October 17, 2024

Ms. Laura Buffo
Chair of the Trade Policy Staff Committee
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508
ForeignTradeBarriersReport@ustr.eop.gov

Re: Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report, 89 Fed. Reg. 71775 (Sept. 3, 2024): Docket Number USTR–2024–0015

Dear Ms. Buffo,

BSA | The Software Alliance[1] provides the following information in response to your request[2] for written submissions to the Trade Policy Staff Committee (TPSC) regarding significant trade barriers for inclusion in the National Trade Estimate on Foreign Trade Barriers (NTE Report). The efforts of the Office of the US Trade Representative (USTR) to support open markets and combat trade barriers are critical to supporting the global economic recovery amidst numerous global challenges. We look forward to any questions that you may have regarding our submission.

Sincerely yours,

Joseph Whitlock

---

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. 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. BSA's members include: BSA's members include:
BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] *See* USTR, Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report, 89 Fed. Reg. 71775 (Sept. 3, 2024), at: https://www.federalregister.gov/documents/2024/09/03/2024-19694/request-for-comments-on-significant-foreign-trade-barriers-for-the-2025-national-trade-estimate#:~:text=USTR%20invites%20comments%20to%20assist%20it

Submission of BSA | The Software Alliance re
National Trade Estimate on Foreign Trade Barriers

This document responds to USTR's solicitation of information relevant to the NTE Report, and contains the following major sections:

I. Executive Summary

The following executive summary introduces the importance of software and digital trade, relevant NTE criteria for digital trade, and key market access and intellectual property (IP) priorities in select economies.

A. Software and Digital Trade — Statistical Overview

Over the past decade, the US software industry and cross-border digital trade have become a primary driver of the global economy. As illustrated below, the US software industry has helped build stability and resilience into the US economy:

- Software drives growth: As of 2021, the US software industry (including US software exports) was responsible for $1.9 trillion of total US value added GDP and 15.8 million jobs.[3]
- Software drives innovation: Annual US software research and development (R&D) investments exceed $100 billion, accounting for nearly one-third of all private sector R&D.[4]
- Software drives economic opportunity: Jobs in software development, computer programming, and related fields are growing so rapidly that the US Bureau of Labor Statistics estimates 1 million computer programming jobs need to be filled in the United States.[5]

Internationally, these trends are also pronounced, and they have only accelerated in the wake of the recent years amidst growing economic and geopolitical uncertainty. Today, digital trade is central to the US and global economies, and to USTR's vision of a worker-centered trade policy:

---

[3] Software.org, Software – Supporting US Through COVID (2021), available at: https://software.org/wp-content/uploads/2021SoftwareJobs.pdf
[4] Software.org, Growing US Jobs and the GDP (Sept. 2019), available at: software.org/wp-content/uploads/2019SoftwareJobs.pdf.
[5] BSA | The Software Alliance, *A Policy Agenda to Build Tomorrow's Workforce* (2018), available at: https://www.bsa.org/files/policy-filings/05022018BSAWorkforceDevelopmentAgenda.pdf.

- Digital trade drives the global economy: Software-enabled cross-border data transfers are estimated to contribute trillions of dollars to global GDP,[6] with 75 percent of the value of cross-border data transfers benefitting industries like agriculture, logistics, and manufacturing.[7]

- Digital trade is key to a worker-centered trade policy that recognizes the critical role that cross-border data transfers and cross-border access to knowledge and digital tools play in protecting and promoting: (A) small businesses, (B) workers, (C) human rights, (D) economic opportunity in the developing world, and (E) digital inclusion, privacy, cybersecurity, anti-corruption, rule of law, and other policy priorities in the developing world.[8]

- Digital trade benefits every sector: At every stage of the production value chain, cloud- and software-enabled data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes to create jobs, boost efficiency, drive quality, and improve output.[9]

B. NTE Report Statutory Criteria and Policy Priorities for Software and Digital Trade

Unfortunately, trade barriers and digital protectionism continue to grow. Against this background, USTR's review of trade barriers under Section 181 of the Trade Act of 1974, as amended (19 USC § 2241), has ever greater salience. The statute requires USTR to "identify and analyze acts, policies, or practices of each foreign country which constitute significant barriers to, or distortions of —

- United States exports of goods or services (including … property protected by trademarks, patents, and copyrights exported or licensed by United States persons);

- foreign direct investment by United States persons, especially if such investment has implications for trade in goods or services; and

- United States electronic commerce."[10]

Section 181 of the Trade Act also requires USTR to "make an estimate of the trade-distorting impact" of these barriers and to quantify the lost or foregone value of "additional of [US] goods and services, foreign direct investment, and electronic commerce … if each of such acts, policies, and practices of such country did not exist."

In this submission, we address all three statutory elements of Section 181 of the Trade Act as they relate to the trade-related challenges that BSA members increasingly face abroad, and as they relate to BSA's Digital Trade Agenda.[11] Drawing on these BSA resources, BSA's NTE submission address policies of note in the following markets: Australia, Brazil, China, India, Indonesia, Japan, Korea, Singapore, Thailand, Vietnam, and the European Union (EU).

---

[6] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), at https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.
[7] *Ibid*.
[8] BSA | The Software Alliance, *A Worker-Centered Digital Trade Policy* (2023), at: https://www.bsa.org/policy-issues/trade
[9] *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.
[10] 19 USC 2411 *et seq.*
[11] BSA | The Software Alliance, *Digital Trade Agenda* (2018), at: https://www.bsa.org/files/policy-filings/05072019bsa_advancingdigitaltradeagenda.pdf.

C. Digital Market Access and Intellectual Property (IP) Issues in Select Economies

To realize the full potential of digital trade, it is important to establish legal frameworks that foster innovation and promote confidence in the digital economy. We discuss several digital market access issues and several intellectual property (IP) issues below.

1. Digital Market Access Issues

We highlight the following digital market access issues: (1) cross-border data transfers and data localization; (2) discriminatory trade barriers including discriminatory digital taxes; (3) customs requirements on electronic transmissions; (4) security; (5) standards; and (6) procurement restrictions.

Cross-Border Data Transfers and Data Localization: The ability of US companies to continue leading global advances in artificial intelligence and other innovative technology is under a rising threat from foreign government policies that restrict digital trade and market access. These barriers have risen by 600% in the Asia-Pacific alone in recent years.

Data-related market access barriers take many forms. Sometimes the policies expressly require data to stay in-country or impose unreasonable conditions on sending data abroad. In other cases, the policies require the use of domestic data centers or other equipment, or the need for such data centers to be operated by local vendors. Sometimes these measures are based on privacy or security concerns, but too often the real motivation appears to be protectionist, as reflected in their design and operation. For example, these measures may:

- Reflect a choice of policy tools that are significantly more trade-restrictive than necessary to achieve the stated public policy goal;
- Constitute unnecessary, unjustified, and/or disguised restrictions on data transfers across borders, or may be more restrictive of data transfers than necessary; or
- Treat cross-border data transfers less favorably than domestic data transfers.

Sustained attention to these threats is critical. Unfortunately, some economies, including **China, India, South Korea, Indonesia, and Vietnam**, have adopted, or have proposed, rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory.

China has published numerous measures that require data localization or restrict data transfers including the Data Security Law, the Personal Information Protection Law, and the Cybersecurity Law, as well as numerous subsidiary measures, such as the outbound data transfer security assessment measures and (at the municipal or provincial level) various "negative lists" of data whose transfer must be restricted. Purported efforts at reform (such as the proposed Provisions on Promoting Cross-Border Data Transfers)[12] have done little to improve this situation.

While India's Digital Personal Data Protection Act does not contain onerous cross-border data transfer restrictions and localization requirements, India maintains other sectoral measures that do, such as India's Directive on Storage of Payment System Data issued by the Reserve Bank of India in 2018.[13]

In Indonesia, improper cross-border data restrictions or data localization requirements are found in the proposed implementation regulation for Indonesia's Government Regulation 71/2019, OJK Regulation 13/2020, and the draft Regulations concerning Public Scope Electronic System Operators.

---

[12] http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm
[13] *Reserve Bank of India Storage of Payment System Data Directive (2018)* at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0 and *Ministry of Electronics and Information Technology Guidelines for Government Departments on Contractual Terms Related to Cloud Services* at: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.

Likewise, Vietnam's 2024 draft Personal Data Protection Law, its 2024 draft Data Law, its Cybersecurity Law,[14] and numerous implementing regulations and decrees, including Decree 53/2022 and Decree 72, impose improper data localization requirements or other cross-border data restrictions.[15] We have serious questions as to whether these restrictions violate Vietnam's commitments to the United States under the US-Vietnam Bilateral Trade Agreement[16] and in its WTO schedule of commitments under the General Agreement on Trade in Services (GATS).

Finally, BSA continues to monitor the application of measures in the **EU** that govern cross-border data transfers that could restrict cross-border data transfers with third countries. BSA is concerned with the final text (to be adopted formally by the EU Parliament and Council before the end of the year) on the EU Health Data Space (EHDS) which mandates that Health Data Access Bodies, single data holders, and Union data access services store and process personal health electronic data within the EU for any personal data processing operations in preparation for a secondary use, such as pseudonymization and anonymization. Moreover, Articles 60, 61, 62, and 63 introduce additional restrictions on the transfers of electronic health data to third countries.

Customs Requirements on Electronic Transmissions: Across a broad cross-section of economic sectors, there are growing concerns about proposed domestic policies to improperly impose customs duties and other requirements on software and other electronic transmissions. Since 1998, World Trade Organization (WTO) Members have maintained a moratorium on customs duties on electronic transmissions. However, **Indonesia** has amended Indonesia's Harmonized Tariff Schedule to add Chapter 99: "[s]oftware and other digital products transmitted electronically."[17] Indonesia also imposes customs declaration requirements on electronic transmissions.[18] Some countries, including **India** and **South Africa**, also have expressed support for the imposition of customs duties on electronic transmissions. If successful, these misguided efforts would increase costs of digital products and services and reduce productivity and competitiveness for local industries in the implementing countries.

Security: Governments have a legitimate interest in ensuring software-enabled products, services, and equipment deployed in their countries are reliable, safe, and secure. However, some measures — including some in **China, India, South Korea, Thailand, and Vietnam** — that are predicated on security concerns may also be used as a means of justifying *de facto* trade barriers. Requiring cloud service providers to confine data in-country does not improve security but instead ultimately hinders it. First, storing data at geographically diverse locations can enable companies to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location and obscure the location of data to reduce the risk of physical attacks. In addition, cross-border data 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.

Standards: Technology standards play a vital role in facilitating global trade in software-enabled services and IT. When standards are developed through voluntary, industry-led processes and widely used across markets, they generate efficiencies of scale and speed the development and distribution of innovative products and services. Unfortunately, some countries have developed or are developing country-specific standards or proposing mandatory cybersecurity certification for ICT products, services, and processes. The adoption of country-specific standards creates *de facto* trade barriers,

---

[14] *Vietnam's 2018 Cybersecurity Law* at: https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-luat-an-ninh-mang-so-24-2018-qh14-164904-d1.html#noidung.
[15] For a list of the Vietnam's numerous data localization requirements and data transfer restrictions, please see BSA, Comments on Draft Decree superseding Decree No. 72/2013/ND-CP (Sept. 2023), at: https://www.bsa.org/files/policy-filings/09152023decree72.pdf
[16] https://vn.usembassy.gov/the-u-s-vietnam-bilateral-trade-agreement-bta-resources-for-understanding/
[17] *See* Regulation No.17/PMK.010/2018 (Regulation 17) (2018). Regulation 17 purports to cover a wide array of categories, classified in Indonesia's tariff schedule between subheadings 9901.10.00 to subheading 9901.90.00, including "multimedia (audio, video or audiovisual)"; operating system software; application software; "support or driver data, including design for machinery system"; and a broad catch-all category covering "other software and digital products."
[18] *See* MOF Regulation No. 190/PMK.04/2022.

raising the costs of cutting-edge technologies for consumers and enterprises. Countries adopting nationalized standards for IT products include **China and South Korea**.

