of loss in the event of power outages or natural or manmade disasters.
- Advanced Threat Detection: CSPs leverage state-of-the-art enhanced security intelligence They use regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- Automated Patch Deployment: Automated and centralized patch deployment and real time 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.

risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information." Accordingly, regulatory authorities in many countries actually encourage the responsible transfer of data across borders. Likewise, data transfers are critical to other public policy priorities, including anti-money laundering; anti-corruption; and other legal compliance objectives.[18]

**Data Transfers & Fraud Prevention**: Prohibitions on cross-border data transfers in respect of financial data can have significant negative impacts on the effectiveness of fraud prevention and mitigation tools. Effective fraud mitigation as provided by banks, card networks and other players in the financial services sector demands sophisticated monitoring and rapid detection at the time of transaction to interpret and weigh the risk of fraud of each payment transaction as weighed by the facts of that payment transaction as against norms for all payment transactions and that account. Fraud detection models are typically built on global transaction data or transaction data collected from multiple countries since fraud patterns are not limited by national boundaries. Fraud trends which appear in one region or country may apply in others as cardholders travel to different countries, cardholders transact online with merchants in different countries, and the perpetrators of fraud do not respect any national boundary lines. Thus, to build effective fraud models and to gain the necessary insights into fraudulent activity in order to help prevent them, these models must be built off of global or multi-country data sets, based both on the location of the merchant and the location of the cardholder.

**Data Transfers & Innovation:** Some claim that cross-border data restrictions promote innovation. On the contrary, data localisation 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.[19]

**Data Transfers & Healthcare:** Healthcare R&D, the submission of health-technology-assessment and regulatory filings, and the provision of services in the life-science industries are increasingly cross-border endeavors which rely on the responsible and secure flow of large volumes of data. These transfers can support the adoption of data analytics and machine-learning technologies, and processing of data from multi-country clinical studies and other research activities. Supporting cross-border data transfers, in a way that is compatible with the best practices in ensuring patient and customer privacy, is essential for the innovation of healthcare products and services, collaboration across multiple public and private research organizations, and the early detection of regional or global health risks. Restricting such data transfers will undermine the ability to identify new treatments and improve healthcare delivery, to the ultimate detriment of patients in those countries that restrict transfers.[20]

**Data Transfers & Tech Policies:** From artificial intelligence to 5G to the cloud, government tech policies can help coordinate public-private dialogue, support investment, and maximize the benefits of 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 localisation 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;

---

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

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

- Cross-border collaboration and communication with foreign business partners;
- Foreign transactions and business opportunities; and
- Improved resiliency resulting from data storage across multiple geographical locations

**Data Transfers & COVID-19 Recovery:** As governments seek to limit the spread of COVID-19, cross-border access to technology and data transfers have become essential for countries seeking to sustain jobs, health, and education. This is particularly true for the remote work, remote health, supply chain management, and innovation-related technologies that depend on cross-border access to cloud computing resources.

---

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

[2] In a span of just over two years, UK trade negotiations have produced remarkable results, including in the UK-EU Trade and Cooperation Agreement, the UK-Japan Comprehensive Economic Partnership Agreement, the UK-Australia Free Trade Agreement (FTA), the UK-New Zealand Free Trade Agreement, and the UK-Singapore Digital Economy Agreement, among other agreements. Ongoing negotiations present an opportunity to build upon these results with trading partners including Canada, India, Israel, Mexico, Switzerland, Ukraine, the United States, as well as the CPTPP Parties and the Gulf Cooperation Council. Many of the negotiated outcomes in these agreement represent the state of the art in cross-border data policy matters.

[3] More information to illustrate the cross border digital interests of different sectors can be found here: https://globaldataalliance.org/sectors/

[4] South Korea call for input information note (publishing.service.gov.uk)

[5] Id.

[6] KSDPA, Art. 14.15(4).

[7] nited States-Singapore Joint Statement on Financial Services Data Connectivity, February 2020, https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity

**[8]** A measure does not meet the conditions of paragraph 2(a) if it accords different treatment to transfers of information solely on the basis that those transfers are cross-border and if it does so in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.

[9] The Parties recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access. Each Party shall, to the extent practicable, provide a covered person with a reasonable opportunity to remediate a lack of access to information as described in paragraph 2 before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of another jurisdiction.

[10] "Technical regulation," "standard" and "conformity assessment procedure" have the meaning set forth in the WTO Agreement on Technical Barriers to Trade, Annex 1, at: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm

[11] "Licensing requirement and procedure" has the meaning set forth in the WTO Reference Paper on Services Domestic Regulation, at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/1129.pdf&Open=True

[12] *Id.*

[13] A measure does not meet the conditions of paragraph 4(a) if it modifies conditions of competition to the detriment of service suppliers of another Party by according different treatment on the basis of the location of computing facilities used, or on the basis of the location of data storage or processing.

**[14]** "Customs duty" includes any duty or charge of any kind imposed on or in connection with the importation of a good, and any surtax or surcharge imposed in connection with such importation, but does not include any:
(i) charge equivalent to an internal tax imposed consistently with paragraph 2 of Article III of the GATT 1994;
(ii) fee or other charge in connection with the importation commensurate with the cost of services rendered; or
(iii) antidumping or countervailing duty.

[15] For greater certainty, a Party may comply with the obligation paragraph 1 by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.