23 December 2022

BSA COMMENTS ON THE DRAFT LAW ON TELECOMMUNICATIONS

Respectfully 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 soliciting feedback from the private sector on the Draft Law on Telecommunications (**Draft Law**). The Draft Law seeks to broaden the scope of the existing law to include new services and notably proposes a new chapter — Chapter X on "Doing Business in Data Center and Cloud Computing Services" — which seeks to regulate data center and cloud computing services.

In the past few years, BSA has followed with great interest developments in digital governance in Vietnam. For instance, BSA provided comments on Decree 53 in September 2022[2] and the Draft Law on Electronic Transactions in June 2022.[3] BSA also proposed amendments to the draft Decree 72 in September 2021[4] and December 2021[5] and provided comments on the Law on Cybersecurity in December 2018.[6]

Respectfully, we are concerned about several issues in the Draft Law and provide suggestions for MIC's consideration.

Chapter X on "Doing Business in Data Center and Cloud Computing Services"

The Draft Law introduces Chapter X on "Doing Business in Data Center and Cloud Computing Services". This Chapter requires enterprises offering data center and cloud computing services to register with MIC and perform licensing procedures. This is not in line

[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 Decree 53 to Implement the Law on Cybersecurity

[3] Vietnam: BSA Comments on Draft Law on Electronic Transactions

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

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

[6] Vietnam: BSA Comments on Draft Decree Implementing Law on Cybersecurity | 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

with most regulatory frameworks and detracts from the purpose of the Draft Law, which is to specify regulatory obligations for telecommunications services.

Governments of other countries are typically unwilling to extend the scope of what constitutes a telecommunications service to cover data center and cloud computing services. Rather, most jurisdictions clearly differentiate between entities that set up the telecommunications networks; entities that provide communications intermediation, connectivity, or Internet/mobile access through telecommunications networks; and entities that provide content and facilities over telecommunications networks and services. The latter are not subject to telecommunication requirements or licenses and are not generally considered to be providers of equivalent services.

For example, the Australian federal telecommunications law regulates 'carriers' — entities that set up telecommunications networks — and carriage service providers — entities that provide Internet and connectivity services based on the infrastructure of the carrier.[7] Carriers require a license from the government,[8] while carriage service providers must only follow the applicable law.[9] Content service providers, which use carriage services to provide content to the public, do not require a license and are subject to lighter rules than both carriers and carriage service providers.[10] Moreover, the Australian Competition and Consumer Commission also recommends against the equal regulatory treatment of traditional telecommunications services and over-the-top (**OTT**) communication services as they do not consider OTT communications services to be full substitutes for voice service due to differences in functionality.[11] Similarly, in the United Kingdom, while both electronic communication networks and electronic communication services are subject to a general authorization regime[12] — content services are excluded from this requirement.[13]

To maintain the focus on the Telecommunication Law on telecommunication services and to keep Vietnam's legal regime in line with international approaches, the Draft Law should not extend to data center and cloud computing services. Therefore, BSA **recommends deleting Chapter X on "Doing Business in Data Center and Cloud Computing Services" entirely and refrain from imposing licensing or registration requirements on data center and**

[7] Section 41, Telecommunications Act (Australia)

[8] Section 41, Telecommunications Act (Australia)

[9] About carriers and carriage service providers, Australian communications and media authority, https://www.acma.gov.au/about-carriers-and-carriage-service-providers#:~:text=CSPs%20do%20not%20need%20a,and%20Service%20Standards)%20Act%201999

[10] Section 97, Division 4, Telecommunications Act (Australia). Except in the case of content service providers which provide gambling promotional content which require a license to operate. *See* Rule 4, Broadcasting services (Online content service providers Rules), April 2018.

[11] Australian Competition and Consumer Commission's Communications Sector Market Study, April 2018, https://apo.org.au/node/139446 (see page 41)

[12] General conditions of entitlement, Ofcom, https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-competition-regulation/general-conditions-of-entitlement

[13] Department for Digital, Culture, Media and Sport, Audience Protection Standards on VoD services, 28 April 2022 https://www.gov.uk/government/consultations/audience-protection-standards-on-video-on-demand-services/audience-protection-standards-on-video-on-demand-services#ensuring-vod-services-are-regulated

cloud computing service providers. In addition, ***BSA recommends removing references to data center and cloud computing services in Articles 1 and 2***.