Procurement Restrictions: Governments are among the biggest consumers of software products and services, yet many impose significant restrictions on foreign suppliers' ability to serve public-sector customers. Not only do such policies eliminate potential sales of products designed and produced by US workers, but they also deny government purchasers the freedom to choose the best available products and services to meet their needs. US trading partners with existing or proposed restrictions on public procurement of foreign software products and services include **China, India, and South Korea.**

2. Intellectual Property Issues

Trade Secrets and Other Proprietary Information: BSA members rely on the ability to protect valuable trade secrets and other proprietary information to maintain their competitive position in the global marketplace. Countries with weak trade secret protection rules, or that have (or are proposing) policies requiring disclosure of sensitive information include **China, India, and Indonesia.** BSA is also concerned with the impact on trade secrets under the EU Data Act. Furthermore, **China** has implemented or proposed policies, such as sector-specific outsourcing or IT risk management frameworks, that require source code review of technologies or services.

Patents: BSA members depend around the world upon effective patent protection to eligible computer-implemented inventions, in line with their international obligations.

Copyrights: Innovation in the digital environment requires legal frameworks that provide copyright holders with the tools necessary to effectively enforce their copyrights. An effective framework for online copyright enforcement must balance the legitimate needs and interests of all parties with a role in driving innovation, including content creators, Internet service providers, online platform providers (i.e., intermediaries), and members of the public. For example, with respect to infringing material online, these interests are best accommodated through safe harbor frameworks that provide online intermediaries with limitations on monetary liability for third party content in exchange for removing content upon notification of claimed copyright infringement from a relevant rights holder. Outside of the United States, Singapore, and a few other market, few US trading partners have modernized their copyright frameworks in this regard.

Artificial Intelligence and Machine Learning: IP frameworks are critical to data-enabled innovations, including artificial intelligence (AI), machine learning, cloud-based analytics, and the Internet of Things (IoT). AI, machine-learning, and data analytics systems are "trained" by ingesting large data sets to identify underlying patterns, relationships, and trends that are then transformed into mathematical models that can make predictions based on new data inputs.[19] Countries around the world are taking a range of approaches to modernize their legal frameworks for AI systems. This includes Japan's May 2018 Copyright Law[20] and Singapore's Copyright Act 2021,[21] which permit data analytics to be performed for both non-commercial and commercial purposes subject to requirements of lawful access. The EU has also incorporated text and data mining exceptions to its copyright regime. Finally, in the United States, the "non-consumptive" reproductions that are necessary for the development of AI-related technologies are considered fair use. BSA urges the US government to continue promoting

[19] Likewise, AI is critical to advances in creativity and innovation. AI provides creators with new tools to enhance their craft — in special effects in film, in sound mixing, in architectural planning, and in vehicular styling and design.

[20] Copyright Law of Japan (Amended 2018), available at https://www.cric.or.jp/english/clj/index.html . See Articles 30-4(iii),

[21] Singapore Copyright Act 2021, available at: https://sso.agc.gov.sg/Act/CA2021?ProvIds=pr7-. See Articles 243-244.

such AI-focused legal frameworks, including in countries like **Australia**[22] and **Brazil,** to foster innovation and creativity.[23]

Software License Compliance: The use of unlicensed software by enterprises and governments is a major commercial challenge for BSA members, having a commercial value of at least US$46 billion.[24] Unlicensed software also presents a serious security risk: Malware from unlicensed software costs companies worldwide nearly US$359 billion a year, and a single malware attack can cost a company US$2.4 million on average and can take up to 50 days to resolve. One means of mitigating these risks is through voluntary compliance measures, such as effective, transparent, and verifiable software asset management (SAM) procedures, where enterprises and government agencies implement the necessary processes to efficiently manage their software assets, including for licensing purposes. Governments should lead by example and adopt such measures for their own procurement and IT maintenance systems.

D. Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the NTE Report and the United States' engagement with important trading partners in 2025. We look forward to working with USTR and the US agencies represented on the TPSC to achieve meaningful progress in addressing the barriers to trade, investment, and e-commerce identified in this submission.

[22] The copyright regime in Australia does not have an exception allowing the use of text and data mining for the purposes of develop AI algorithms. The current round of copyright reforms in Australia failed to address the private sectors' concerns and focused on non-commercial and government use exceptions. They are detailed at: https://www.communications.gov.au/departmental-news/copyright-access-reforms.

[23] See *BSA | The Software Alliance, Comments on the Draft 2018-2022 Strategic Plan of the United States Patent and Trademark Office* (September 18, 2018), pp. 4-5, available at: www.bsa.org/~/media/Files/Policy/IntellectualProperty/09202018USPTOCommentsonDraft20182022StrategicPlan.pdf.

[24] See BSA Global Software Survey – In Brief (June 2018), available at: https://gss.bsa.org/wp-content/uploads/2018/06/2018_BSA_GSS_InBrief_US.pdf.

II. Country-by-Country Analysis

A. Australia

Overview/Business Environment

The Australian Government traditionally has been a strong proponent of facilitating cross-border data transfers and avoiding data localization requirements, recognizing that such restrictions on data will raise costs for businesses and act as a market barrier and in most cases not materially reducing cyber risk. However, disparate departments within the Government also have been prolific in policy making designed to address perceived challenges in the Australian technology ecosystem, but that non-unified approach represents complexity and overhead challenges to organizations to comply, and operational difficulties to technology companies best suited to help drive digital transformation and security in Australia.

Hosting Certification Framework (HCF): Service Providers that deliver or manage hosting services to Australian Government customers, including the facilities that host government data, their systems and supply chains, are required to be HCF-certified. The HCF was originally conceived to address supply chain and foreign ownership risks presented by data hosting providers.[25] While the Department of Home Affairs (**DHA**) has made clear that the HCF currently only applies to data centre providers and cloud service providers that "provide hosting services directly to Australian government customers",[26] the Government has previously suggested that the HCF may be expanded to cover Software-as-a-Service (**SaaS**) providers. This would add an unnecessary layer of certification on top of existing security guidelines and mechanisms, which are already fit for purpose.

Privacy Act Reform

On September 12, 2024 the Australian Government introduced the Privacy and Other Legislation Amendment Bill 2024 (**Privacy Amendment Bill**), which aims to implement some of the legislative proposals identified from the multi-year review of the Australian *Privacy Act 1988.*[27] On data transfers, the Privacy Amendment Bill proposes to introduce a mechanism for the Governor-General to "whitelist" certain overseas jurisdictions by prescribing that a country or binding scheme provides substantially similar privacy protections to the Australian Privacy Principles (**APP**). If a country or scheme is "whitelisted", Australian entities can disclose personal information to recipients in that country without needing to comply with APP 8 on cross-border disclosure.[28] On September 19, 2024, the Senate referred the Privacy Amendment Bill to the Senate Legal and Constitutional Affairs Legislation Committee (Committee) for inquiry and report by November 14, 2024.

Online Privacy Bill

In 2021, Australia introduced the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*.[29] The Bill was intended to implement the recommendations of the Australian Competition and Consumer Commission (ACCC) as described in the July 2019 report of the Digital Platforms Inquiry.[30] Among other things, the Online Safety Bill was intended to establish the development

---

[25] Release of the Hosting Certification Framework, March 2021, https://www.dta.gov.au/news/release-hosting-certification-framework

[26] Hosting Certification Framework – Service Providers, https://www.hostingcertification.gov.au/service-providers#section3.

[27] Australia Privacy Act 1988, https://www.legislation.gov.au/Details/C2020C00237

[28] The text of the Privacy Amendment Bill, Explanatory Memorandum, and Attorney-General Mark Dreyfus's media statement on the reforms are at the following links: Text of Bill; Explanatory Memorandum; and Attorney General's (AG) media statement on amendments.

[29] https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-exposure-draft.pdf

[30] https://www.accc.gov.au/focus-areas/inquiries-finalised/digital-platforms-inquiry-0

of a privacy code for digital platforms and to increase the penalties for breach of the Privacy Act.[31] BSA filed comments at that time.[32] We understand the Bill is no longer under active consideration and we encourage the Australian Government to pursue any necessary legal reforms through the Privacy Act Review process (see above).

Online Safety

In June 2021, Australia enacted the Online Safety Act.[33] The purpose of the Act is to "create a new framework for online safety for Australians" and to "create a modern, fit for purpose regulatory framework that builds on the strengths of the existing legislative scheme for online safety."[34] BSA filed comments on the legislation when it was still before Parliament primarily urging that the legislation focus on high-risk consumer content delivery platforms and to exclude from the scope of coverage enterprise software solutions, including cloud computing services.[35] The final legislation did not exclude low risk enterprise solutions and BSA has worked with other stakeholders to develop the Industry Codes (Codes) called for under Division 7 of the Act.

[31] *See* Explanatory paper: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, October 2021, https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf
[32] *See* BSA Comments on the Australian Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, https://www.bsa.org/files/policy-filings/12062021auonlinepriv.pdf
[33] Online Safety Act 2021, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680
[34] Online Safety Bill 2021, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6680_ems_3499aa77-c5e0-451e-9b1f-01339b8ad871/upload_pdf/JC001336%20Clean4.pdf;fileType=application%2Fpdf
[35] BSA Comments to the Online Safety Bill 2021 Committee Inquiry, March 2, 2021, https://www.bsa.org/files/policy-filings/03022021ausonlinesafetycmte.pdf

B. Brazil

Overview/Business Environment

Although Brazil has taken positive steps to improve market access for cloud service providers, the overall market environment in Brazil remains challenging.

Market Access

In the context of personal data protection, the Brazilian Data Protection Authority has taken steps to mitigate the risk of such barriers by actively promoting the adoption of interoperable legal frameworks for cross-border data. In other contexts, including procurements and AI regulation, market access barriers continue to arise.

***Personal Data Protection and Cross-Border Data**:* On August 23, 2024, the Brazilian Data Protection Authority (ANPD) published Resolution CD/ANPD No. 19/2024 – Brazil's regulations governing international data transfers. The regulations promote streamlined and interoperable transfer mechanisms; recognize the importance of cross-border data transfers for various commercial and public policy goals; and advance principles of accountability and transparency. The Regulations address international data transfers in four scenarios:

- To countries or international organizations that provide adequate protection, as recognized by the ANPD, or
- When a controller guarantees protections consistent with the LGPD through the use of:
    - Specific contractual clauses (with new text for Brazilian SCCs contained in Annex II)
    - Standard contractual clauses
    - Global corporate standards

Data and Server Localization Requirements: The first Guidelines on Government Procurement of Cloud Services were issued in late 2018 and a newer version was issued in late August 2021 still including server and data localization requirements that will negatively impact the procurement of cloud computing services by all federal agencies.[36] The latest version of the Guidelines adequate the language to the LGPD and add new concepts such as "cloud broker". BSA submitted comments on first draft guidelines urging Brazil to remove the localization requirements. However, Brazil did not adopt these recommendations, and the final Guidelines include the localization requirements.[37] A new Procurement Model for Software and Cloud Computing Services was published in October 2023 and became mandatory for procurement processes started after April, 2024, maintaining the localization requirements.

Copyright Enforcement Environment

According to the most recent data, the rate of unlicensed software use in Brazil is 46 percent. This represents a commercial value of approximately US$1.7 billion in unlicensed software.[38] This is a far greater value of unlicensed commercial software than what has been measured throughout the rest of the region. Although recently improvements have occurred, BSA's enforcement programs in Brazil still suffer from a very slow court system that prevents cases from being settled quickly and efficiently.

---

[36] https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684
[37] Comments available at: https://www.bsa.org/~/media/Files/Policy/Filings/CommentsBSA_CloudProcurement.pdf
[38] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at http://www.bsa.org/globalstudy. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2017 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Notice and Takedown: Notice and Takedown is a process not currently codified by the Brazilian Copyright Law. Although the Brazilian Superior Court of Justice has once ruled that notice and takedown principles apply to assess internet provider liability, the ruling does not address the issue completely, and due to the nature of the Brazilian legal system, it is unclear how, if at all, the ruling would apply to other cases. It is, therefore, important that the issue by codified and the relevant provisions added to the revised Brazilian copyright law. We also noted in our comments that it is very important to ensure that the appropriate safe harbors are in place to protect ISPs from liability for copyright infringing content posted by third parties, and that such safe harbors should not be conditioned on any obligation by the ISP to monitor or filter infringing activity.

