30 September 2022

BSA COMMENTS ON DECREE 53 TO IMPLEMENT THE LAW ON CYBERSECURITY

Respectfully to: The Ministry of Public Security
Copy to: The Ministry of Information and Communications

On behalf of BSA | The Software Alliance (**BSA**),[1] we send you our sincere regards and thank you for providing guidance on several provisions within the Law on Cybersecurity (**LOCS**). In the past few years, BSA has followed with great interest developments related to the LOCS. For instance, BSA provided comments on proposed amendments to the draft Decree 72 in September 2021[2] and December 2021[3] and commented on the draft Decree Implementing Law on Cybersecurity in December 2018[4]. BSA also contributed joint industry association comments on draft Cybersecurity Law v15 and v18 in February 2018[5] and June 2018.[6]

I. Recommendations

On 15 August 2022, the Ministry of Public Security (**MPS**) published the final Decree No. 53/2022/ND-CP (**Decree 53**). Respectfully, we are concerned about the following issues in the final Decree 53 and provide suggestions for MPS's consideration:

a) Possible inconsistencies in the definition of "domestic enterprise" and the scope of applicable service providers for which Decree 53 would apply.

Article 26.2 of Decree 53 requires domestic enterprises to store data in Vietnam, and Article 2.11 of Decree 53 defines a "domestic enterprise" as an enterprise established or registered for establishment under Vietnamese law and having its head office located in Vietnam. While we are appreciative that a good number of BSA's member companies would be excluded

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

BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Vietnam: BSA Comments on Proposed Amendments to Draft Decree 72 | BSA | The Software Alliance

[3] Vietnam: BSA Comments on Proposed Amendments to Draft Decree 72 | BSA | The Software Alliance

[4] Vietnam: BSA Comments on Draft Decree Implementing Law on Cybersecurity | BSA | The Software Alliance

[5] Vietnam: Cybersecurity Law 15th Version-Joint Industry Association Comments | BSA | The Software Alliance

[6] Vietnam: Joint Industry Association Comments on draft Cybersecurity Law (v18) | BSA | The Software Alliance

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

from the definition and will not be required to store required data within Vietnam, we are concerned that certain enterprises such as foreign-direct-investment (FDI) companies with head offices in Vietnam would be considered domestic enterprises. **We recommend issuing a formal interpretation specifying that Article 26.2 does not include foreign-invested enterprises or subsidiaries of foreign or multinational corporations within the scope of "domestic enterprises".**

Article 2.2 defines "service users" as "organizations [and/or] individuals in the use of services in cyberspace" and Article 2.3 defines "service users in Vietnam" as "organizations [and/or] individuals using cyberspace with the territory of the Socialist Republic of Vietnam." **We recommend that MPS clarify that the term "service user", defined in Articles 2.2 and 2.3, does *not* require domestic or foreign enterprises to consider their employees or other internal staff as "service users".** This would allow Vietnamese domestic enterprises to continue using internationally available cloud services for their internal business operations.

b) Article 26.2 of Decree 53 requires domestic enterprises to store data in Vietnam. We wish to confirm that such data can be transferred, stored, and processed outside of Vietnam so long as the data itself is also stored in Vietnam.

Data localization requirements, such as those imposed in Decree 53 will have a chilling effect on the local economy if they do not allow enterprises to fully benefit from cutting edge technology and services available in the global marketplace. For instance, data localization requirements may restrict domestic enterprises, both small and medium-sized enterprises (**SMEs**) and larger organizations such as hospitals and banks, from using world leading information technology (**IT**) and cloud computing solutions from service providers that offer their services from outside of Vietnam.[7] Such services frequently provide best in class security capabilities; prohibiting domestic companies from using such services may reduce their competitiveness, especially internationally, and expose them to great data security risks.

BSA's recommendation is to eliminate the data localization requirements from Decree 53 altogether. However, until the Government rescinds the data localization requirements, **we recommend that MPS makes clear the requirement to store data in Vietnam is achieved when a domestic enterprise stores an electronic copy of the required data in Vietnam in a form determined by that enterprise.[8]** This would allow a domestic enterprise to continue to use cloud-based services that do not or cannot store data in Vietnam as part of their services.

BSA supports efforts to ensure data is protected commensurate with the risk its compromise poses but requiring data localization does not increase the protection of data and indeed can increase the risk that such data may be compromised.

---

[7] Cloud services delivered across-borders provide security advantages over alternative IT delivery approaches (on-premises or local cloud services):

- Physical Security: Certified personnel can carefully monitor servers 24/7 to prevent physical breaches and can apply consistent protocols over a small number of locations.
- Data Security: Cloud Service Providers (CSPs) can ensure data integrity through use of state-of-the-art encryption protocols for data at-rest and in-transit. CSPs can establish redundant backups of data in geographically dispersed data centers, mitigating risk of loss in the event of power outages or natural or manmade disasters.
- Advanced Threat Detection: CSPs leverage state-of-the-art enhanced security intelligence They use regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- Automated Patch Deployment: Automated and centralized patch deployment and real time updates to network security protocols work to protect systems from newly identified vulnerabilities.
- Incident Management and Response: CSPs maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- Certification: CSPs are typically certified to international security standards and go through regular audits to maintain their certifications.

[8] Decree 53 Article 26.5 states "The form of data storage in Vietnam shall be decided by the enterprise."

c) **The effective date of implementation of Decree 53 is too short and covered enterprises will not be able to migrate data and workloads effectively prior to October 1, 2022.**

The short timeframe for compliance does not afford domestic enterprises enough time to make necessary changes and would be highly disruptive to ongoing operations. Requiring domestic enterprises to rush into compliance could result in the lowering of cybersecurity postures as enterprises may create poorly constructed or secured data bases in order to meet the current effective date. If data migration is required, domestic enterprises would need time for the migration of data and workloads to store data in Vietnam.