1. Possible Data Localization Requirements

Article 75(1) requires enterprises engaged in data center services and cloud computing service businesses to be responsible for "storing data in Vietnam in accordance with the relevant laws." As noted in a previous submission to MPS on Decree 53,[14] data localization requirements will have a chilling effect on the local economy as they do not allow domestic enterprises and other organizations to fully benefit from cutting edge technology and services available in the global marketplace, inhibiting their ability to embrace the digital economy. 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 and cloud computing solutions from service providers that offer their services from outside of Vietnam.[15] Such services frequently provide best in class security capabilities with economies of scale; prohibiting domestic companies from using such services may reduce their competitiveness, especially internationally, and expose them to greater data security risks. While BSA supports efforts to ensure data is protected commensurate with the risk its compromise poses, requiring data localization does not increase the protection of data and indeed can increase the risk that such data may be compromised.

In addition, the requirement to store data in Vietnam "in accordance with relevant laws" found in ***Article 75(1)*** creates legal uncertainty for enterprises because several relevant laws and draft regulations require local storage to different, and possibly contradictory, extents. For example, the Law on Cyber Security, the draft Personal Data Protection Bill, Decree 72, and Decree 53 each contain varying data localization requirements. It is not clear how ***Article 75(1)*** should be interpreted by enterprises facing multiple diverging data localization obligations.

Data localization requirements also raise concerns regarding Vietnam's commitments in international agreements and present challenges to Vietnam's efforts to harness digital

---

[14] Vietnam: BSA Comments on Decree 53 to Implement the Law on Cybersecurity

[15] Cloud services, including those delivered across-borders, provide security advantages over alternative IT delivery approaches such as on-premises solutions):

- 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.

transformation for the benefit of its economy and citizens. For example, data localization requirements are incompatible with Vietnam's commitments under the Comprehensive and Progressive Trans-Pacific Partnership Agreement (**CPTPP**). Further, removing data localization requirements would enhance Vietnam's ability to participate in and benefit from regional trade initiatives, such as the Indo-Pacific Economic Framework (**IPEF**).

Therefore, **BSA recommends removing data localization requirements within the Draft Law and specifically recommends, if other portions of Chapter X are retained, to delete *Article 75(1)*.**

2. Compliance with Standards

In the event that MIC retains elements of Chapter X, we note that ***Article 74(1)(a)*** requires enterprises engaged in data center service and cloud computing service to "comply with the standards, [and] technical regulations during the design, construction and operation, [and] exploitation of data center, as well as comply with standards, [and] technical regulations on network information safety, protection of service user data, and concurrently, be consistent with the planning of information and communication infrastructure."

To ensure that Vietnam continues to have access to leading edge technology and innovations from around the world, **Vietnam should refrain from developing unique standards and instead rely on internationally recognized standards**.

3. Overlap with Existing or Draft Regulations

If MIC chooses to retain elements of Chapter X, we note that there are requirements within Chapter X that overlap with existing or draft laws or rules. ***Articles 73 and 74*** set forth registration requirements and compliance with technical standards already covered under draft amendments to *Decree No. 72/2013/NC-CP*.

In the Draft Law, the requirements to secure user information in ***Article 75(2)-(4)*** are already covered under the *Law on Cybersecurity*, *Decree No. 53/2022/ND-CP*, and the *draft Decree on Sanctions Against Administrative Violations in the Field of Cybersecurity*. Further, the requirement to delete, return, or transfer data at the end of a service agreement should lie with service users to ensure that they instruct the removal of their content, and the obligation of service providers should be to comply with the instructions of the service user.

Article 74(1)(d) specifies that enterprises are to "refrain from performing the acts of competition suppression, unfair competition, acts of oppressing, [or] hindering other enterprises from doing business," which is more appropriately addressed under the *Law on Competition*.

Article 76(2) on violating copyright, intellectual property rights, and provisions of law are already covered under the *Decree on Sanctions Against Administrative Violations in the Field of Cybersecurity*.

Further, both ***Articles 76(1) and 76(2)*** do not appropriately recognize the difference between cloud computing service providers, which have very limited visibility into enterprise customer data and content, and the enterprise customers themselves that are more

appropriately subject to rules related to the detection, reporting, and removal of content. Specifically, ***Article 76(1)*** requires enterprises engaged in data center services and cloud computing service businesses "must immediately notify the Ministry of Information and Communications upon detecting such activities abusing data center services, [or] cloud computing services to commit illegal acts." An affirmative obligation for cloud computing service providers to monitor or detect their enterprise customers' data and content would be impossible for many such providers for technical, contractual, and legal reasons.

Therefore, if MIC chooses to retain elements of Chapter X, **BSA recommends deleting *Articles 73, 74, 75(2)-(4), and Article 76* from the Draft Law to avoid overlap with other regulations.**

4. Scope of Chapter X

Most of the concepts of Chapter X relate to infrastructure services (see Article 71), except for Articles 72(2)(b) and (c), which specifically identify Platform-as-a-Service and Software-as-a-Service (**SaaS**).