Information Analysis*:* In legal systems that do not have a flexible fair use provision, which is the case of Brazil, there can be some uncertainty about the permissibility of reproductions used for information analysis or research. It is therefore extremely important to create a specific data analysis provision to avoid any questions about the non-infringing nature of data analysis uses. This will help foster innovation through the continued use of data analysis for innovation purposes, without potential barriers that the threat of potential legal sanctions for copyright infringement could pose.

Compliance and Enforcement: BSA's enforcement program is based on civil cases brought against enterprises that use unlicensed or under-licensed software. In addition, BSA promotes voluntary compliance measures, such as effective, transparent, and verifiable SAM procedures, where enterprises conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed. BSA's efforts in Brazil also include a comprehensive educational communication campaign. This campaign is conducted exclusively online. The campaign is meant to drive awareness of the risks of using unlicensed software.

BSA's relationship with the enforcement authorities in the past years improved due to increasing public awareness of IP-related issues. While civil cases continue to encounter court backlogs, judges in several major jurisdictions are responding well to requests for trials. Additionally, *ex parte* measures are available when necessary, and the courts order companies to cease using unlicensed software.

The Superior Court of Justice has reaffirmed earlier rulings that it is insufficient to simply order companies to pay the license fee they would have had to pay in the first place for the software they have been using without authorization. Instead, fines of multiple times the market value of the unlicensed software are being imposed. This provides greater deterrence in those cases that proceed to final judgment, but also sends a message to companies that they should not wait to be sued before legalizing their software use.

While these are positive trends, there is room for improvement. The Brazilian court system is generally slow. For example, in many instances, it may take anywhere from six to twelve months for an expert report to be ratified by the Court, allowing lawsuits to continue. In addition, Brazilian courts in certain cases continue to require high fees for forensic experts who conduct searches and seizures. Finally, court cases filed in the northern, northeastern, and midwestern regions of the country present additional challenges due to local judges' lack of IP expertise and the low number of qualified experts to perform inspections in those locations. The Ministry of Justice's National Council to Combat Piracy and Intellectual Property Crimes (CNCP) is the main governmental entity responsible for the central coordination and implementation of Brazil's national anti-counterfeiting and piracy campaign. It is critical that the CNCP be properly funded.

Legislative Changes: The Brazilian Ministry of Culture, under the Secretariat for Copyright and Intellectual Property Rights is considering amendments to the current Brazilian Copyright Law. Stakeholders have been invited to comment on whether amending the law is necessary, and, if so, which provisions should be modified or added to the current law. BSA submitted comments suggesting the law be amended to add sections codifying notice and takedown, as well as provisions clarifying the permissibility of reproduction of content used for information analysis or research.

C. China

Overview/Business Environment

BSA members and other international technology providers face a particularly challenging commercial environment in China.[39] BSA members recognize the importance of resolving longstanding bilateral challenges with China and have seen first-hand the challenges and evolution of China's policies in the technology sector. China continues to present major market access challenges to BSA members. In 2017, the Government of China enacted the Cybersecurity Law,[40] which impose onerous cross-border data transfer restrictions and data localization requirements. Since that time, Chinese efforts to regulate cross-border data transfers have accelerated. BSA urges the US Government to continue to engage closely with the Government of China to make meaningful progress on the range of issues mentioned in this submission to ensure fair and equitable market access for BSA members and other US and foreign companies.

Market Access

Cloud computing, despite being identified as an area of strategic development in China, remains largely off limits to foreign Cloud Service Providers (CSPs) due to several policy challenges, including equity caps, investment restrictions, and connectivity requirements. These challenges are exacerbated by market entry barriers, such as restrictions on the ability to engage in cross-border data transfers and requirements to localize computing infrastructure.

BSA welcomed the commitments negotiated by the United States and China in relation to cloud service purchases in the so-called “Phase One” trade agreement. The Phase One purchasing commitments included payments for the use of IP, which encompasses royalties for the computer software. More critically, the Phase One agreement contains purchasing commitments that cover “cloud and related services”, a critical area of economic activity for US services exporters that have faced a challenging investment and export environment for these services for many years. Covered services include: (1) data hosting, processing, and related services; (2) telecommunication services; (3) computer services; and (4) information services. BSA urges both countries to continue working towards fulfillment of those important commitments.

Restrictions on Cross-Border Data Transfers

The Government of China has put in place several laws and regulations restricting the transfers of data across borders and forcing data to be stored locally including the CSL. For BSA members that provide cloud computing services or that rely heavily upon cloud computing for their business operations, these restrictions create an uneven playing field — advantaging domestic businesses that already have local infrastructure and preventing foreign businesses from operating efficiently or at all.

***Data Security Law*:** The Data Security Law (DSL), enacted on June 1, went into effect on September 1, 2021. The DSL (a) requires the State Internet Information Department to draft rules for all “other data handlers” (i.e., not just CII operators) to restrict those other handlers’ exportation of “important data”; (b) applies to “[any person] handling important data”; (c) requires the State to create a “categorical and hierarchical system for data protection” as well as “catalog of” for “important data”, and to assess the “importance” of data based on broad criteria relating to: economic development, social development, national security, the public interest, and the lawful rights and interests of citizens or organizations; (d) authorizes each region and department to set a “catalog of important data” within that region and in

---

[39] AmCham China: China Business Climate Survey Report, at: http://www.amchamchina.org/policy-advocacy/business-climate-survey/; *See generally,* BSA Cloud Scorecard – 2018 China Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_China.pdf.

[40] *Cybersecurity Law of the People’s Republic of China*, November 11, 2016 (CSL) (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm. Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

corresponding industries and sectors; and (e) requires the State to create a "monitoring and early warning system" for important data, which will apparently help it prevent the exportation of “important data”

Following the swift enactment of the DSL, the Cyberspace Administration of China and sectoral regulators such as the Ministry of Industry and Information Technology have developed guidelines to establish the requisite frameworks for data categorization and classification under the DSL. As China works on classifying the scope of “important data” and other data classifications under the auspices of the DSL, it will be important to ensure that those categories of classification are not overbroad and do not automatically and improperly sweep in data categories, such as intra-company data transfers (e.g., of internal business and operational data) that are otherwise protected.

***Personal Information Protection Law*:** The Personal Information Protection Law (PIPL)[41] took effect on November 1, 2021. Of particular concern are requirements for *ex ante* security assessments that impact data transfers that global companies have long engaged in for their daily business operations. The PIPL also raises the following concerns:

(1) data localization requirements for “personal information” (PIPL Art. 40) and highly restrictive data transfer provisions for “personal information” (PIPL Arts. 38-40);

(2) lack of definition or overbroad scope for key concepts that implicate data localization requirements and data transfer restrictions, including what constitutes a “justified need,” or a “large volume [of data]” (PIPL Art 40);

(3) mandates for data assessments requiring governmental notification and/or approval in conjunction with the data localization and data transfer provisions noted above (PIPL Art. 38(1), 40);

(4) proposed data transfer “standard contracts” that, while encouraging, may not be interoperable with standard contractual clauses under the EU General Data Protection Regulation (GDPR) or other established personal data protection frameworks (PIPL, Art. 38(3));

(5) the absence from the PIPL of other internationally recognized data transfer mechanisms, such as intra-corporate binding rules, trustmarks, and regional certifications (PIPL, Art. 38);

(6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established. (PIPL, Art. 39); and

(7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43).

BSA and 31 other global associations raised these concerns in a letter submitted to China during the drafting process, but the concerns were not addressed.[42]

***Measures for Security Assessment of Cross-Border Data Transfers*:** On September 1, 2022, the Measures for Security Assessment of Cross-Border Data Transfers of the Cyberspace Administration of China (CAC) took effect. These security assessment measures are required only for a limited subset of companies engaging cross-border data transfers – specifically:

- A critical information infrastructure operator or a personal information processor based in China (akin to a “data controller” under the GDPR) that processes personal information for 1 million or more persons;
- A transferor of “important data”;

[41] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[42] Multi-association Letter on Draft Personal Information Protection Law and Draft Data Security Law, June 2, 2021, at: https://www.globaldataalliance.org/downloads/en06022021gdachinadslpip.pdf

- A processor of the personal data of more than 1 million individuals; a transferor of personal information of more than 100,000 individuals; or a transferor of sensitive personal information of more than 10,000 individuals. The latter criteria apply to the period beginning on January 1 of the preceding calendar year.

CAC also issued the Guidelines on Application of Security Assessment of Cross-border Data Transfers (First Version) on August 31, 2022.[43]

Regulations on Promoting and Standardizing Cross-Border Data Transfers: On **March 22, 2024**, the CAC issued its long-anticipated final Regulations on Promoting and Standardizing Cross-Border Data Transfers. The Regulations, which went into effect immediately, do not appear to materially alter China's restrictive cross-border data policy regulatory landscape, but they do loosen some restrictions (e.g., on intra-company transfers of human resources data.

Negative Lists of Data Whose Transfer is Prohibited or Restricted: Throughout **2024**, several Free Trade Zones published catalogues of "important data" the transfer of which is explicitly be restricted. For example, on **May 17, 2024**, the Tianjin Free Trade Zone published its Data Outbound Management List – Negative List of data that cannot be transferred out of China without securing the approval of the local CAC authorities via a data security assessment, securing the approval of Chinese authorities pursuant to a standard contract, or securing a personal information protection certificate.

For example, the Tianjin Pilot Free Trade Zone's negative list covers 46 different data subclasses, including data subclasses that are typically publicly available in other countries, including: (1) international trade data; (2) international agricultural cooperation data; (3) agricultural market data; (4) place names and addresses; (5) meteorological data; (6) scientific data; (7) production data; (8) financial transaction data; (9) macro-economic statistics; (10) data about the Chinese language, history, customs or national values; and so forth.

Similarly, on August 30, 2024, authorities in Beijing the Data Export Management List (Negative List) of China (Beijing) Pilot Free Trade Zone ("Negative List") and the Administrative Measures for the Negative List ("Administrative Measures"). The Administrative Measures propose rules referencing 13 categories and 41 subcategories of data and for uniform identification of important data. The Negative List specify five industries – automotive, pharmaceutical, retail, civil aviation and artificial intelligence – which are a particular focus of Beijing's efforts to restrict data exports, outlining 23 business scenarios and 198 data elements subject to restrictions.

Foreign Direct Investment Restrictions

[43] The Guidelines on Application of Security Assessment of Cross-border Data Transfers require a person making a security assessment application to prepare:

- a certified copy of its unified social credit code certificate;
- a certified copy of its legal representative's ID card;
- a Power of Attorney appointing an agent handling the application related matters – a template of this is included in the Guidelines;
- a certified copy of the appointed agent's ID card;
- a completed Application Form for Security Assessment of Cross-border Data Transfers – a template of this is included in the Guidelines;
- a certified copy of the agreements or other legal documents with the overseas data recipients. (In practice, it may be preferable to fulfill this requirement by submitting a copy of a China-approved standard contract (if and when they are published. However, the viability of this approach remains to be seen);
- a Report of Self-assessment of Risks in Cross-border Data Transfers – a template of this is included in the Guidelines (including an explanation, and risk/compliance/mitigation analyses for each transfer); and
- other supporting documents and materials

US businesses seeking to operate in China are subject to a range of foreign direct investment restrictions, including equity caps, and in-country hosting requirements, as well as challenging processes for obtaining licenses and other prerequisites for entering the market. These restrictions are particularly acute for cloud computing services. For example, under China's Telecommunications Service Catalog and related measures,[44] China incorrectly classifies a wide range of technologies and services as value-added telecom service (VATS) or basic telecom service (BTS), when in fact they are computer or business services that utilize the public telecommunications network as a method of delivery. For example, the catalog classifies cloud computing, content delivery networks, and online interactive platforms (called information services) as telecommunications services. Foreign firms that provide value-added services in China can only operate through joint ventures, of which they may own no more than 50 percent for VATS and 49 percent for BTS. In short, because of the update, foreign firms that provide a range of IT services are now subject to explicit limitations on market access, which also apply indirectly to local partners of joint ventures.

