April 11, 2024

Ms. Tina Lim-Keasberry
Assistant Chief Executive
Authority for Info-communications Technology Industry
Via email: tina.lim@aiti.gov.bn

Dear Assistant Chief Executive Lim-Keasberry,

We at BSA | The Software Alliance[1] (**BSA**) and the Global Data Alliance (**GDA**)[2] would like to express our appreciation to Brunei for your ongoing work in negotiating the ASEAN Digital Economy Framework Agreement (**DEFA**).

In the Leaders' Statement on the Development of the ASEAN DEFA, the ASEAN member states agreed to, *inter alia*, develop a "modern, comprehensive and coherent digital transformation strategy towards an ASEAN digital economy, where the seamless and secure flow of goods, services, and data is underpinned by enabling rules, regulation, infrastructure, and talent". We applaud Brunei and ASEAN's acknowledgement that having rules that enable data transfers is necessary to unlock the potential of the region. Indeed, data transfers and digital networks lie at the heart of ASEAN's digital economy: they support jobs in every country, across every sector, and at every stage of the value chain in billions of transactions every day.

In this regard, we urge Brunei and your fellow ASEAN states to support strong and binding rules that prohibit: a) unnecessary restrictions on data transfers; b) data localization requirements; c) customs duties on electronic transmissions; d) forced technology transfer requirements and improper source code disclosure mandates; and e) the misuse of technical regulations and standards to create barriers to digital trade and discriminate against non-national persons and technologies. These rules are an important bulwark against digital protectionism, which undermine legal predictability and economic opportunity for citizens and businesses alike, widening the digital divide.

In **Annex I** to this letter, we provide evidentiary support for the benefits of cross-border data commitments, including how they will benefit regional economic growth. In **Annex II**, we present model provisions on cross-border data transfers and digital trust for your consideration.

We would welcome the opportunity to engage with your staff in connection with the DEFA negotiations. Please do not hesitate to have your staff reach out to me or Jared Ragland, BSA's Senior Director of Policy for APAC (jaredr@bsa.org), with any questions or comments.

Sincerely,

Tham Shen Hong

Tham Shen Hong
Senior Manager, Policy – APAC

[1] BSA | The Software Alliance is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

[2] 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 are active in a broad array of sectors, including aerospace, agriculture, automotive, energy, electronics, finance, health, logistics, and telecommunications, among others.

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

## ANNEX I: Evidentiary Support for Cross-Border Data Commitments

To unlock the value of the ASEAN's digital economy and achieve its economic imperatives, it is critical that the DEFA 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 are summarized below.

**Data Transfers & Economic Growth**: Cross-border data transfers — valued in the trillions of dollars[3] — 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."[4] Local enterprises rely on data flows to drive quality, reach international customers, achieve economies of scale, and improve output,[5] often benefiting from cross-border access to tailored data-enhanced analytics and insights.[6] Cross-border data commitments can promote economic growth and job creation among ASEAN states.

**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.[7] Conversely, data restrictions are harmful in this area. For example, a 2021 GSMA study conducted in three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on IoT applications and machine-to-machine (**M2M**) data processing could result in: (a) loss of 59-68% of their productivity and revenue gains; (b) investment losses ranging from $4-5 billion; and (c) job losses ranging from 182,000-372,000 jobs.[8] Cross-border data commitments can promote manufacturing across the region.

**Data Transfers & Services**: As services are increasingly enabled by digital means, cross-border data transfers have increased in importance. A 2020 World Economic Forum study found that, "approximately half of cross-border [services] trade is enabled by digital connectivity[, which] … has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution. … Developing countries ... accounted for 29.7% of services exports in 2019."[9] Cross-border data commitments can help support the growth of services across the region.

---

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

[4] 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..."

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

[6] 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.

[7] 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

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

[9] 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

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

**Data Transfers & Trade Facilitation**: Cross-border technology access and data transfers also reduce supply chain-related transaction costs.[10] One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.[11] 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%.[12] Cross-border data commitments in the ASEAN DEFA 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).[13] Cross-border data commitments can help promote uptake of sustainable agricultural practices and technologies across the region.

**Data Transfers & Sustainable Economic Development**: Analyses by development banks consistently show that cross-border access to technology and data transfers promote sustainable economic growth. For example, there remain over 2.5 billion unbanked people worldwide, many living in remote locations lacking physical banking infrastructure.[14] 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.[15]

Unfortunately, some economies are erecting costly data transfer restrictions vis-à-vis one another.[16] 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.[17]

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

---

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

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

[12] 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

[13] 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."

