



30 December 2021

BSA COMMENTS ON PROPOSED AMENDMENTS TO DRAFT DECREE 72

Respectfully to: The Ministry of Information and Communication and the Ministry of Justice

On behalf of BSA | The Software Alliance (**BSA**)¹, we would like to send you our sincere regards and express our appreciation to provide further comments on the proposed amendments to Decree No. 72 on the Management, Provision and Use of Internet Services and Online Information (**Decree 72**).

BSA [commented](#) on the July version of the draft Decree 72 in September, and understands that draft Decree 72 has since been revised in light of feedback from industry and stakeholders.

We are grateful that some of our recommendations have been taken on board in the revised draft, notably our suggestion to remove data localization requirements in Article 22.3(d). The scope of localized data is also now limited to Vietnamese organisations and individuals under the new Article 44k.4. However, we remain concerned about the following proposals:

- a) **Enterprise-focused cloud service providers and data center service providers are still inappropriately caught within the scope of Articles 22**, which will require them to block or remove content that they may not have access to. In addition, data center service providers are required to suspend or stop providing services to their service users committing illegal activities upon written request from a competent State management authority under Article 44k.3. As explained in our earlier submission, these enterprise service providers are bound by contractual obligations and typically have limited access to their enterprise customers' data. Furthermore, many of these service providers only provide and maintain the underlying infrastructure – it is in fact the customer's responsibility for using the infrastructure, including the deployment of applications on that infrastructure. As such, to subject them to the obligations under Articles 22 and 44.k.3 would not only be technically and practically unfeasible, but could also place these entities in breach of their contractual and other legal obligations. **BSA therefore urges Viet Nam to consider the following suggestions:**

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 spark the economy. 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, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

- i. **The obligations under Article 22 should only be applied to consumer-facing businesses that deal directly with individual customers and are making information available for access by the public at large.**
 - ii. **Article 44k.3 should be amended to state that a data center service provider should only be required to suspend or stop providing its services to the applicable customer following a court judgment or legal determination confirming that the applicable customer violated the laws or regulations.**
- b) **Data localization requirements under Articles 44.** Requirements in Article 44k.4 that “[d]ata of data center service users (being Vietnamese organizations and individuals) must be stored in Viet Nam” raise concerns regarding compliance with Viet Nam's obligations under Articles 14.11² and 14.13³ of the Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP). As Viet Nam's grace period to bring itself into compliance with CPTPP Article 14.11 and 14.13 will be ending soon, the requirements of Articles 44k.4 could ultimately put Viet Nam in breach of its international obligations. We urge Viet Nam to duly account for these important commitments in its review process.

Additionally, the scope of localized data under the new Article 44k.4, covers “Vietnamese organisations and individuals”, which would indirectly affect all cloud service providers operating in Viet Nam. Such data localization requirements will increase the business costs of providing online services in Viet Nam, which may result in end-users and SMEs in Viet Nam paying additional costs or being deprived of advanced offshore enterprise services and may impede their ability to compete internationally.

Furthermore, we note that under the new Article 44i.3, data created by state agencies are required to be stored only in Viet Nam. While this requirement may stem from concerns regarding the security of data created by state agencies, how the data is being protected is more important than where the data is located. Indeed, the most direct path toward improved security is in prioritizing and funding the effective implementation and operationalization of strong, existing cybersecurity and data security risk management practices. **BSA continues to strongly urge Viet Nam to remove the data localization measures in Articles 44i.3 and 44k.4.**

- c) While data center service providers are no longer required to “develop and implement technical plans and solutions to promptly detect and prevent illegal activities”, the new Article 44dd requires data center service providers to have technical plans “compatible with the standards and technical regulations on network information security and protection of service users' data”. In addition, Article 44i.2 requires data center service providers to meet the “minimum standard of level 3 in accordance with TCVN 9250” when providing services to state agencies. While BSA agrees that data center service providers should employ reasonable and appropriate security measures to safeguard customers' personal data, it would be **helpful to reference the specific international standards to which the legislation is referring in Article 44dd and further urge that these "standards and technical regulations" be aligned with internationally recognized security standards.**
- d) **The scope of possible violations in Article 22.2(a) has been widened significantly.** While the previous draft limited violations to breaches of Article 5 of Decree 72, Article 8.1 of the Cybersecurity Law and Article 28 of the Intellectual Property Law, the current draft extends this to

² CPTPP, Article 14.11, “[e]ach Party shall allow the cross-border transfer of information by electronic means...”