Standards and Technical Regulations

Cybersecurity Classified Protection Scheme: In May 2020, China posted the final version of the Cybersecurity Classified Protection Scheme (CCPS),[45] a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL. The CCPS is a continuation of the Multi-level Protection Scheme (MLPS).[46] Like the MLPS, the CCPS ranks the importance of network and information systems, based on their importance to China's national security, social order, public interests, and the legitimate interests of individuals and organizations and unnecessarily excludes access to foreign technology to the networks of moderate to high national importance — constituting a significant point of concern for the industry at large. The Government of China continues to release supporting standards and guidance on implementing the CCPS. For example, the September 22, 2020 "*Guiding Opinions on Implementing CCPS and CII Protection Scheme*"[47] which includes new concepts such as supply chain security and applies the CCPS to critical infrastructure protection. The CCPS came into effect on November 1, 2020.

Encryption: The China National Information Security Standards Technical Committee (TC-260) continues to release a myriad of draft cybersecurity standards involving encryption for public comment. A consistent and worrying trend exhibited by these standards is the extent to which they can be used to make it more difficult to participate in China's market, by creating a basis for favoring locally developed products over those developed outside of China. Such changes to algorithms or encryption mechanisms create technical barriers to trade and undermine interoperability.

In late 2019, the Government of China enacted the Cryptography Law.[48] BSA is concerned with the law for several reasons. First, while the updated Law states that commercial cryptography would not be subject to import licensing or export controls, the subsequent draft implementation regulations released suggest otherwise. Certification requirements for commercial cryptography are also being introduced. This overall regulatory framework could potentially restrict foreign competition in commercial

---

[44] *Classification Catalogue of Telecommunications Services (2015 Edition)*, December 28, 2015 (Chinese), as revised in June 2019, at: http://www.miit.gov.cn/n1146290/n4388791/c69928928/content.html.
[45] *Cybersecurity Classified Protection Regulations (Draft for Comment)*, June 27, 2018 (CCPS) (Chinese), at: http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html?from=timeline&isappinstalled=0.
[46] *Administrative Measures for the Multi-level Protection Scheme of Information Security*, June 22, 2007 (MLPS) (Chinese), at: http://www.mps.gov.cn/n2254314/n2254409/n2254431/n2254438/c3697388/content.html.
[47] *Guiding Opinions on Implementing CCPS and CII Protection Scheme,* September 2020 (English) at: https://www.mps.gov.cn/n6557558/c7369310/content.html.
[48] *The Cryptography Law of the People's Republic of China*, December 2020 (Chinese), at: http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml; *China's New Cryptography Law – Still No Place to Hide,* December 2020, at: https://www.chinalawblog.com/2019/11/chinas-new-cryptography-law-still-no-place-to-hide.html#:~:text=The%20PRC%20National%20People%27s%20Congress,effect%20on%20January%201%2C%202020.&text=The%20Law%20provides%20that%20it%20welcomes%20foreign%20providers%20of%20commercial%20encryption.

cryptographic products. In implementation, it will also be important to avoid unwarranted source code disclosure requirements and to ensure that safeguards protect any trade secrets or other proprietary information. It is necessary for the USG to address the serious concerns of the software industry regarding privacy, security, and trade secret protection.

Sensitive Data Classification: In September 2024, the National Information Security Standardization Technical Committee (TC260) released the cybersecurity standard practice - sensitive personal information identification guidelines. The purported aim of the guidelines is to enhance the management and protection of sensitive personal information by outlining specific rules for identifying sensitive personal information, which includes data categories such as biometric information, religious beliefs, medical health, and financial accounts. Sensitive personal information is subject to much lower cross-border data permission thresholds (than other data types) by Chinese authorities under the PIPL, the Data Security Law, and the Cybersecurity Law.

Intellectual Property

Compliance and Enforcement: BSA and its members have had some success with China's IP Courts and tribunals. Unfortunately, we are observing capacity issues as the limited resources of those IP Courts and tribunals are tested against the growing backlog of cases. Given the positive experience BSA and our members have had with the existing system, BSA encourages the Government of China to establish additional specialized courts and provide more resources to the existing courts and tribunals.

Significant hurdles to effectively address the use of unlicensed software in China remain. In civil cases, most courts have relaxed excessively high burdens for granting evidence preservation orders, but others remain highly reluctant to issue such orders. Courts should also increase the amount of damages awarded against enterprises found using unlicensed software. China also needs to increase statutory damages beyond those currently proposed in the draft amendments to the Copyright Act.

The Criminal Case Transfer Regulations do not adequately address existing challenges to the effective transfer of administrative cases to criminal investigations and prosecution authorities. Some enforcement authorities have interpreted the regulations as requiring proof of illegal proceeds, rather than allowing transfer upon reasonable suspicion. Administrative authorities, however, do not employ investigative powers to ascertain such proof. We recommend that the regulations be updated to expressly include the "reasonable suspicion" rule.

D. European Union

Overview/Business Environment

Over the past several years, the European Union has modernized its digital economy regulatory and policy framework relevant to software and data service providers, in particular with regards to privacy, cybersecurity, data transfers, and copyright. The new European Commission is actively pursuing an assertive digital policy agenda, guided by at times competing ambitions to promote Europe's "digital sovereignty" while pursuing "open strategic autonomy." The European Strategy for Data adopted in February 2020 clearly endorses that the EU will maintain an open, but assertive approach to international data transfers and pledges that the EU will continue to address unjustified obstacles and restrictions to data transfers in bilateral discussions and international fora. However, calls for data localization or for measures that seek to ensure EU organizations are immune from third countries' extraterritorial legislation continue to have traction at EU level and in some Member States, especially in the wake of the CJEU Schrems II decision and in light of the increased reliance on global digital technologies during the pandemic. While BSA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, and in harnessing the value of data, some of the measures considered, including in the areas of data privacy, cybersecurity, data governance, and cloud resilience in the financial sector (the so-called the 'Digital Operational Resilience Act' (DORA)), may constitute *de facto* market access barriers or dramatically hinder the ability of US organizations to move data across border.

The EU-US Trade and Technology Council can be an important asset to the transatlantic digital policy debate. BSA encourages both sides to use the TTC to exchange on common priorities and seek joint outcomes on *inter alia* Artificial Intelligence, data governance and international data transfers.

Market Access

As the EU co-legislators develop and implement new proposals, BSA asks that the US Government closely follow these developments, work intensively to protect existing transatlantic data transfer mechanisms, and push back against policies that pose the most significant market access barriers.

Cross-Border Data Transfers: Measures that impede the transfer of data across borders impose substantial burdens on US service providers and negatively impact US jobs. European authorities are historically focused on data transfers to the United States. The Commission has recently applied similar levels of scrutiny to the United Kingdom and the Republic of South Korea as both Third Countries sought an adequacy decision, but has not yet done so to data transfers relating to other markets such as China or Russia.

A New US-EU Data Privacy Framework: In 2023, the United States and the EU launched a new Transatlantic Data Privacy Framework (DPF) to replace its predecessor Privacy Shield framework. The DPF is accompanied by an Executive Order (EO) on Enhancing Safeguards For United States Signals Intelligence Activities.[49] The EO creates new safeguards on US signals intelligence activities, establishes a new redress mechanism, and enhances US oversight of signals intelligence. In October 2024, the European Commission published a report on the first-year review of the DPF, concluding that U.S. authorities have put in place all the constitutive elements of the framework and adding they will carry out the next review in 2027.

EU Standard Contractual Clauses for Data Transfers: The European Commission released a new set of SCCs in June 2021. It is anticipated that another SCC will be issued in late 2024 or 2025. SCCs contain general clauses that are common to all transfer scenarios, as well as tailored modules applicable to different transfer scenarios. A particular challenge with the current SCC framework is the obligation for companies to undertake detailed legal assessments for each country to which data is transferred. Paragraph 20 states

[49] White House, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities (Oct. 2022), at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

that: "different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer." More detailed and consistent EU guidance on third country legal frameworks would be welcome.

Cybersecurity Certification Scheme for Cloud Services (EUCS): In 2024, the EUCS framework continued to represent a concerning development given the original inclusion of sovereignty provisions that discriminate against non-national cloud service providers. On the one hand, the proposed by the European Commission and the European Union Agency for Cybersecurity (ENISA) to remove references to sovereignty requirements from the EUCS is positive. On the other hand, the possibility that member states will be able to impose sovereignty requirements in national law on top of the technical requirements outlined (*see e.g.,* France's SecNumCloud) continue to present a challenge.[50] It will be important to ensure that, once the EUCS enters into force, any discriminatory national schemes are phased out, consistent with the EU Cybersecurity Act.

EU Data Act: BSA continues to be concerned with drafting ambiguities in the draft EU Data Act relating to cross-border data transfers. We continue to recommend that the Commission clarify the ambiguity and breadth of the text of Article 27.1 of the Data Act to make clear that "conflicts" with EU law or member state law are only expected to arise if the corresponding law expressly precludes the transfer of data to a particular third country jurisdiction. Conversely, if data transfers or access are halted in an unpredictable and broad manner, it could raise questions regarding the international obligations and the ability of EU and foreign entities to engage in cross-border commerce, R&D, and other activities.

Data Transfers in Trade Agreements with Third Countries: In 2024, the European Commission advanced new provisions on cross-border data transfers for purposes of its free trade agreement negotiations. These new provisions are an improvement over prior cross-border data transfer norms. However, additional room for improvement remains – particularly in relation to self-judging exceptions text relating to privacy matters.

For example, April 29, 2024, the EU Council adopted the protocol adding this new cross-border data flows provisions to the EU-Japan Economic Partnership Agreement. The protocol introduces proportionality and necessity tests for legitimate public policy objectives, and requires parties to provide for instruments enabling cross-border transfers. Once the agreement has been ratified by Japan, and the EU and Japan have notified each other about the completion of their internal procedures, the agreement can enter into force.[51]

Digital Operators Resilience Act (DORA): in September 2020, the European Commission adopted a new Digital Finance Package, which includes a proposal for an EU regulatory framework on digital operational resilience, the 'Digital Operational Resilience Act' (DORA). This proposed regulation aims at ensuring that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. The proposed legislation will require all firms to ensure that they can withstand all types of Information and Communication Technology (ICT) - related disruptions and threats and the proposal introduces an oversight framework for ICT providers, such as cloud computing service providers.

This proposal, which builds on the European Banking Authority guidelines for outsourcing to cloud providers, could have potentially negative consequences for cloud computing service providers to financial services companies, and the current recommendations from the guidelines would become mandatory. Those would include, among others, the imposition of model contract clauses that would cover inspection and audit rights, termination rights and exit strategies; a new EU supervisory body to

[50] See discussion on this point in Euractiv, Reuters.
[51] The EU-Japan negotiations concluded in principle on October 28, 2023; both Parties signed the Agreement on January 31, 2024; and the EU Parliament gave its consent to the protocol on March 14, 2024

oversee large cloud providers, or large penalties for non-compliance. Moreover, non-EU headquartered providers may be subject to higher levels of scrutiny.

E. India

Overview/Business Environment

The commercial environment for BSA members remains challenging in India. In addition to certain policy and regulatory developments that may require data localization and hinder cross-border data transfers, preferences for domestic products and services contained in certain procurement policies could restrict market access for BSA members.

AI Governance

Government of India's ambitious India AI mission spells out the roadmap for AI governance.[52] The Ministry of Electronics and Information Technology (MeitY) intends to promote the responsible and ethical use of AI-based tools but also promote AI innovation. This vision is borne out through the IndiaAI mission The Government of India is currently not considering policy proposals to regulate AI but MeitY is considering voluntary commitments by industry players and the setting up of an AI Safety Institute.