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

[15] 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

[16] 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

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

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

**Data Transfers & Privacy**: Some argue that data localization requirements and cross-border data restrictions are necessary for privacy reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. This argument is incorrect. Cross-border restrictions are not necessary to protect privacy and can undermine data security. In lieu of such restrictive policies, countries with robust data protection frameworks often adhere to the accountability principle and interoperable legal frameworks that protect data consistent with national standards, even as the data is transferred across borders. Organizations that transfer data globally typically adopt a set of best practices and internal controls to ensure that the data is protected even when transferred outside of the country. To that end, organizations often rely on various approved data transfer mechanisms, as discussed above.[18]

**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.[19] When governments mandate localization 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 localization requirements can increase … operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information." Accordingly, regulatory authorities in many countries actually encourage the responsible transfer of data across borders. Likewise, data transfers are critical to other public policy priorities, including anti-money laundering; anti-corruption; and other legal compliance objectives.[20]

**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

---

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

[19] 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.

[20] 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

or multi-country data sets, based both on the location of the merchant and the location of the cardholder.

**Data Transfers & Innovation:** Some claim that cross-border data restrictions promote innovation. On the contrary, data localization mandates and data transfer restrictions undermine beneficial innovation processes — from accessing global scientific and technical research databases, to engaging in cross-border research and development (R&D), to securing intellectual property rights for new inventions, and regulatory product approvals for new products and services.[21]

**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.[22]

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

[22] 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/

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

## ANNEX II: Model International Agreement Provisions re Cross-Border Data Transfers & 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:

1. The legitimate policy objectives of the Parties, including those relating to the protection of the environment, health, privacy, safety, security, and regulatory compliance;
2. Sustainable economic development and shared economic prosperity, including through greater cross-border connectivity, including for Micro-, Small-, and Medium-Sized Enterprises;
3. Financial inclusion and security, including for those lacking access to banking resources, as well as fraud prevention, anti-money laundering, and financial transparency;
4. Healthcare delivery, research and development of new healthcare treatments, cross-border healthcare regulatory collaboration, and global medical humanitarian assistance;
5. 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;
6. 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
7. 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;[23] 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

[23] 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.

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

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.[24]

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 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;[25]
        ii. licensing requirements and procedures;[26]
        iii. qualification requirements and procedures;[27] or
        iv. other governmental measures that affect trade; or
        v. 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;[28] 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[29] on electronic transmissions, including content transmitted

---

[24] 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.

[25] "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.

[26] "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

[27] *Id.*

[28] 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.

[29] "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.

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

electronically, between a person of a Party and a person of the other Party.

**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, consumer protection, and safeguards against unsolicited electronic communications can help enhance confidence in digital trade and can facilitate the delivery of economic and social benefits to citizens;
2. Protecting the integrity of source code and algorithms from malicious cyber-related compromise or theft necessitates limits on forced technology transfer and access mandates, but – at the same time – regulatory bodies and judicial authorities can have legitimate regulatory or judicial reasons to require that source code or algorithms be preserved or made available for a specific investigation, inspection, examination, enforcement action, or judicial proceeding;
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
4. Adopting Artificial Intelligence (AI) risk management frameworks can help ensure that AI is developed and deployed to produce benefits for the health and well-being of citizens, to safeguard democratic values, and to help enterprises map, measure, manage, and govern high-risk uses of AI, including those that may result in unlawful discrimination.

**Article __: Protecting Personal Information and Privacy**

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.[30] 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

[30] 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.

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

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 5 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 the APEC Cross Border Privacy Rules System.

**Article __: Protecting Source Code Integrity**

1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available[31] the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.

**Article ___: Protecting Cybersecurity**

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.

**Article ___: Promoting Trust in Artificial Intelligence**

1. Each Party recognizes the importance of developing governance frameworks for the trusted,

[31] This making available shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

safe, and responsible development and use of AI technologies. To that end, each Party should take into account the OECD Principles on Artificial Intelligence. The Parties endorse the OECD's five recommendations to policymakers pertaining to national policies and international co-operation for trustworthy AI, namely: (2.1) investing in AI research and development; (2.2) fostering a digital ecosystem for AI; (2.3) shaping an enabling policy environment for AI; (2.4) building human capacity and preparing for labor market transformation; (2.5) and international co-operation for trustworthy AI.

2. Consistent with OECD Recommendations 2.2 – 2.3, the Parties acknowledge the benefits of supporting interoperable legal frameworks and voluntary consensus-based standards and best practices relating to AI. Each Party shall encourage organizations within their jurisdiction that develop and deploy AI systems to risk-based approaches that rely on consensus-based standards and risk management best practices to map, measure, manage, and govern high-risk uses of AI.

3. Consistent with OECD Recommendation 2.5, each Party recognizes that AI systems should not result in unlawful discrimination on people based on their race, color, religion, sex, national origin, age, disability and genetic information or any other classification protected by the law of the Party. Each Party also recognizes that existing nondiscrimination laws remain enforceable in instances involving the use of AI.