³ CPTPP, Article 14.13, “No Party shall require a covered person to use or locate computing facilities in that Party's territory, including personal information, when this activity is for the conduct of the business of a covered person

“the laws of Viet Nam”. This widened scope, which does not specify the laws and regulations which businesses should take note of, generates legal uncertainty for businesses and would likely increase compliance and legal costs considerably. **In the circumstances, we urge Viet Nam to reinstate the language used in the previous draft of Decree 72, which referred specifically to violations arising from Article 5 of Decree 72, Article 8.1 of the Cybersecurity Law and Article 28 of the Intellectual Property Law.**

As many of the points stated above have been raised in detail in our previous submission on Decree 72 in September, please find re-enclosed our submission for your consideration. We would also urge the Government of Viet Nam to conduct in-depth consultations with the enterprise-focused cloud services and data center services industry, including relevant impact assessments of the proposed regulations on the industry.

Please do not hesitate to contact us if you require any clarification or further information. Thank you once more for the opportunity to comment on Decree 72.

Sincerely,



Tham Shen Hong
Manager, Policy – APAC



3 September 2021

BSA COMMENTS ON PROPOSED AMENDMENTS TO DRAFT DECREE 72

Submitted Electronically to the Ministry of Information and Communication

BSA | The Software Alliance (BSA)¹ welcomes the opportunity to provide our comments to the Ministry of Information and Communication (**MIC**) on the proposed amendments to Decree 72 on the Management, Provision and Use of Internet Services and Online Information (**Decree 72**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that spark the economy.

BSA commends the Government of Viet Nam for soliciting stakeholder input on Decree 72 and its aim to improve the regulation of digital services and promote a safe online environment in Viet Nam. Enacting sound policies and regulations can help to grow a vibrant and innovative domestic digital economy which will enable Vietnamese companies to engage with the global digital economy.

This submission to the MIC provides comments and recommendations on the following topics:

- Scope of Covered Entities under Cross-border Provision of Information
- Obligations related to "Business Data Center Services"
- Extraterritorial Application of Decree 72
- Data Localization Requirements

Scope of Covered Entities under Cross-border Provision of Information

BSA is concerned with some of the proposed amendments under Article 22² which will be imposed on organizations involved in the cross-border provision of information, including those that "lease space for digital information storage in Viet Nam" (i.e., provide hosting services) or are accessed by 100,000

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](https://twitter.com/BSAnews).

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

² Article 22.2 and 22.3, Draft Decree 72.

unique visitors monthly. These include requirements to: i) collaborate with MIC to take down or block access to illegal content on their platforms; ii) store data and set up a branch or representative office in Viet Nam according to the Cybersecurity Law and its guiding regulation; iii) enter into content cooperation agreements with Vietnamese press agencies; and iv) establish a department dedicated to receiving, processing, and responding to requests from competent authorities and handle complaints from Vietnamese users within 24 hours from receipt of the complaints.

We understand that Decree 72 is part of Viet Nam's larger effort to develop policies and regulations for the Internet in Viet Nam. In developing these regulations to promote a safe online environment there should be a clearer distinction between consumer-facing entities - such as online news websites, social media, and e-commerce platforms, and providers of enterprise services or B2B services. Unlike consumer-focused services, enterprise services are not typically used by consumers but instead by organizations of all sizes and across all industries to operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow. In some cases, B2B service providers have no way to establish how many end-users their corporate customers have granted access to the services.

Obligations under Article 22 currently cover entities that are "providing information across border that lease space for digital information storage". For avoidance of doubt, we request that **the provision include language excluding enterprise focused cloud service providers and data center service providers from the scope**. Such enterprise service providers typically have limited access to their business customers' data, including any communications content, individual end-user identities, or contact details. Access to and knowledge of an enterprise customer's data is generally limited by privacy and security controls built into enterprise products and enforced by contractual terms between the enterprise service providers and their business customers. These entities are also subject to security and privacy laws of other jurisdictions that require them to keep such data strictly confidential. Furthermore, it is the enterprise service customer (not the service provider) that holds the relationship with the ultimate end-user or consumer and has effective control of such data. Therefore, to subject enterprise service providers to the obligations under Article 22 would not only be technically and practically unfeasible; it could also place these entities in breach of their contractual and other legal obligations.

Requests to block or 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 the business customer such as a cloud service provider or data center service provider. The enterprise customer will be best placed to deal with requests of this nature. In most instances, an enterprise service provider will pass such requests onto the customer for action. We therefore recommend for the **obligations under Article 22 to be applied appropriately to only the consumer facing businesses that deal directly with individual customers** and are making information available for access by the public at large.