Therefore, if MIC chooses to retain elements of Chapter X, **BSA recommends deleting Articles 72(2)(b) and (c) to more closely align the entities identified in Chapter X to the obligations it establishes**.

Communication Service Not Utilizing Telecommunication Number Storage

We agree with the exclusion in ***Article 3(8)*** of "services where the features of making voice calls [and/or] and texting are only secondary [and/or] dependent characteristics of another service." This is an important distinction and will advance innovation and is consistent with laws in many other markets.

However, it is unclear in ***Article 3(8)*** if "Communication service not utilizing telecommunication number storage" refers to standalone voice call and/or texting services, or also includes SaaS that provide voice call/texting functions as part of a broader suite of services. Based on the ***Article 36***, it appears that the policy intent is the former, i.e., to regulate OTT services that are specifically designed to provide text and audio communication services. To more explicitly limit this to standalone OTT services only, and to avoid including services where such functionality is ancillary to the service provided, **BSA proposes amending Article 3(8) to include the insertion underlined below**:

> Communication service not utilizing telecommunications number storage means **standalone** voice call [and/or] texting service on the Internet that does not connect to telecommunications subscribers assigned with the telecommunications number storage.

Territorial Scope of Draft Law

Article 2 applies the Draft Law to "foreign organizations […] directly engaged in or related to telecommunications activities and business operation in data center and cloud computing services in Vietnam." In line with global practices and to maintain a conducive regulatory environment to attract international investment and digital service providers **BSA**

recommends that the territorial scope of the Draft Law be restricted to entities formed or recognized under the laws of Vietnam. Furthermore, as explained elsewhere, **we recommend removing from the scope of *Article 2* "business operation in data center and cloud computing services"**. We suggest revising ***Article 2*** as follows:

> This Law applies to domestic~~, [and] foreign~~ organizations, [and] individuals directly engaged in or related to telecommunications activities ~~and business operation in data center and cloud computing services~~ in Vietnam.

Assurance of Safety

Article 5(1) requires all organizations and individuals to be responsible for promptly reporting acts of sabotaging and infringing upon telecommunications infrastructure but does not specify the expectation on reporting and what constitutes a reportable matter. If MIC intends to further quantify such expectations in a specific regulation, **BSA recommends putting in place a risk-based reporting requirement depending on the incident severity**.

Article 5(4) requires that "organizations and individuals engaged in telecommunications activities shall submit to the management, inspection, [and] examination by competent state agencies and respond to requests of these agencies regarding the assurance of safety of the telecommunications infrastructure." By covering all telecommunications activities, the scope of ***Article 5(4)*** is overly broad and would impose unreasonable regulatory obligations on companies, even small- and medium-sized enterprises, that have no connection to operating facilities or that provide services that are not the focus of this law**. BSA recommends amending *Article 5(4)* to focus only on "Telecommunications Enterprises" providing "Telecommunications Services".**

Assurance of Information Confidentiality

Article 6(1) requires organizations and individuals engaged in telecommunications activities to "be responsible for protecting State secrets in accordance with the provisions of the law on protection of State secrets." The scope of the responsible party is overly broad. It should be the responsibility of the enterprise holding direct control over the content to ensure appropriate tools and services offered by telecommunications enterprises and other parties are used to protect State secrets. Telecommunications enterprises and other parties may have no ability to know or detect whether information transmitted or stored using their service constitutes a State secret. **BSA recommends amending *Article 6(1)* to make clear that the information owners are responsible for protecting State secrets**.

Article 6(4) prohibits the disclosure of certain private information of telecommunications service users, except in enumerated circumstances. Some of the information listed must be disclosed to other providers in order to provide the service. Accordingly, **BSA recommends adding another exception "for the purpose of providing the service" or by clarifying that users have implicitly agreed to such disclosure when they sign up for and utilize the service.**

Rights and Obligations of Telecommunications Enterprises

Article 14(1.2)(a) requires service providing enterprises without infrastructure to make financial contributions to the Vietnam Public-Utility Telecommunications Service Fund. This could result in deterring smaller companies from offering service in Vietnam, could become complicated and difficult to administer (particularly with respect to services that are offered free of charge), and could increase the cost of the expanded scope of telecommunications services offered to individuals and enterprises in Vietnam. **BSA recommends deleting *Article 14(1.2)(a)* or amending it to make financial contributions required only by those entities eligible to receive subsidies for providing telecommunications services.**

Investment in telecommunications service business

BSA recommends amending *Article 18* to make it clear that companies not organized under the laws of Vietnam are eligible for registration to provide telecommunications services in Vietnam.

Conclusion

We would like to thank the MIC for considering our comments on the Draft Law and hope that the MIC will positively implement our recommendations. We urge MIC 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