



May 24, 2021

Infocomm Media Development Authority  
10 Pasir Panjang Road  
#03-01 S117438

By electronic submission

## **SURVEY ON THE DIGITAL ECONOMY AGREEMENTS BSA COMMENTS**

BSA | The Software Alliance (**BSA**)<sup>1</sup> welcomes the opportunity to provide comments in response to the survey on digital economy agreements (**DEAs**) published by Singapore's Infocomm Media Development Authority (IMDA) in April 2021.<sup>2</sup>

The Government of Singapore is playing a leading role in advancing a new international legal framework for the digital economy through its proactive and creative approach to negotiating DEAs. The ambitious, high-standard commitments in DEAs will benefit both Singapore and its trading partners, supporting job creation, innovation, productivity growth, and overall competitiveness in the digital economy. Furthermore, at a time when some countries are placing limits on international technological collaboration and the cross-border transfer of information, Singapore's leadership in advancing DEAs provides an essential counter-narrative that will help ensure that open and innovative economies will be able to collaborate with like-minded partners to develop new scientific and innovative solutions to address the health, environmental, and economic challenges of our generation.

### **BSA'S RECOMMENDATIONS FOR DIGITAL ECONOMY AGREEMENTS**

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are at the forefront of the data-driven innovation that is fueling global economic growth and recovery, including through cutting-edge advancements in cloud computing, security solutions, artificial intelligence (**AI**) and machine learning, and the Internet of Things (**IoT**). BSA member companies provide services and solutions to enterprise customers, so they understand the critical importance of enabling a trusted digital environment, where enterprise customers, government agencies, and individual consumers trust that their data will remain secure and accessible and will be used in accordance with reasonable expectations.

Accordingly, BSA recommends that the Government of Singapore continue to enhance the DEAs to include meaningful and enforceable commitments in the following areas:

- **Securing the New Data Economy**
- **Promoting Trust and Security**
- **Advancing the Use of Technology in Government**

---

<sup>1</sup> BSA's members include: Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

<sup>2</sup> <https://form.gov.sg/#!/607f804eb2603300117ccf1f>

## SECURING THE NEW DATA ECONOMY

The availability and movement of data underpins digital trade and the digital economy. Data is also at the core of new and rapidly growing service supply models such as cloud computing, the Internet of Things (IoT), and Artificial Intelligence (AI). DEAs can play an important role in building new digital trade rules in these emerging areas.

### *International Data Transfers*

DEAs should include commitments that prohibit governments from imposing barriers to cross-border data transfers.

Recognizing that a government may determine it to be necessary to adopt or maintain certain measures for legitimate domestic public policy purposes that are not consistent with this obligation, including for purposes of personal data protection or data security, DEAs should stipulate that any such measures must not discriminate against foreign service providers or constitute a disguised restriction on trade, and must be necessary to achieve the specific objective.

Furthermore, where a government treats domestic data transfers differently from international data transfers, such differential treatment must not result in less favorable treatment to foreign service providers.

Finally, with respect to this discipline and others across the agreement, a dispute settlement mechanism should be available to allow scrutiny and enforcement of measures that derogate from this obligation.

### *Data Localization Requirements*

DEAs should prohibit governments from imposing data localization requirements as a condition of market access for any sector of the economy. For example, a government should not require a software service provider to establish or use a data center inside its borders as a condition for doing business in its territory.

Consistent with our earlier comment on cross border data transfers, while in some circumstances a government may deem it necessary to adopt or maintain certain measures for legitimate domestic public policy purposes that are not consistent with this obligation, including to protect privacy or promote data security, the DEAs should stipulate that such measures must not discriminate against foreign service providers or constitute a disguised restriction on trade and must be narrowly tailored to achieve the specific objective.

The prohibition to data localization requirements should apply to sector-specific policies as well. In general, rules specific to any specific sector, such as financial services, which are typically addressed in separate chapters of free trade agreements, should be substantially the same as the rules of general applicability on cross-border data transfers and data localization and must not contain any special rules that could be interpreted to deviate from the general commitments.

A dispute settlement mechanism should also be available to allow scrutiny and enforcement of measures that derogate from this obligation.

### *New Digital Products and Services*

DEAs should ensure that robust market access commitments cover both existing categories of digital products and services and new ones that may emerge in the future. Innovative new digital products and services should be protected against future discrimination and trade agreements should not become obsolete as markets evolve and technology advances. By design, protections for services and investment should continue to apply as markets change and innovative technologies emerge unless a specific, negotiated exception applies.

### *Artificial Intelligence (AI)*

Given that traditional trade agreements have not yet included disciplines regarding AI, Singapore is well-placed to set ambitious benchmarks for its trading partners through the DEAs. The DEAs should include provisions that will provide for an open regulatory environment for the trade and investment in, and development of, AI and emerging technologies and related services. These

include:

- providing for ample, timely, and transparent opportunities for public engagement in developing relevant policies;
- adhering to risk-based policy development processes, including to assess and manage potential risks associated with specific AI applications;
- taking into account voluntary, internationally recognized standards when developing technical standards and other policies;
- giving due consideration to core principles of technological interoperability and technology neutrality;
- ensuring that commercial text and data mining of lawfully accessible content is permitted;
- avoiding discrimination against AI applications or technologies based on, for example, the origin of the application or technology; and
- promoting sustained investment in AI research and development on a non-discriminatory and transparent basis.