We recommend that covered enterprises be given 24 months to comply with Decree 53 even if the effective date of implementation is 1 October 2022. Providing the Vietnamese business community with a transition period of 24 months will enable businesses to have adequate time to familiarize themselves with these new obligations and implement measures to comply with them while ensuring that their cybersecurity posture remains high. This would also avoid a situation in which the law would be in force, but enterprises are unable, though not unwilling, to comply.

II. Concerns Regarding Vietnam's Commitments in International Agreements

The above recommendations are designed to make clear uncertainties in the current Decree or to suggest proposals that would mitigate the negative impact of the data localization requirements. However, we also wish to note that some of the data localization requirements may raise concerns regarding Vietnam's commitments in international agreements and present challenges to Vietnam's efforts to harness digital transformation for the benefit of its economy and citizens.

a) **Inconsistency with CPTPP Commitments:** The data localization requirements in Articles 26.1 and 26.2 of the Decree raise concerns regarding Vietnam's compliance with its international obligations under the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP). While these two Articles appear to require only domestic enterprises to store data within Vietnam, in effect they would also require any foreign enterprises offering data storage or processing services to Vietnamese entities to "use or locate computing facilities" in Vietnam as a condition for conducting business. These localization requirements appear to be incompatible with CPTPP Article 14.13, which states (in relevant part) as follows:

> "Article 14.13: Location of Computing Facilities: … 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

Vietnam's limited transition period to comply with this obligation will expire in January 2024, meaning that such localization requirements will be formally out of compliance with Vietnam's CPTPP commitments at that time.

b) **Ineligibility for CPTPP Exceptions:** The data localization requirements may not qualify as reasonable or permissible exceptions within the meaning of CPTPP Article 14.13.3.[9] Derogations from the aforementioned CPTPP provisions must be "necessary" to secure compliance with domestic laws (such as those relating to cybersecurity) and "not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective." Unfortunately, Decree 53 does not appear to meet this standard. Indeed, far from advancing cybersecurity objectives, the data localization mandates in Decree 53 could undermine the Decree's stated objectives of improving data security and protection in Vietnam. Cross-border data transfers help improve data security, allowing for real-time visibility and response to emergent cyberthreats, including malware, online fraud, and other criminal activity online. It also provides greater resiliency by enabling backups and redundancy outside of the country. Imposing data localization requirements may impede cross-border data transfers and reduce the ability of Vietnamese enterprises to respond to threats to their data — creating unintended data security vulnerabilities for Vietnam.

c) **Exclusion from IPEF and Other Regional Trade Initiatives:** The data localization requirements in the Decree would also threaten Vietnam's ability to participate in and benefit from regional trade initiatives, such as the Indo-Pacific Economic Framework (IPEF). If Vietnam fails to abide by existing international commitments, it may raise questions about the strength and value of commitments that Vietnam seeks to undertake in other negotiations. A loss of trust in Vietnam's ability to abide by its international commitments could undermine the willingness of partner economies to engage in digital trade negotiations with Vietnam in the future.

   Provisions on protecting cross-border data transfers, prohibiting data localization and digital customs duties, and promoting cybersecurity and personal data protection are core pillars of the IPEF trade pillar. Those provisions will be based on standards found in the US-Japan Digital Trade Agreement (USJDTA), the Australia-Singapore Digital Economy Agreement (DEA), the Singapore-Korea Digital Partnership Agreement (DPA), the Digital Economic Partnership Agreement (DEPA), the US-Mexico-Canada Agreement, and the CPTPP, among others. Unfortunately, the restrictions outlined in Decree 53 would be incompatible with the aforementioned provisions in each of the named agreements. By amending the Decree to remove its data localization requirements, Vietnam would also avoid disqualifying itself from participating in the IPEF trade pillar negotiations on cross-border data matters.

d) **Threat to Vietnam's Innovation and Technology Ecosystem:** The Decree's data localization requirements could threaten Vietnam' ecosystem for software and technology start-ups, and its ability to attract investment and to compete with peer nations. By imposing restrictions that make it more difficult for foreign enterprises to engage with Vietnam in cross-border software development and technology transfer, Vietnam risks hobbling its own indigenous enterprises and making itself less attractive (in both absolute and relative terms) to foreign investment in software development and other emerging technologies. Again, amending the Decree to remove its data localization requirements would help Vietnam avoid this negative outcome.

---

[9] CPTPP Article 14.13.3. states as follows:

"Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

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

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."

BSA represents the global enterprise software industry. Our members are at the forefront of data-driven innovation, developing cutting-edge advancements in artificial intelligence, machine learning, and cloud-based analytics. Our members earn users' confidence by providing essential security technologies that protect against cyberthreats. By working closely with governments around the world on cybersecurity policy and legislative development, BSA has witnessed the potential for cybersecurity laws and regulations to both deter and manage cyberthreats while also protecting privacy and civil liberties of citizens.

We would like to thank the MPS for considering our comments on Decree 53 and hope MPS will positively implement our recommendations. We urge MPS to continue to engage in dialogue with the private sector and to continue open discussions to achieve common goals for developing a vibrant and competitive digital economy.

Please do not hesitate to contact us if you require any clarification or further information. Thank you once more for your time and consideration.

Sincerely,

Wong Wai San

Wong Wai San
Senior Manager, Policy – APAC