18 November 2021

BSA COMMENTS ON DRAFT DECREE ON SANCTIONS AGAINST ADMINISTRATIVE VIOLATIONS IN THE FIELD OF CYBERSECURITY

Submitted Electronically to the Ministry of Public Security

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide our comments to the Ministry of Public Security (**MPS**) on the draft Decree on Sanctions against Administrative Violations in the field of Cybersecurity (**Draft Decree**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. We have extensive experience engaging with governments around the world to promote effective, internationally interoperable legal systems that raise cybersecurity standards, protect personal information while supporting responsible uses of data-driven technologies.

BSA's members are at the forefront of data-driven innovation, developing cutting-edge advancements in artificial intelligence, machine learning, and cloud-based analytics. Our members recognize the need to earn users' trust and confidence by acting responsibly with their personal data and provide the essential security technologies that protect against cyberthreats.

BSA and our members have a significant interest in Viet Nam's Law on Cyber Security (**LOCS**) and its corresponding draft decrees and have provided comments on the LOCS and draft decrees through the various public consultations conducted by MPS.[2] We appreciate the Government of Viet Nam's continuous efforts to develop a legal framework for cyber and information security. We also acknowledge and recognize the important task that MPS has undertaken to ensure that Viet Nam is well-positioned to deter and manage different types of violations and threats in the cyberspace.

It is our understanding that this Draft Decree will sit under the LOCS and seeks to consolidate the various administrative sanctions for violations under the Draft Decree on Cybersecurity (**Cybersecurity Decree**) and Draft Decree on Personal Data Protection (**PDP Decree**). We are concerned however that an excessively broad implementation of the LOCS and its corresponding

---

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

BSA's members include: Adobe, Altium, Atlassian, Autodesk, AVEVA, Amazon Web Services, Bentley Systems, Box, Cisco, Dassault Systems, DocuSign, IBM, Informatica, Intel, Mastercam, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell Automation, Salesforce, ServiceNow, Shopify, Siemens PLM Software, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Unity, Workday, Zendesk, and Zoom.

[2] https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-vietnam-personal-data-protection-decree

https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-implementing-law-on-cybersecurity

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

draft decrees, namely the Cybersecurity Decree and the PDP Decree, would be an ineffective method for achieving this goal and may have a chilling effect on innovation and investments. We offer the following comments in the hope that they will be helpful as MPS continues its efforts to finalize the Cybersecurity Decree and PDP Decree and consider their impact on the Draft Decree on Sanctions Against Administrative Violations in the field of Cybersecurity.

General Observations

At the outset, we would like to highlight that both the Cybersecurity and PDP Decrees are yet to be finalized even though the Draft Decree is meant to consolidate the various administrative sanctions for violations under the two aforementioned decrees. While we appreciate the level of transparency and stakeholder engagement demonstrated by MPS through this public consultation process, it is difficult for the industry to provide substantive input to the Draft Decree without a clear understanding of the obligations in the other two Decrees. In this regard, we urge the MPS to continue working with the industry on the draft Cybersecurity and PDP Decrees and to make the text of these two draft Decrees available to us for further comment and consultation.

BSA notes the extremely broad scope in enforcement targets, which include "*foreign enterprises or their branches, representative offices, business locations that provide services on telecommunication networks of the Internet, content provision services in cyberspace, information technology, cybersecurity and cyber information security*", covering both onshore and offshore service suppliers. Enforcement can only be effective and efficient if the obligations placed on the different entities are clear and tailored to each entity's roles and responsibilities which we describe in greater detail in the next section.