An inter-ministerial committee (Committee) formed under the office of the Principal Scientific Adviser (PSA) to explore approaches for governing AI in India. The Committee was formed around October-November 2023, composed of bureaucrats from the Department of Science & Technology, Department of Telecom, MeitY, and the Ministry of Home Affairs (MHA). A sub-committee also has been established under this committee to examine the gaps in existing laws/regulations and provide recommendations for an AI governance framework. The PSA's office is yet to release the report.

Digital India Act

The Government of India is currently NOT considering a revamp of the Information Technology Act (**IT Act**) due to existing political environment where the ruling party does not hold an independent majority in the Parliament floor. The Ministry of Electronics and Information Technology (MeitY) had earlier started the process to revamp the IT Act through a new Digital India Act (**DIA**) but the process has lost steam after the commencement of the third tenure of Prime Minister Modi in June 2024. MeitY would continue to amendment the IT Act as and when policy issues occur.

Personal Data Protection Bill

In Fall 2023, India's Digital Personal Data Protection (DPDP) Act was passed as law by Parliament. As compared with data transfer provisions in the draft Bill, the provisions in the final Act are significantly improved. Nevertheless, they continue to raise significant concerns. The Act presumes that personal data may be transferred outside of India. However, the Act creates broad and vague authorities for the Central Government to restrict transfers by data fiduciaries without setting clear guardrails around those powers. This is a critical issue for companies that rely on international data transfers and require a stable, predictable legal framework that supports transfers. However, the government has indicated that this power may be used sparingly, in exceptional circumstances.

More specifically, the Central Government is given broad authority to "restrict the transfer of personal data by a data fiduciary for processing to such country or territory outside India" upon notification. (Sec. 16(1).) In addition, the Bill does not restrict other laws from restricting transfers of personal data, which could create fragmented rules for transfer across different industries. (Sec. 16(2).)

Only a small number of scenarios are clearly outside the scope of any potential data transfer restrictions, including when personal data is necessary for enforcing any legal right or clam; personal data is processed in the interest of preventing, detecting, investigating, or prosecution of an offense under Indian law, processing is in the context of a merger, or when the processing is pursuant to a contract with a non-

[52] Cabinet Approves Over Rs 10,300 Crore for IndiaAI Mission, will Empower AI Startups and Expand Compute Infrastructure Access, Press Release by Ministry of Electronics and Information Technology https://pib.gov.in/PressReleasePage.aspx?PRID=2012375

Indian customer and relates to personal data of non-Indian residents. The Government of India is expected to conduct a public consultation on the implementing rules. The Government of India is expected to conduct a public consultation on the implementing rules. We urge the Government of India to provide some guardrails or guidelines to the cross-border data provisions of the PDPD Act in order to provide certainty to the industry.

Non-Personal Data Governance

On September 2019, MeitY constituted a Committee of Experts to develop a governance framework for non-personal data (NPD Framework). In August 2020, the Committee released its report.[53] In December, the Committee published the revised report.[54] In our written comments, BSA highlighted numerous concerns including mandatory sharing of proprietary non-personal data, restrictions on cross-border data transfers and local storage requirements.[55] Such mandatory obligations are counterproductive throughout the data ecosystem, and present additional complications if applied to "data processors," including enterprise software and cloud service providers. The framework proposes additional compliance obligations for businesses by creating a new regulator in addition to the proposed Data Protection Authority (DPA) under PDP 2019 and the proposed e-commerce regulator. The mandatory data-sharing framework proposed in the NPD framework is in addition to the sharing requirements proposed in the PDP 2019, which was withdrawn by MeitY by August 2022. There is a suggestion that such provisions may be revisited in the proposed Digital India Act or through amendments to the IT Act. Such proposals can have a chilling effect on innovation and investment in the digital economy. We urge India to avoid the proposal of such measures in the future.

Intermediary Guidelines

In December 2018, MeitY issued the Draft Information Technology [Intermediary Guidelines (Amendment) Rules] ("Draft Guidelines").[56] The Draft Guidelines include problematic filtering obligations that will create significant privacy and data protection concerns for consumers. BSA has highlighted these concerns and urged MeitY to eliminate unnecessary obligations imposed on businesses.[57] The revised Draft Guidelines were issued in February 2021 by placing heightened obligations on a new category of intermediaries called the 'Significant Social Media Intermediaries (SSMIs)' which partially addressed concerns raised by BSA. The MeitY has continued to amend the Guidelines, focusing on issues of online safety, content moderation and cybersecurity.

CERT-In Directions

In April 2022, the Indian Computer Emergency Response Team (CERT-In) released *'Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*' (Directions).[58] The Directions mandated many onerous obligations on cyber incident reporting including reporting of all cyber incidents within six hours besides validating all user information collected by service providers. Based on stakeholder feedback, CERT-In released FAQs which provided additional clarifications on some of the onerous provisions, but the Directions continue to remain a

[53] Report by the Committee of Experts on Non-Personal Data Governance Framework, August 2020, https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf
[54] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dec 2020, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf
[55] BSA Submission on Revised Non-Personal Data Governance Framework, January 2021, https://www.bsa.org/policy-filings/india-bsa-submission-on-revised-non-personal-data-governance-framework
[56] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 – Draft available at: https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf
[57] BSA Submission on Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 available at: https://www.bsa.org/files/policy-filings/01312019BSAResponseDraftIntermediaryGuidelinesMeitY.pdf
[58] Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet by CERT-In, MeitY accessible at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

challenge to implement for companies. [59] BSA highlighted these challenges in a letter to MeitY.[60] A As of 2024, the incident reporting guidelines as proposed by CERT-In continues to pose a challenge for the industry given the lack of clarity on the risk profile of incidents that need to be reported and the sharp timeline for reporting.

The Telecommunications Act 2023

In December 2023, the Indian Telecommunications Act, 2023 was passed by the Indian Parliament.[61] The Government indicates that it does not intend to apply the definition of "telecommunication services" to cover a wide range of internet and digital services under a telecom licensing requirement. However, due to the broad language, uncertainty remains. As of September 2024, the government has started the process of formulating implementing rules and the uncertainty continues to remain.

Public Procurement Preferences

Technology mandates and domestic preferences for government procurement have been clearly demonstrated as part of a larger "Make in India" initiative adopted by the Government of India.

The Make in India Order,[62] issued by the India Department for Industrial Policy and Promotion (DIPP) in June 2017 and revised in 2020 and 2021, aims to promote local manufacturing, requires every government department to give preference to local suppliers when procuring goods and services. The Make in India Order is the first enabling framework for preferential market access in software products and services. The order places an emphasis on the *situs* of manufacturing or provision of service (based on a definition of "local content"). However, government departments are granted the discretion to implement the Make in India Order according to their own requirements. By pegging procurement preference to 'local content', the order creates uncertainty and difficulty for global software companies to participate in any government tenders/procurement processes.[63]

Subsequently, MeitY issued the Draft Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order for public comment.[64] In July 2018, MeitY issued the final notification with only minor changes.[65]

The Notification and similar developments could significantly affect India's ability to acquire best-in-class products and services and negatively impact US companies' ability to effectively participate in public procurement opportunities.

This order poses a significant compliance challenge in particular to foreign software and cloud service providers (CSPs) to demonstrate local value add. This model does not consider the investments and other contributions made by foreign CSPs that enable the Indian Tech ecosystem and their global competitiveness, such as skilling initiatives, cloud innovation centers, quantum computing lab etc. Even if CSPs don't directly bid for government contracts, partners need to certify their percentage of local content, for which they rely on their vendors' local value addition as well. For example, where cloud services are a substantial cost element in a public procurement bid, percentage of local value add from

---

[59] Frequently Asked Questions (FAQs) on Cyber Security Directions of 28.04.2022 accessible at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf
[60] BSA concerns on the CERT-In Directions on Information Security Practices accessible at: https://www.bsa.org/files/policy-filings/05302022meitycertin.pdf
[61] The Telecommunications Act, 2023 accessible at: https://egazette.gov.in/WriteReadData/2023/250880.pdf
[62] *Public Procurement Order 2017 (Make in India Order)* at: http://dipp.nic.in/sites/default/files/publicProcurement_MakeinIndia_15June2017.pdf
[63] BSA Letter to MeitY on Public Procurement of Software at: https://www.bsa.org/policy-filings/india-bsa-letter-to-meity-on-public-procurement-of-software
[64] *Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order* (Draft Notification) at: http://meity.gov.in/writereaddata/files/Draft%20Notficationn_Cyber%20Security_PPO%202017.pdf.
[65] *Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products* at: http://meity.gov.in/writereaddata/files/public_procurement-preference_to_make_in_india-order_2018_for_cyber_security_products.pdf.

a CSP becomes important. Moreover, the Indian government is considering revisions to the order and increasing the minimum local content requirement for Class-I suppliers to 60% and Class-II suppliers to 30%.

Government procurement policies remain outmoded and inefficient because of local content and technology preferences. In 2020, DIPP (now the Department of Promotion of Industry and Internal Trade – DPIIT) revised the Public Procurement Order 2017 (Make in India Order), which requires government departments to give preference to local suppliers in procuring goods and services.[66] The Ministry of Electronic and Information Technology (MeitY)'s guidelines to government departments on cloud services contracts also contain requirements for data to be localized in India.[67] In addition, the Draft National Policy on Software Products would promote the use of domestically developed software products in public sector procurements and strategic sectors like defense, telecommunications, energy, and healthcare. Such policies do not offer a level playing field to US technology providers that are bringing cutting-edge technologies and services to India. Amendments to the Make in India Order as of September 2024, have not addressed these concerns and rather advanced the government's preference for products that has local value addition.

[66] *Make in India Order*
[67] *Guidelines for Government Departments On Contractual Terms Related to Cloud Services* at: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.

F. Indonesia

Overview/Business Environment

The commercial environment for the software and IT sector in Indonesia is very challenging. A variety of authorities have issued, or are in the process of developing, policies that will make, or threaten to make, it increasingly difficult to provide digital products and services to the Indonesian market.

Market Access

A variety of policies affecting the IT industry have been developed or proposed over the last several years that make, or threaten to make, it increasingly difficult to provide digital products and services to the Indonesian market.

Duties on Digital Products: In February 2018, the Ministry of Finance (MOF) issued Regulation 17, which amended Indonesia's Harmonized Tariff Schedule (HTS) to add Chapter 99 "[s]oftware and other digital products transmitted electronically."[68] Although Chapter 99 is currently duty free, Chapter 99 effectively treats electronic transmissions as imports, to which customs requirements apply, including requirements to comply with all customs laws that attach to imports, prepare and file import declarations, and pay 10 percent value-added tax (VAT) and 2.5 percent income tax. Indonesia supplemented these provisions with a new Regulation 190, which imposes a customs tariff currently set at 0% and requires the filing of import declarations for data moving across transnational digital networks – the first such measure of its kind anywhere in the world.

Personal Data Protection: Indonesia has been developing a draft Personal Data Protection (PDP) Bill since 2014 and successfully enacted the PDP Bill on October 17, 2022. Based on BSA's reading of the law, it draws from several principles and aspects of the European Union's General Data Protection Regulation (GDPR), focusing on five main areas: data collection, data processing, data security, data breach, and the right for individuals to have their personal data erased. BSA's chief concerns with the law relate to potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors. The law provides for a two-year grace period for data controller and data processors to adjust their practices to comply with the law. A data protection authority that reports to the President will be set up within this period. Unfortunately, with only a short time before the Law will take effect, neither the implementing regulations nor the regulation directing the establishment of the DPA have been issued. We are concerned that there will be no grace period for organizations to adjust to the new rules, and this has been confirmed informally at meetings with KOMINFO.

GR71*:* Government Regulation 71/2019, revising GR 82/2012, requires public and private sector electronic system operators (ESOs) to register their electronic systems and requires private sector ESOs to facilitate "supervision" by government agencies, including by granting access to electronic systems and data for monitoring and law enforcement purposes. Our latest interactions with KOMINFO on this confirm that they are contemplating amendments to GR71 that seek to encourage investment in data centers through data localization regulations. However, no draft amendments have been released.