### **Electronic Authentication and Smart Contracts**

DEAs should advance the mutual recognition of electronic authentications, signatures, and/or digital identity frameworks to enhance interoperability and expand the adoption of paperless trading. In addition, the DEAs should provide for the use of “smart” contracts and other autonomous machine-to-machine means for conducting transactions, such as blockchain. These mechanisms help reduce unnecessary and outdated processes, and support individuals and businesses by allowing them to conduct business quickly and securely with customers and partners.

### **Open Government Data**

Ensuring that quality data is available and accessible to the public and to private enterprises is essential for helping businesses develop and deploy innovative business practices and new products, tools, and solutions to increase their competitiveness in global markets. To unlock the value of data across their economies and to attract foreign investments, DEAs should include provisions to make non-sensitive government-generated data freely available to the public on a non-discriminatory basis and in machine-readable formats. The DEAs can also encourage the development and use of privacy-enhancing technologies that enable data collaboration in ways that align with the public’s expectations for privacy.

### **Customs Duties on Electronic Transmissions**

DEAs should prohibit governments from imposing customs duties or other customs requirements on software or other digital products transmitted electronically.

## **PROMOTING TRUST AND SECURITY**

Privacy and security are bedrock principles for software services providers. BSA members are committed to protecting customers’ privacy and data security. Our companies regularly update their software products and services as well as their policies to ensure that their customers can securely use their services and other offerings, and that they comply with the laws of each market in which they operate. DEAs can enhance the interoperability of legislative frameworks and reiterate the importance of aligning with internationally recognized standards.

### **Data Privacy**

Singapore’s Personal Data Protection Act provides solid foundations for an international transfers regime as it recognizes the importance of international transfers of personal data with effective privacy safeguards and provides tools for organizations to legally transfer personal data abroad.

The DEAs offer an opportunity for the Government of Singapore to make progress on the interoperability of data privacy frameworks and cross border data transfer mechanisms with key trading partners in the region and globally. The DEAs should include provisions that will enhance the

interoperability of data protection and privacy frameworks and recognize the use of a variety data transfer mechanisms that meet the domestic standards of both Singapore and its negotiating partners.

### **Cybersecurity**

Domestic policies and international cooperation should aim to reduce cybersecurity risks (for instance by safeguarding information technology systems, sensitive data, and networks), leverage common solutions such as internationally recognized standards and innovative practices to improve efficiency, increase security, and meet organizations' needs. Therefore, DEAs should include provisions that will advance mutually beneficial approaches to cybersecurity and strengthen the foundations of digital trade and innovation. This can be done through building upon previous negotiating experience, such as the principles proposed by the United Nations Group of Government Experts and endorsed by the G-7.

Although businesses, private citizens, and government agencies all share responsibility for enhancing cybersecurity, governments play a primary role in advancing globally recognized standards, adopting internationally interoperable regulations, and introducing appropriate market incentives for the private sector to invest in cybersecurity. A G2G instrument like the DEA can encourage the mutual adoption of voluntary, standards-based, outcome-focused cyber risk management frameworks to drive the adoption of more effective cybersecurity measures by both governments and industry stakeholders.

### **Internationally Recognized Standards**

DEAs should ensure application of the rules agreed under the WTO Agreement on Technical Barriers to Trade (**TBT**) as updated and revised in later agreements like the Comprehensive and Progressive Trans-Pacific Partnership (**CPTPP**) to apply to digital products, services, and technologies. Coverage should include cloud computing, cybersecurity, AI/data analytics/machine learning, and other new and innovative digital products, services, and technologies. Reflecting a shared commitment among DEA participants to apply these TBT disciplines in this manner would significantly enhance legal predictability among countries that seek to improve the business and operational environment for companies that operate, invest, and provide employment in their jurisdictions.

### **Encryption**

DEAs should prevent governments from undermining the use of encryption in commercial products by prohibiting restrictions on security technologies used to protect data in-transit or at-rest. Such a provision should preclude governments from mandating how encryption and other security technologies are designed or implemented, including by prohibiting requirements to build in vulnerabilities or "back-doors" or otherwise requiring the disclosure of encryption keys.

## **ADVANCING THE USE OF TECHNOLOGY IN GOVERNMENT**

DEAs should promote the use of innovative technology in government operations, including operations involved in providing services to citizens.

### **Procurement**

Procurement rules should ensure that each participating government opens its government procurement market to enterprises of the other Party, including in relationship to technology, software, and cloud computing procurements.

### **Encourage Open Digital Architectures and Ensure Technology Choice**

DEAs should ensure that companies and government agencies are free to choose and use the technologies and solutions that best suit their needs. Government procurement rules should not require government agencies to purchase and use local or other specific technology. This will enable companies in participating economies to achieve greater security and drive innovation in key technologies, including cloud computing, AI, and 5G telecommunications.

## CONCLUSION

BSA appreciates the opportunity to submit our comments to this DEA survey which we hope will be helpful as IMDA continues to refine and enhance Singapore's approach on DEAs. We look forward to continued collaborations with the Government of Singapore and their global trade partners in advancing international norms on digital trade. If you require any clarification or further information in respect of this submission, please contact the undersigned at [eunicel@bsa.org](mailto:eunicel@bsa.org).

Yours faithfully,



Eunice Lim

Senior Manager, Policy – APAC

BSA | The Software Alliance