4. Consistent with OECD Recommendation 2.4, and recognizing the importance of workforce development for AI-related technical skills to empower and enable current and future generations of workers and to improve the quality of life of our people, the Parties shall, subject to the availability of resources, upon request, and on mutually agreeable terms and conditions, exchange information and best practices, and otherwise cooperate, to:

    a. develop programs to train and reskill workers for AI and other high-demand technology skills;

    b. invest in apprenticeship programs and other alternative pathways to future employment that require AI and other high-demand technology skills;

    c. explore public-private partnerships to expand the availability of real-time labor data that can improve employer and worker visibility into the AI and other digital skillsets that are most in-demand in their markets, allowing them to make informed choices about the types of reskilling efforts that will generate the most opportunity; and

    d. invest in inclusive science, technology, engineering and math education, with an emphasis on computer science, at all levels of the educational system.

5. Consistent with OECD Recommendation 2.1, each Party shall promote sustained investment in AI R&D and public-private collaboration across the region. The Parties shall, subject to the availability of resources, upon request, and on mutually agreeable terms and conditions, collaborate to:

    a. take stock of and utilize existing science and technology cooperation and multilateral cooperation frameworks involving Parties;

    b. recommend priorities for future cooperation, particularly in R&D areas where the Parties share strong common interests, face similar challenges, or possess relevant expertise;

    c. coordinate as appropriate the planning and programming of relevant activities, including promoting collaboration among government entities, the private sector, and the scientific community;

    d. promote AI R&D, focusing on challenging technical issues, and protecting against efforts to adopt and apply these technologies in the service of authoritarianism and repression; and

    e. explore the development of sharing best practices on public data sets to unlock AI innovation and exchanges of information on regulatory frameworks to remove barriers to innovation.

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

**Article __: Protecting Transparency and Fairness in Digital Standard-Setting**

1. Scope and Definitions
    a. Scope: This section applies to technical regulations, standards and conformity assessment procedures regarding the development, distribution, and supply of digitally enabled services.
    b. Definitions:
        i. Digitally enabled services are services that are performed or delivered electronically. They include services that relate to a process or a production method associated with a product. They also include services that do not relate to such a process or method.[32]
        ii. "Technical regulations," "standards," and "conformity assessment procedures" are defined as set forth in the WTO Agreement on Technical Barriers to Trade.
2. Affirmation of the Right to Regulate

    The Parties reaffirm the right to regulate within their territories through measures necessary to achieve legitimate policy objectives as set forth in GATS Article XIV.
3. Application of WTO Domestic Regulations text and Good Regulatory Practices Provisions to digitally enabled services standards and conformity assessment procedures

    For greater certainty, the provisions of the Domestic Regulations and Good Regulatory Practices provisions included in this Agreement shall apply to digitally enabled services standards and conformity assessment procedures.
4. Best Regulatory Practices Regarding Digitally Enabled Services Standards and conformity assessment Procedures.

    To promote transparency, interoperability, and non-discrimination, each Party agrees to:
    a. treat non-national products, services, or technologies no less favorably than like domestic products, services, or technologies in relation to technical regulations, standards and conformity assessment procedures;
    b. adhere to relevant international standards, where they exist or their completion is imminent;
    c. provide an explanation and justification if the Party does not adhere to a relevant international standard; and
    d. commit to provide adequate notice and consultation periods prior to adopting any new technical regulation, standard, or conformity assessment procedure relating to digitally enabled services.

**Article __: Protecting Democratic Accountability in Government Access to Privately Held Data:**

Each Party affirms its support for the OECD Declaration on Government Access to Personal Data held by Private Sector Entities and affirms the importance of the seven core principles of that Declaration, including legal basis, legitimate aims, approvals, data handling, transparency, oversight, and redress. Each Party shall adopt or maintain a legal framework that implements these seven principles.

[32] For greater certainty, digitally enabled services technical regulations and standards that relate to product characteristics or their related processes and production methods, or the terminology, symbols, symbols, packaging, marking or labelling requirements as they apply to a product, process or production method are within the scope of the WTO TBT Agreement and therefore subject to its requirements and procedures.

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

**Article __: Protecting Consumers Online**

1. The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent or deceptive commercial activities as referred to in Article ___ (cross reference to Consumer Protection) when they engage in digital trade.
2. Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.
3. The Parties recognize the importance of, and public interest in, cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border digital trade in order to enhance consumer welfare. To this end, the Parties affirm that cooperation under consumer protection under Article __ (cross reference) includes cooperation with respect to online commercial activities.

**Article __: Protecting Against Unsolicited Commercial Electronic Communications**

1. Each Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic communications.
2. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic communications sent to an electronic mail address that:
    a. require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or
    b. require the consent, as specified in the laws and regulations of each Party, of recipients to receive commercial electronic messages.
3. Each Party shall endeavor to adopt or maintain measures that enable consumers to reduce or prevent unsolicited commercial electronic communications sent other than to an electronic mail address.
4. Each Party shall provide recourse in its law against suppliers of unsolicited commercial electronic communications that do not comply with a measure adopted or maintained pursuant to paragraph 2 or 3.
5. The Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic communications.

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org