GR71's implementing regulations continue to be a significant barrier to digital trade. Public Scope ESPs are defined to also include public administration which goes beyond national security and intelligence data. No further clarity has been made on the circumstances by which data can be stored and processed offshore in the case of Public Scope ESP including the guidelines that KOMINFO will use when reviewing every individual data offshoring request by Private Scope ESPs. KOMINFO's implementing Regulation No. 5/2022 requires private sector ESOs to register with KOMINFO through an Online Single Submission (OSS) system or face significant penalties for non-compliance including blocking by KOMINFO. Failure to comply with government takedown orders for a potentially broad category of "prohibited electronic information" can also result in blocking.

---

[68] *Regulation No. 17/PMK.010/2018 (Regulation 17)* (Indonesian) at: https://jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf.

Cloud Services: Indonesia's regulatory framework is among the least conductive for the adoption of public cloud technology in the financial services industry. The biggest barriers are in the form of data localization, burdensome requirements to seek prior regulatory approval, and the lack of differentiation in the materiality of workloads. To begin, the financial regulator (OJK) does not permit transactions to be processed offshore in sectors like such as multi-financing and lending based technology. These rules are reportedly motivated in part by regulators' lack of trust in multilateral law enforcement systems. Second, the OJK requires financial institutions to go through a lengthy approval process before moving workloads to the public cloud. This applies to commercial banks planning to operate an electronic system outside Indonesia and financial institutions that plan to outsource the operation of their data centers or disaster recovery centers. Additionally, Regulation No. 9/POJK.03/2016 only allows commercial banks to outsource "support work" (i.e., activities that are low risk, do not require high banking competency and skills qualification, and do not directly relate to operational decision-making). These workloads that can be outsourced are all subject to the same regulatory requirements, with no differentiation in terms of materiality, unlike in other jurisdictions, such as Australia and Singapore.

Data Localization in the Financial Sector: The Bank of Indonesia still requires core/important financial transactions to be processed domestically. The Financial Services Authority (OJK) has incrementally allowed some electronic processing systems to be based offshore for banking services, insurance services, multi-financing services, and lending-based technology, but for the most part, the policy remains highly restrictive and burdensome for global companies trying to operate within Indonesia.

Local Content Requirements for Software*:* Indonesia's Ministry of Industry issued regulation No.22/2020 (IR22) on the Calculation of Local Content Requirements (LCR) for Electronics and Telematics, with a government target to achieve 35% import substitution by 2025. IR22 provides specific and extensive requirements for manufacturing and development for both digital and non-digital physical products. The government has signaled an intention to build on this LCR requirement and add similar LCRs for software and applications, which would impact companies that provide services over the internet, including cloud services. In addition to that, Presidential Instruction Number 2 Year 2022 requires government agencies to plan, allocate, and realize at least 40% of the national budget for goods/services to utilize MSMEs and Cooperative products from domestic production.

G. Japan

Overview/Business Environment

Japan has a strong market for software-enabled products and services with a comprehensive suite of modern laws that support and facilitate the digital economy. However, the Government of Japan must accelerate the uptake of cloud services and digital transformation in the public and private sectors.

In 2021, Japan established the Digital Agency,[69] which functions as the control tower to promote digital transformation across society, including management and oversight of central government information systems, standardization of local government information systems, improving administrative services utilizing the My Number (personal number) system, and digitalization in various fields including education, disaster prevention, and medical care through better use of data.

Prime Minister Kishida created a new ministerial post for economic security in the Cabinet, aiming to strengthen Japan's "strategic autonomy" and promulgated the "Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures"[70] in May 2022 which includes the introduction of a new system by the Government to pre-examine the installation and entrustment /management/control of specified critical facilitiest used in specified essential infrastructure services to ensure that they are not used as means to "interfere the stable provision of services from outside Japan". BSA has recommended that the government ensure that these policies are cohesive, embrace well-defined criteria; and are based on robust public consultation. Also, Japan should avoid a misunderstanding that locally hosted data is safer, when in fact it is subject to many of the same cyberattacks as cloud services.

Cloud Security Assessment

The Government of Japan launched the Information System Security Management and Assessment Program (ISMAP)[71] in 2020, a cloud security assessment program for government procurement, creating a register of cloud services that have met security requirements for central government procurement. While the Government's commitment to promote a "cloud-by-default' principle is a positive move, the ISMAP imposes high hurdles to be registered on the ISMAP Cloud Service List. BSA has urged the Government to reduce repetitive auditing process by exempting the application of security controls that are duplicative with internationally recognized standards for which certifications have already been received. Given that many global CSPs already have internationally accredited certifications (e.g., ISMS-JISQ/ISO 27000 series, SOC2), acknowledging them and eliminating repetitive procedures and requirements to reuse evidence already provided in prior certifications from ISMAP will contribute to alleviating the burden on the Government of Japan and on CSPs. In an era of friend-shoring and ally-shoring, we urge Japan to avoid imposing requirements that are significantly more onerous than internationally accredited certifications would be.

AI Governance

BSA welcomes the Japanese government's "Approach to AI Systems" publication, and encourages Japan's AI Strategy Team to focus on regulatory interoperability with the United States and other allied economies. This should include ensuring that any certification and testing requirements are focused on high-risk uses of AI. Imposing such requirements on low risk AI would deter innovation by small and medium enterprises in both the US and Japan, thus undermining the broader US-Japan AI ecosystem.

---

[69] https://www.digital.go.jp/en
[70] https://elaws.e-gov.go.jp/document?lawid=504AC0000000043_20230517_000000000000000 (Japanese) https://static1.squarespace.com/static/5eb491d611335c743fef24ce/t/627dec876ba75369ad752dc6/1652419721341/Economic+Se_ (unofficial English translation); Official English translations, at: https://www.japaneselawtranslation.go.jp/ja/laws/view/4716 and https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/pamphlet_dounyu_eng.pdf
[71] https://www.ismap.go.jp/csm?id=csm_ismap_index

Physical Network Separation

The Ministry of Internal Affairs and Communication (MIC) issued “Guidelines on Information Security Policy for Local Governments (Guidelines)”[72] which continue to support the use of physical network separation as a cybersecurity solution. This guidance discourages government agencies from adopting the latest commercial cloud computing and related services. BSA has highlighted the need to modernize security approaches through public-private sector collaboration and to promote policies supporting a "cloud-native" architecture that are not based on physical network separation.

[72] https://www.soumu.go.jp/main_content/000805453.pdf; https://www.soumu.go.jp/main_content/000970479.pdf

G. Republic of Korea

Overview/Business Environment

The overall commercial environment in the Republic of Korea (South Korea) for BSA members and the software sector is mixed. South Korea has a strong market for software-enabled products and services and a mature legal system. However, the Government of South Korea has policies that present substantial market access barriers to foreign software products and services. Such policies include local testing requirements and requirements to comply with national technical standards even when commonly used internationally recognized standards are available. Data residency, physical network separation, and other requirements for industry sectors, such as government/public services, finance, healthcare, and education, hamper the ability to provide cloud-based services to users in these sectors. These requirements may also be institutionalized by the National Assembly, with a bill recently proposed to create legal bindings to Cloud Security Assurance Program (CSAP).

Market Access

The adoption of procurement preferences for domestic firms and imposition of additional burdensome measures, often with security concerns cited as justification, have decreased market access for BSA members in South Korea. These policies especially affect those providing software-enabled services, such as cloud-computing and data analytics services.

Cross-Border Data Transfers and Server Localization: It remains very difficult for commercial cloud services providers (CSPs) to offer cloud services to entities in South Korea's very broadly defined public sector. This is due to onerous certification requirements imposed by the Korea Internet Security Agency (KISA) under the Cloud Security Assurance Program (CSAP) on CSPs that provide cloud services to public sector agencies and requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data onshoring apply to healthcare sectors.[73]

Recent amendments to the CSAP in 2023 created a tiered system that classifies public sector data systems into three grades — "High", "Medium", and "Low" — depending on the sensitivity of data handled. Under these amendments, CSPs certified to manage public sector data systems at the "Low" level are not required to use physical network separation and instead may use logical network separation to keep customer workloads distinct. However, all three levels of CSAP classification will continue to require CSPs to ensure data residency and use only Korea-developed encryption algorithms (i.e., ARIA and SEED) rather than those more widely used and vetted internationally. As such, the amendments do not adequately address the technical and administrative burdens presented by CSAP, and significant barriers to providing cloud computing and related services in South Korea remain. Given the emergence of different third party security assessment requirements in Australia and Japan, it would be helpful to promote greater alignment and potentially cross-recognition of these requirements.

Physical Network Separation: Although the Government of Korea is committed to promoting the adoption of cloud computing, security concerns by the National Intelligence Service (NIS) have resulted in policies requiring physical network separation. Physical network separation requirements prevent or discourage government agencies and other regulated sectors (e.g., healthcare) from adopting commercial cloud computing and related services.

In 2016, the Ministry of the Interior and Safety (MOIS) and the Ministry of Science and ICT (MIST) adopted the CSAP, announcing certain revisions in 2019.[74] Since 2016, the CSAP has contained

---

[73] On June 1 of 2020, a new certification framework that includes CSAP requirements was applied to electronic medical records. *See* Enforcement Decree of the Medical Service Act (Article 10-5: Standardization of Electronic Medical Records) (indicating that "matters subject to standardization to be determined and publicly notified by the Minister of Health and Welfare pursuant to Article 23-2 (1) of the Act shall be as follows: "2. Facilities and equipment necessary for the safe management and preservation of electronic medical records under Article 23 (2) of the Act").
[74] *See* https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939.

problematic physical network separation requirements.[75] In other mature markets, physical network separation requirements are rarely applied throughout the public sector, including in workloads or institutions that handle non-sensitive (and sometimes, public) data, such as public universities. The uniformly applied physical network separation requirements do little to enhance security while undermining the main benefit of cloud computing services, which is the economy of scale and state-of-the-art security capabilities of multi-tenant cloud services. As described in BSA's August 2019 comments,[76] these requirements will have a negative impact on South Korea's digital ecosystem and curtail its ability to participate effectively in the global digital economy — raising the cost of providing services and inhibiting the choice of technology available to end-users and procuring entities. The costs associated with such additional infrastructure will need to be recovered, which would ultimately increase the costs for end consumers.

South Korea's regulatory environment for the use of cloud services in the financial services sector has improved somewhat of late. The Financial Services Commission (FSC) allowed logical network separation and enabled the use of AI and cloud services, and recently approved the use of personal credit information by public cloud services and may be considering additional measures to expand the ability to manage financial data on the public cloud. However, the FSC specifically requires that such data be maintained on servers located in South Korea.[77]

Encryption: The revisions to the CSAP require that "cloud computing services providers shall use government-certified standard encryption technology when providing an encryption method for important material created through the cloud service." These kinds of national approaches to encryption requiring the use of locally selected algorithms rather than internationally recognized algorithms, however, constrain the choices of technologies available to organizations and citizens in South Korea, including leading edge security solutions that defend against latest threats. Cryptography certification in South Korea also requires a review of source code, which could raise concerns regarding protection of proprietary information and trade secrets. This is also impractical for many leading cloud service providers, which already use state-of-the-art encryption algorithms that meet internationally recognized standards and are accepted for applications in the most sensitive circumstances in other markets. In fact, as outlined in BSA's comments, this kind of fragmented and piecemeal approach that only allows the use of domestically certified encryption standards may deprive organizations from using best-in-class encryption technologies, and this would weaken rather than strengthen the protection of sensitive data.[78] There are indications that the government may be willing to exclude Korea-specific altorighms like SEED and ARIA from their requirements, and we would urge the US Government to continue advocating for that change.

Personal Information Protection Regime: South Korea's personal information protection regime is one of the most stringent in the region and has significantly decreased the ability for BSA members to serve the South Korean market.