The 24-hour time period for entities to identify and remove violating information that has been reported and to take appropriate action also causes undue operational burdens. If enterprise service providers are not clearly removed from scope, 24 hours is insufficient for an overseas service provider, which may be operating in a different time zone, to consult with the customer responsible for publishing the content and to enable that customer to take the necessary action, including the conduct of investigations and/or remediation decisions. Instead of an arbitrary threshold of 24 hours, we recommend that **the response time be amended to "as soon as practicable" or "without undue delay"**.

Obligations related to "Business Data Center Services"

The current draft Decree 72 introduces a new chapter under Article 44 requiring providers of data center services to register with the MIC and to comply with standards and technical regulations in designing, building, and operating the data center, to have the necessary tools to manage and store customers' information, and to have a process to validate and protect customers' data. BSA

acknowledges the need to ensure that the provision of cloud services meets security, reliability, and availability requirements. However, any domestic regulations should be aligned with internationally recognized security standards, such as the ISO 27000 family of standards (and cloud-specific updates in ISO 27017 and 27018), to ensure interoperability and assurance of security compliance.

Article 44h.1 contains additional obligations for service providers to “develop and implement technical plans and solutions to promptly detect and prevent illegal activities.” As we highlighted earlier, in many instances, cloud service providers do not have visibility into the content of their customers and are also subject to contractual and other legal obligations to preserve the secrecy of such content. Compliance with Article 44h.1 would thus require cloud service providers 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. Moreover, efforts to comply with Article 44h.1 would be inconsistent with Article 44h.4, which prohibits cloud service providers from accessing, using, or disclosing their customers’ data without the customers’ consent. Hence, it is highly impractical to obligate cloud service providers or data center service providers to detect and prevent illegal activities. In addition, it is unrealistic to place the burden of determining what is “illegal” on the cloud service provider. Therefore, we recommend for MIC to **revise Article 44h to ensure that the obligations are placed on the consumer facing customers of the data center services which are the most appropriate parties to address content related concerns**. We further recommend that a data center service provider should be required to discontinue its service with a particular customer only after receiving a court judgment confirming that its customer has violated the applicable law

Extraterritorial Application of Decree 72

Offshore companies appear to be expected to comply with certain provisions under Decree 72 such as Article 22.7 and Article 44h. However, it would neither be practicable nor enforceable for Viet Nam to exercise extraterritorial jurisdiction of these provisions over offshore companies. For example, it would be difficult for offshore companies to take down customer content hosted on their systems deemed to be unlawful in Viet Nam but not considered illegal in the jurisdiction under which the offshore company operates. Offshore companies may also not be in a position to assess and act on notifications or complaints by individuals in Vietnam regarding the legality of content hosted on their systems. Given so, we respectfully recommend that **Decree 72 should only be applicable to entities formed or established under the laws of Viet Nam, and the provisions should be exercised in line with emerging international approaches to privacy and electronic transactions**.

Data Localization Requirements

Limitations on the cross-border transfer of personal data in the form of data localization or other highly restrictive requirements do not advance data protection goals and may trigger unintended consequences. They disrupt companies’ operations and make it costlier to provide services in Viet Nam, even if that is not the intent, effectively depriving end-users and particularly SMEs in Viet Nam of advanced services and putting them at a competitive disadvantage compared with companies in other countries. Currently, many Vietnamese enterprises and startups rely on offshore enterprise services, such as cloud computing, to (1) improve security, (2) ensure quality control, and (3) access innovative services in data analytics, machine learning, and the Internet of Things. The data localization requirements in Decree 72 will cut off Vietnamese companies from the services they are already using to serve customers, causing significant disruption to their services and business models. Furthermore, beyond the economic benefits that cross border data flows can bring, the COVID-19 pandemic has also demonstrated the importance of cross-border data flows in enabling

data sharing for medical research and the adoption of digital services such as online video calls with friends and family to stay in touch during lockdowns. **We strongly recommend that the measures outlined in Article 22.3(d) and Article 44h.5 be removed.**

Conclusion

Once again, BSA expresses our appreciation to MIC for the opportunity to comment on Decree 72. If you require any clarification or further information in respect of this submission, please contact the undersigned at eunicel@bsa.org.

Yours faithfully,



Eunice Lim
Senior Manager, Policy – APAC
BSA | The Software Alliance