The Draft Decree specifies the monetary values of the various penalties which range from VND 10 to 100 million (approximately US$440 to $4,400). It also states that, depending on the severity, consequences, and nature of the violation, the penalties levied can be up to 5% of the violating organization's annual revenue in Viet Nam. Civil penalties should be proportionate to the harm caused to individual; and due consideration should be given to both aggravating and mitigating factors when deciding on the penalties. The Draft Decree currently only considers aggravating factors (such as the number of individuals affected and whether it is a repeated violation) when deciding whether penalties should be increased. However, mitigating measures taken by organizations to remedy the situation should also be given due consideration. Such mitigating factors include: (a) how actively and promptly the organization has tried to resolve the matter with the affected individual(s); (b) whether the organization took reasonable steps to prevent or reduce the harm caused by the breach or violation; and (c) whether the organization has provided affected individual(s) with remedies. **BSA therefore recommends MPS to review the penalty structure to also take into consideration the various aforementioned mitigating factors when deciding the level and value of penalties**.

Specific Comments and Recommendations

In this section, we provide comments and recommendations on the provisions under Section 2, "Violations of Regulations on Personal Data Protection" (Articles 14 – 30), Section 3 "Violations of Regulations on the Prevention of and Combatting Against Cyber-attack" (Articles 31-33), and Section 4, "Violations of Regulations on the Implementation of Cybersecurity Protection Activities" (Articles 34-39)

Penalties on "Personal Data Processors and Third Parties"

Section 2 of the Draft Decree includes references to "*Personal Data Controllers*", "*Parties that Control and Process Personal Data*", "*Personal Data Processors*", and "*Third Parties*". This seems to suggest that the PDP Decree may now recognize the concepts of data controllers, data controllers who also act as a data processor, data processors, and third parties. While we still do not know how these concepts will be defined in the PDP Decree, BSA continues to encourage MPS **to align the definitions for "data controllers" and "data processors" with those in other laws and their obligations should accordingly fit their roles**. We also recommend that **the roles and**

responsibilities of "Personal Data Processors" vis-à-vis "Third Parties" should be clearly established in the PDP Decree.

BSA further notes that many of the penalties under Section 2 are directed at "*Personal Data Controllers*" and "*Parties that Control and Process Personal Data*" for consumer facing obligations. These include provisions such as Articles 15-1(dd), 15-1(e), 15-1(i), 17, and 22-23. This is a welcome development because obligations such as obtaining the data subjects' consent to process their data and the requirement to honor data subjects' rights requests should rightfully be placed on data controllers who have a direct relationship with data subjects. However, we note that **provisions under Article 15-1(g), 15-1(h), 19-1(b) would still penalize "Personal Data Processors" and "Third Parties" for obligations that should belong to data controllers. Therefore, we continue to encourage MPS to exclude "Personal Data Processors" and "Third Parties" from such obligations**.

Penalties Related to Cross-border Transfer of Personal Data

Article 26-1(a) states that a fine will be imposed if personal data of Vietnamese nationals were transferred without meeting all three conditions under paragraph 2 of Article 16 of the Decree on Personal Data Protection. Although the PDP Decree is not finalized and we do not know what the three conditions will be, we do note that Article 26-1(b) and (c) include references to "impact assessment" and legally binding agreements. In addition, there are also requirements in the Draft Decree for transferring organizations to notify the Personal Data Protection Authority of the transfer, and to retain dossiers of the impact assessment and/or legally binding agreements for audit purposes.

Taken collectively, we are deeply concerned with the restrictive requirements on cross border transfers of personal data. To require organizations to fulfill multiple conditions such as those described above before they are allowed to transfer personal data will undermine the ability of global companies to do business in Viet Nam and harm the ability of companies in Viet Nam to provide global services. The additional notification and retention obligations increases compliance costs on businesses while providing no practical value to data subjects and may inadvertently create new privacy and security concerns by forcing them to store and access data they otherwise would not. **We urge MPS to revise the provisions in the draft PDP pertaining to cross-border transfer of personal data to allow for further flexibility.**

Penalties Related to Prevention and Handling of Dangerous Cybersecurity Situations

Article 33-1 requires organizations to cooperate in the implementation of technical and professional solutions to prevent, detect, and/or handle dangerous cybersecurity situations and to prevent or remove content that risks causing riots, disrupting security, and/or triggering terrorism. We note that the July 2018 version of the draft Cybersecurity Decree neither contains any clear definition or explanation of the term "dangerous cybersecurity situation", nor does it outline the mechanism for how takedown requests are to be issued. Therefore, we urge MPS to make clear what would be deemed a "dangerous cybersecurity situation" and develop a clear mechanism with official communication channels and formal content takedown requests in the Cybersecurity Decree.