In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[79] the Act on Promotion of Information and Communication Network Utilization and

---

[75] As of the 2019 amendments, the physical network separation requirements stipulate that, "the physical location of the cloud system and data shall be restricted to in country and cloud service area for public institutions shall be physically separated from the cloud service area for private institutions."
[76] Comments available at: https://www.bsa.org/files/policy filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.
[77] E.g., under RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.
[78] Comments available at: https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.
[79] *Personal Information Protection Act* (2017). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.

Information Protection (Network Act),[80] and the Credit Information and Protection Act.[81] The primary result of the legislative package is to consolidate the legal protection and enforcement provisions for personal information primarily in the PIPA, and to elevate the Personal Information Protection Commission (PIPC) to a central government-level agency under the Prime Minister.

The PIPA has subsequently undergone further amendments. and the European Commission has issued "adequacy" recognition to South Korea. However, more work is required to reform South Korea's personal data protection regime. There should be a clearer distinction between data controllers versus data processors to better delineate the roles and responsibilities of different entities. South Korea should also adopt measures that expand the legal basis for processing personal information beyond consent. This would enhance investment and innovation in emerging technologies, like data analytics and machine learning, while ensuring that personal information is appropriately and adequately protected.

In April 2024, Korea's Personal Information Protection Committee (PIPC) published its PIPA Compliance Guidelines for Overseas Businesses (Guidelines). The Guidelines and the associated press release can be accessed at this link. In brief, the Guide is intended to make clear the legal obligations that will apply to overseas businesses under the recently revised PIPA. The Guidelines address three categories of overseas businesses: (1) overseas businesses that provide goods or services to Korea data subjects; (2) overseas businesses that process personal information of Korea data subjects in a way that affects them; and (3) overseas businesses that have a business establishment in Korean territory.

Discriminatory Security Certification Requirements Applied for Foreign IT Products: Since 2011, the Government of Korea has imposed additional security verification requirements for international Common Criteria (CC)-certified information security products that are procured by government agencies. In 2014, the Government of Korea extended similar security conformity testing requirements to international Common Criteria-certified networking products procured by any South Korean government agency.

South Korea is a member of the Common Criteria Recognition Arrangement (CCRA) and therefore should recognize international certifications from accredited laboratories and should not impose further requirements for Common Criteria-certified products.[82] The additional requirements are in tension with the spirit of CCRA, which is to "eliminate the burden of duplicating evaluation of IT products and protection profiles."[83]

The NIS revised the Security Evaluation Scheme (SES) in early October 2022, allowing institutions with relatively low security sensitivity, such as basic-level local governments and public schools, to use internationally CC-certified ICT products without additional domestic security verification. However, most major public institutions which account for an overwhelming proportion of the public sector market, including all central administrative institutions and metropolitan local governments, are still required to only use products with domestic security certification, limiting market access for US companies.

Copyright and Enforcement

Compliance and Enforcement: Criminal enforcement has been an effective mechanism for BSA members to protect their rights and enforce against the use of unlicensed software by enterprises in South Korea. The police, the prosecutors' offices, and the special judicial police under the Ministry of Culture, Sports, and Tourism (MCST) are the authorities primarily involved in enforcement activities

[80] *Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act)* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.
[81] *Credit Information and Protection Act* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.
[82] Common Criteria Recognition Arrangement (CCRA) at: https://www.commoncriteriaportal.org/ccra/
[83] CCRA

against enterprises using unlicensed software.

The special judicial police are specifically tasked with investigations and inspections concerning copyright violations and they are relatively active in conducting enforcement activities against enterprises using unlicensed software. However, they have limited resources and BSA members also rely on the enforcement actions of the police. In line with the Government of Korea's goal of reducing the rate of unlicensed software use, BSA recommends that the special judicial police increase its resources with a view to increasing the volume of enforcement activities against infringers.

BSA members also rely on civil litigation to take action against enterprises using unlicensed software. However, more can be done to improve the current system. For example, although preliminary injunctions are available, they are not often issued. It is also difficult to acquire evidence in civil cases without first going through a criminal raid. The option of aggravated damages is also not available to copyright holders under South Korean law. As a result, the damages awarded in civil cases tend to be too low to compensate rights holders or to deter future infringements. South Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules in civil cases.[84]

[84] *Civil Procedure Act* (2017). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

H. Singapore

Overview/Business Environment

Singapore has a strong market for software-enabled products and services and comprehensive and well-functioning legal system to enable the development and deployment of such technologies.

The Government of Singapore has generally consulted with industry prior to introducing legislative changes. However, in a few important instances, the Singapore Government has tended toward closed consultations with a select group of key industry players without adequately consulting the breadth of stakeholders that will be both affected by, and could contribute to, such legislation and policy making.

Cybersecurity Act

In February 2018, Singapore enacted its first comprehensive law on cybersecurity and critical infrastructure protection, the Cyber Security Act.[85] This was the culmination of several years of intense consultation. The substantial input the Cyber Security Agency (CSA) received from industry and other interested stakeholders led to substantial improvements in the final legislation.[86]

In 2022, the CSA announced revisions to the Cybersecurity Code of Practice (CCoP).[87] Initially, the CCoP were informed primarily by consultations with the affected critical infrastructure (CI) operators, and only later were providers of cloud computing systems and other software-enabled services upon which CI operators rely for many of their cybersecurity and information technology needs consulted.[88]

It is important that consultations involving any further amendments to the Cyber Security Act or its implementing rules involve all relevant stakeholders, especially BSA members that provide globally leading services and security to many sectors and customers, including CI operators. These consultations must provide adequate time for meaningful information exchange.

Online Safety Bill

The Online Safety Bill is intended to tackle harmful content available on online services in Singapore and is largely targeted at social media services.[89] Similar to CSA's approach with the Cybersecurity Act, the Infocomm Media Development Authority (IMDA) engaged with large social media providers on the Online Safety Bill but did not include other organizations in the eco-system that would potentially be affected by the Bill. For example, enterprise software organizations which deliver online communications services that are adjacent to the social media services that the Bill targets were not consulted, though they were caught by the broad definition of "online communication service" under the Bill. The result is that IMDA did not have the opportunity to hear from other stakeholders on how to better target the Bill's scope and obligations to achieve the stated objectives without interfering with commercial activities.[90]

While these instances do not, in themselves, constitute a trend, it is worth reiterating that Singapore, as a model of good governance in the region and the world, should redouble its efforts to ensure that legislation with wide-reaching effects on the industry at large are subject wider industry consultations that include the range of affected stakeholders.

---

[85] Cyber Security Act, https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312
[86] Joint Association Comments on Singapore Cybersecurity Bill, August 2017, https://www.bsa.org/policy-filings/singapore-joint-association-comments-on-singapore-cybersecurity-bill
[87] CSA Website – Codes of Practice/Standards of Performance, https://www.csa.gov.sg/Legislation/Codes-of-Practice
[88] BSA Submission on the Cybersecurity Code of Practice, May 2022, https://www.bsa.org/policy-filings/singapore-bsa-submission-on-the-cybersecurity-code-of-practice
[89] Online Safety (Miscellaneous Amendments) Bill, https://sso.agc.gov.sg/Bills-Supp/28-2022/Published/20221003?DocDate=20221003
[90] BSA Comments on Online Safety Public Consultations in Singapore, August 2022, https://www.bsa.org/policy-filings/singapore-bsa-comments-on-online-safety-public-consultations-in-singapore

I. Thailand

Overview/Business Environment

The Royal Thai Government (RTG) is pursuing a range of policies under Thailand 4.0 to promote the digital economy. Two important pieces of legislation enacted in 2019 — one on cybersecurity protection of critical infrastructure, and the other on personal data protection — are important elements of this effort, although the Government has yet to release implementing regulations for public consultation across all issues. BSA agrees that it is important for Thailand to have robust and effective cybersecurity and personal data protection legislation. However, we remain concerned that the implementation of both laws could undermine the RTG's efforts to enhance cybersecurity and personal data protection, interfere with the government's broader goals to drive Thailand 4.0, and unfairly impede BSA member companies' ability to effectively provide products and services to the Thai market.[91]

Market Access

BSA shares the goals of the RTG's Digital Economy initiative, Thailand 4.0, and supports the thoughtful implementation of personal data protection and cybersecurity legislation. The RTG should, however, consider measures to minimize the potential unintended effects of recently enacted cybersecurity and personal data protection legislation that could harm the ability of BSA members and other technology sector companies to provide innovative and effective software products and services.

Security: In May 2019, Thailand enacted its Cybersecurity Act to strengthen the capabilities and authorities of government agencies to prevent, cope with, and mitigate the risk of cyber threats, especially with respect to critical information infrastructure. The Cybersecurity Act raises concerns as it gives the National Cybersecurity Committee (NCSC) broad powers to enter into premises, to monitor and test computers and computer systems, and to seize or freeze computers, computer systems, and equipment, without sufficient protections, such as opportunities to appeal or limit such access. Such broad powers would undermine public confidence and trust in information technology (IT) generally and harm the ability of BSA members to provide the most innovative and effective software solutions and services to the Thai market.[92] There is also criminal liability for organizations and individuals who do not comply with executive orders issued under the Cybersecurity Act.[93]

In August 2021, the Ministry of Digital Economy and Society (MDES) issued a new Notification on "Criteria on Storing Computer Traffic Data of Service Providers B.E. 2564 (2021)" ("New Notification") to replace the previous Notification of Ministry of Information and Communication Technology Re: Criteria on Storing Computer Traffic Data of Service Providers B.E. 2550 (2007) (the "Previous Notification"). This Notification took effect on 14 Aug 2021 without any prior industry consultation, giving digital service providers only 180 days from this date to comply. The new regulation will require Data Centers and Cloud Service Providers to collect and retain extensive user information (e.g. identity info and activity logs) to facilitate authorities' access to users' data. This new regulation will increase compliance costs to both service providers and users, reduce competitiveness for small operators, and risk violating users' privacy rights.

---

[91] *See generally*, BSA Cloud Scorecard – 2018 Thailand Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Thailand.pdf

[92] See BSA's comments, available at: https://www.bsa.org/~/media/Files/Policy/Data/05062015SubmissionCybersecurityBill_EN_DeputyPrimer.pdf; https://www.bsa.org/~/media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf; and https://www.bsa.org/~/media/Files/Policy/Data/10122018EN_BSACommentsCybersecurityBillwith%20Annexes.pdf

[93] In addition to the foregoing measures, the Ministry of Digital Economy and Society (MDES) also issued a so-called Emergency Decree on Electronic Meetings, stipulating that electronic meetings on confidential matters must be conducted through a meeting control system established within the country. As reported, this measure raises concerns about its ambiguity, as well as concerns regarding the imposition of such a local development condition.

Personal Data Protection: The Personal Data Protection Act (PDPA) was enacted in May 2019 and is Thailand's first omnibus legislation on personal data protection. It is designed to build public trust and confidence in the digital economy and to implement the Asia-Pacific Economic Cooperation (APEC) Privacy Framework's principles for cross-border data transfers.[94] It also heavily draws from the General Data Protection Regulation (GDPR) of the European Union. BSA's chief concerns with the PDPA relate to prescriptive and burdensome notification and consent requirements for the collection, use, and disclosure of personal data. There are also potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors.[95]

In May 2020, the Thai Cabinet approved a royal decree granting a one-year exemption from certain provisions of the PDPA 2019, which had been scheduled to take full effect on May 27, 2020. On 5 May 2021, the Cabinet decided to further extend the fully effective date of the PDPA under the Previous Royal Decree from 1 June 2021 to 1 June 2022. The provisions which are exempted include: consent requirements, notification requirements, establishment of lawful basis, requirements on the collection of personal data from other sources, and processing of minors' personal data. The enforcement of a second list of requirements is also postponed, including observance of data subjects' rights and data erasure or destruction requirements, the implementation of appropriate internal security measures to prevent unauthorized access, provision of data breach notifications, appointment of data protection officers (DPOs), filing complaints, and penalties.

The Personal Data Protection Committee (PDPC) was formally established in January 2022. The PDPC has issued a few sets of draft notifications covering topics such as records of processing activities for data processors, security measures for data controllers, rules for the imposition of administrative penalties by the Expert Committees, international transfers of personal data, responsibilities of data processors, data protection impact assessments and obligations of data controllers related to automated processing. The most recent public hearing was for the Draft Notification of the PDPC on Rules and Principles of Appropriate Personal Data Protection for International Transfer, which closed recently on October 24, 2022.[96]

Copyright and Enforcement

BSA enjoys good cooperation with RTG authorities, including with the Economic Crime Suppression Division (ECD) of the Royal Thai Police, in addressing unlicensed use of software in Thailand.

Compliance and Enforcement: Thailand has a specialized intellectual property (IP) court, which has improved the effectiveness of IP litigation in Thailand. Unfortunately, though damages awarded in civil litigation are occasionally reasonable, award amounts are very inconsistent and often inadequate to compensate the rights holder or deter future infringements. Expenses are often awarded, but only very small amounts, and they do not typically cover the actual legal costs. Preliminary injunctions are not granted regularly enough to be an effective tool. In addition, although criminal cases can be effective in Thailand, the courts should apply more deterrent penalties for convictions. In recent cases, courts imposed only a fraction of the potential fines or refrained from imposing any fines at all — simply suspending sentences — even in cases involving significant infringements.

---

[94] *APEC Privacy Framework* at: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework
[95] See BSA's comments, available at: https://www.bsa.org/policy-filings/thailand-bsa-comments-on-the-draft-notification-on-rules-and-methods-of-personal-data-breach-notification-under-the-personal-data-protection-act-2019
[96] https://insightplus.bakermckenzie.com/bm/data-technology/thailand-new-cross-border-data-transfer-rules-officially-published-as-law

J. Vietnam

Overview/Business Environment

Over the past several years, Vietnam has enacted, implemented, and proposed various protectionist measures to regulate the software sector. These measures are likely to reduce fair and equitable market access for BSA members who wish to provide software products and services in Vietnam.[97] The enactment of the Cybersecurity Law in June 2018, and current efforts to develop implementing rules, only exacerbate the existing challenges and threaten to make Vietnam an even less attractive destination for the delivery of cutting-edge software products and services.[98]

Market Access

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). The Law went into effect on January 1, 2019.

The Law raises serious concerns and will likely significantly impact the ability of many BSA members to provide software products and services in Vietnam. The breadth of the Law far exceeds cybersecurity protection and extends to a broad regulation of the Internet generally. The Law also grants vast powers to authorities and imposes stringent requirements on software product and service providers to comply with local cybersecurity standards and regulations and to apply for certification by local agencies. In sum, the Law is a significantly negative development in Vietnam's market access environment for the software sector.

On August 15, 2022, the Ministry of Public Security (MPS) published the final Decree No. 53/2022/ND-CP (Decree 53) that took effect from October 1, 2022. Decree 53 is concerning because it requires domestic enterprises (potentially including domestic customers of foreign service providers) to store data within Vietnam and it is not clear whether domestic enterprises include foreign-invested enterprises or subsidiaries of foreign or multinational corporations with head offices in Vietnam. While Decree 53 is silent on the transfer of data overseas, it requires affected enterprises to store data in Vietnam. This leads to market access issues if domestic enterprises are unable to use cloud-based services that do not or cannot store data in Vietnam as part of their services.

***Personal Data Protection Decree*:**

Following two rounds of public consultations on the draft PDP Decree, in September 2021, the MPS submitted their revised draft PDP Decree to the Ministry of Justice (MOJ) for internal appraisal. However, this version of the draft PDP Decree was kept strictly confidential.

With the issuance of Resolution 27 in March 2022 approving the substantive content of the latest draft PDP Decree, the MPS was assigned to consult the National Assembly on the draft. The draft PDP Decree was expected to be passed in May 2022 following review by the National Assembly. However, this process has been delayed. BSA understands that the draft PDP Decree is still pending at the National Assembly Standing Committee because the lawmakers are waiting on the Central Politburo's comments, which has delayed its passage till now (October 2022).

The MPS has also been assigned to take charge and coordinate with the MOJ to propose the formulation of a Personal Data Protection Law after the PDP Decree has been passed

---

[97] *See generally*, BSA Cloud Scorecard – 2018 Vietnam Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Vietnam.pdf

[98] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) at: https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/. Another measure that we continue to monitor is Vietnam's Outline of Draft Decree on Personal Data Protection, which was published for public comments earlier this year, contains registration requirements for processing of sensitive personal data and transfer of personal data of Vietnamese citizens overseas.

Based on previous iterations of the draft PDP Decree, the PDP Decree will likely impose restrictive data transfer and data localization requirements. In addition, there are also burdensome requirements for personal data processors to store data transfer history for three years, register with the Personal Data Protection Commission (PDPC) for cross-border transfers of sensitive personal data with very detailed requirements for registration, and for the PDPC to carry out annual assessments or audit-like exercises on cross-border data transfers by personal data processors. These obligations are not only impractical, but they may also create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

Draft Decree on Administrative Penalties in the Field of Cybersecurity: On September 23, 2024, the MPS also released a draft Decree on Administrative Penalties in the field of Cybersecurity, to be adopted on the basis of the Cybersecurity Law. Among others the draft details a number of infractions to the draft PDP Decree. The publication of this draft Decree, which is currently open for consultation, came as a surprise because the main PDP Decree is yet to be finalized. It does, however, provide insights in some of the key provisions under the PDP Decree such as data transfers, consent, data breach notification, etc. The latest draft was published in May 2024 and slated to take effect on June 1, 2024, but it has yet to be officially promulgated.

MIC Decisions 1145 and 783: In 2020, under the auspices of Vietnam's National Digital Transformation Strategy by 2025, the Ministry of Information and Communications (MIC) issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, for state agencies and smart cities projects. These measures may create a preferential framework for domestic cloud service providers, and measures currently characterized as "voluntary" will be treated as *de facto* requirements.

Decree 72: In July 2021, the Ministry of Information and Communications (MIC) issued a draft decree to amend both Decree No. 72/2013/ND-CP (Decree 72) on the management, provision and use of Internet services and online information and Decree No.27/2018/ND-CP (Decree 27) which amended and supplemented several articles in Decree No.72. The Decree has undergone several iterations. The latest consultation occurred in September 2023.[99] The proposed amendments aim to allow the government to tighten control over livestreaming activities that generate revenue on social networks and impose obligations on cross-border social network service providers in Vietnam.

Not only does Decree 72 reinforce the data localization requirements found in other Vietnamese laws, BSA is also particularly concerned that the scope of covered entities could potentially include enterprise service providers even though many of the intended regulations are targeted at consumer-facing entities. There is also a new chapter under Decree 72 requiring providers of data center services to register with the MIC and contains additional obligations for data service providers to develop and implement technical plans and solutions to promptly detect and prevent illegal activities. These requirements place unnecessary and impractical burdens on data center service providers who may have to re-engineer their networks to afford them access to their enterprise customers' sensitive data which would be contrary to their contractual and other legal obligations.

Personal Data Protection Law: September 24, 2024, Vietnam published the draft Personal Data Protection Law. The PDPL contains a large number of new restrictions on the ability to transfer data across borders. The draft law is scheduled for enactment in May 2025, with an effective date of January 1, 2026. The draft law imposes obligations to conduct transfer impact assessments, to make impact assessments available to government authorities, and to face severe penalties (including cancellation of the authority to transfer data) for any violations. The definitional scope of "data transfer" is very broad.

- Article 2(24) defines "overseas transfer" to include not only the act of transferring data, but also the act of accessing data from outside of Vietnam: (i.e., the "use of cyberspace, equipment, electronic means or other forms of transfer of personal data of Vietnamese citizens to a location outside the

[99] https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-superseding-decree-no-722013nd-cp

territory of the Socialist Republic of Vietnam or the use of a location outside the territory of the Socialist Republic of Vietnam for the processing of personal data.")

- Article 45 further defines transfers to include: (a) Sharing personal data with recipients outside [Vietnam]; (b) Sharing personal data at an overseas [or meeting]; (d) Publishing personal data in cyberspace that is received by persons outside [Vietnam]; (dd) Providing personal data to other organizations, enterprises and individuals for the purpose of carrying out business activities; and (e) Providing personal data on the fulfillment of legal obligations abroad or according to the laws of the host country.

The foregoing provisions imply the sharing of personal information within Vietnam will be treated as a transfer if it is accessed by those outside of Vietnam, even if that was not the intention and even if that outcome was not foreseeable. Additionally, subparagraphs (c) and (dd) raise questions as to whether provision to a Vietnam-based subsidiary of a foreign enterprise or to a non-national in Vietnam would be deemed to constitute a "transfer."

Copyright and Enforcement

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code,[100] the Criminal Code,[101] and the Administrative Violations Decree.[102] The Civil Code operates in parallel.[103]

The Criminal Code criminalizes "commercial scale" acts of "[c]opying of works, audio recordings and visual recordings" or "[d]istributing the copies of work, audio or video recording." However, there has been a general lack of criminal enforcement against copyright infringement over the years by the relevant authorities.

On January 1, 2018, amendments to Vietnam's Criminal Code (adopted in 2015) went into effect.[104] The revised Criminal Code includes some improvements in provisions addressing copyright infringements. For example, there are several provisions applying criminal penalties for copyright infringements to commercial entities. Article 225 of the revised Criminal Code specifies that a commercial entity that commits copyright infringement is now subject to criminal penalties and may be fined up to VND3 billion (~US$150,000), and its business operations may be suspended for up to two years. However, the Government of Vietnam has yet to issue implementing guidelines in relation to how exactly Article 225 will be enforced. Such guidelines are required to clarify how Article 225 will supplement the existing regime.

Amendments to the Intellectual Property Code over the years have resulted in several improvements in the overall protection of copyright in Vietnam. However, more can be done to strengthen the legal framework for IP protection. BSA recommends introducing pre-established damages upon the election of the right holder, which can be very important in civil cases when the harm caused by the infringement is difficult to calculate.

---

[100] *Law on Intellectual Property (No. 50/2005/QH11) (IP Law)* (2006). English translation at: https://wipolex.wipo.int/en/text/274445
[101] *Criminal Code (No. 100/2015/QH13)* (2016) at: https://wipolex.wipo.int/en/text/446025. English translation at: https://wipolex.wipo.int/en/text/446020
[102] *Decree No. 131/2013/ND-CP on Sanctioning Administrative Violations of Copyright and Related Rights*, entry into force December 15, 2013 (replacing Ordinances No. 47 and 109) at: https://thuvienphapluat.vn/van-ban/So-huu-tri-tue/Decree-No-131-2013-ND-CP-on-sanctioning-administrative-violations-of-copyright-and-related-rights-212865.aspx.
[103] *Civil Code (No. 91/2015/QH13)* (2017) at: https://wipolex.wipo.int/en/text/445451. English translation at: https://wipolex.wipo.int/en/text/445414
[104] *Law No. 12/2017/Q14 (Amended Criminal Code)*, see *Vietnam: 2015 Penal Code to Take Effect on 1 January 2018* at: https://globalcompliancenews.com/vietnam-new-penal-code-20171110/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

Compliance and Enforcement: The lack of criminal enforcement against copyright infringement remains a concern. The general inactivity of the courts in dealing with copyright infringement issues also remains a problem in Vietnam. The Government of Vietnam should issue implementation guidelines on the enforcement of Article 225, which should clarify that the enforcement authorities and the courts are authorized and encouraged to prosecute criminal cases against commercial scale infringement, including against enterprises unlawfully using unlicensed software.

Also, there have been relatively few civil court actions involving copyright infringement in Vietnam. Complicated procedures, delays, and a lack of predictability in the outcome contribute to this problem. BSA remains hopeful that, over time, civil remedies will be available to supplement administrative, and eventually criminal, enforcement. However, the current difficulties in successfully bringing civil software copyright infringement cases coupled with a lack of clarity on how damages will be calculated for unlicensed software use has resulted in an increasing number of infringers being unwilling to settle cases with copyright holders despite clear evidence of rampant unlicensed software use. As a result, it remains challenging for copyright holders to obtain effective redress against infringers in Vietnam.