As we had emphasized earlier, it is important to tailor the obligations and liabilities based on each entity's roles and responsibilities. Given that enterprise service providers are typically not in the position to access their enterprise customers' data due to contractual obligations, BSA further **recommends that enterprise software service providers be excluded from obligations relating to the removal of unlawful content.** Requests to remove unlawful content and to cooperate with law enforcement agencies in relation to unlawful content should be directed to the entity responsible for creating and publishing that content (i.e., the enterprise service customer), not an intermediary that is hosting or transmitting that content on behalf of a business customer such as a cloud service provider. The enterprise customer will be best placed to respond to requests of this nature. In most instances, an enterprise service provider will pass such requests on to the business customer for action. We therefore recommend for the relevant obligations in the Cybersecurity Decree to be applied

appropriately to only the consumer facing businesses that deal directly with individual customers and disseminate information to the public at large.

Penalties Related to Cybersecurity Protection for Information Systems

Articles 34 and 35 outline the penalties which would be imposed on information systems for violations related to cybersecurity protection. Article 34 applies specifically to "information systems of national security importance", while Article 35 applies to all other types of information systems. BSA is encouraged that MPS appears to have taken a differentiated approach where information systems that are not categorized as of "national security importance" would be excluded from requirements such as cybersecurity appraisals, audits, and inspections, among others. This notwithstanding, we continue to urge MPS to:

a) Narrow the definition and scope of an "*information system of national security importance*";

b) Elaborate in greater detail the specific review or appraisal procedures

c) Include more details about cybersecurity inspection procedures (including oversight and rights of appeal for such procedures)

Penalties Related to Data Localization

Article 37-2 specifies that a fine will be imposed if an organization fails to store data or establish a branch or representative office in Viet Nam as prescribed in paragraph 3 of Article 26 of the LOCS. Previous submissions on the Cybersecurity Decree have highlighted the need to clearly define the limits of the data localization and local office requirements.

Broad implementation of data localization and local office policies will negatively affect Viet Nam's economic competitiveness as businesses across all sectors and of all sizes in Viet Nam rely on and benefit from the seamless flow of data into and out of the country. Data localization expenses will inevitably be passed along to consumers in the form of higher prices. Requiring local businesses to use local data centers will add costs that are particularly hard to absorb for small and medium sized businesses. Ultimately, these localization requirements may also undermine cybersecurity by forcing companies to use potentially less secure local servers and to divert funds that could otherwise be focused on enhancing network security.

As Viet Nam continues to implement the LOCS, it should limit localization requirements only to the most sensitive national security data, if deemed necessary. This would enable specialized handling and localization of truly critical data and reduce confusion or uncertainty for international companies interested in investing or expanding investment in Viet Nam.

In addition, the scope for data localization requirements should also be narrowed to exclude organizations that do not disseminate information to the public, including, but not limited to, enterprise software and cloud service providers. We note that Article 26.1.c of draft Cybersecurity Decree (July 2019 version) requires businesses that have "*full knowledge of the fact that the service that the business in question provides is being used to commit acts of violation of Vietnamese laws…*" to store their data in Viet Nam. However, enterprise software service providers typically do not have visibility or knowledge of the content their enterprise customers are uploading to their services, including whether that content constitutes data that would be in violation of Vietnamese laws. Hence, **we recommend that relevant obligations under the draft Cybersecurity Decree regarding data localization should not be applied to businesses that process data on behalf of enterprise customers.**

Conclusion

We would like to thank the MPS again for the opportunity to comment on the Draft Decree. We appreciate MPS's kind consideration of our above comments. For any questions or if any point of clarification is required on any part of this submission, please feel free to contact the undersigned at eunicel@bsa.org. Thank you for your time and consideration.

Yours faithfully,

Eunice Lim

Senior Manager, Policy – APAC

BSA | The Software Alliance