9 July 2026

BSA COMMENTS ON THE DEVELOPMENT OF A LAW ON DATA SECURITY

Respectfully to: The Ministry of Public Security

The Business Software Alliance (**BSA**)[1] thanks the Ministry of Public Security (**MPS**) for the opportunity to comment on the development of the Law on Data Security (**DSL**). BSA is the global trade association of the enterprise software industry. Our members are leaders in artificial intelligence (**AI**), cybersecurity, cloud computing, and other cutting-edge technologies. Over the past years, we have actively engaged with the MPS on cybersecurity,[2] personal data protection,[3] and other laws related to data governance.[4]

National Data Sovereignty

The Policy Dossier on the DSL envisages risk-based governance and layered protection aimed at building a "self-reliant and resilient ecosystem" in which: (1) Core Data requires domestic cryptography and dedicated air-gapped infrastructure; (2) Important Data requires storage of "original" data domestically; and (3) other data is allowed "flexible flow" with a "post-audit" management mechanism and governed by international safety standards. According to the Policy Dossier, this will allow Vietnam to maintain its independence and autonomy in cyberspace, preserve its digital sovereignty, and avoid falling behind in the global economic race.

The Policy Dossier further sets out the following steps to achieve digital sovereignty:

- Build a national data catalogue, classify data groups to apply corresponding protection levels, avoid equating business data with security data.
- Establish a smart "digital border": operate a national data security management unit to automatically monitor data flow 24/7, detect anomalies without reading the content of business data.

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] Examples include attending the Workshop on the Cybersecurity Administrative Sanctions Decree organized by the MPS in November 2022. BSA's most recent comments on cybersecurity were on 6 March 2026 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-draft-decree-detailing-articles-cybersecurity-law.

[3] Examples include presenting views at the Seminar on Personal Data Protection in June 2024 organized by the MPS. BSA's most recent comments on personal data protection were on 3 October 2025 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-decree-on-the-law-on-personal-data-protection.

[4] See BSA Comments on the Draft Decree and Draft Decision to Implement the Data Law on 17 March 2025 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-decree-and-draft-decision-to-implement-the-data-law, and BSA Comments on the Draft Data Law on 4 September 2024 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-data-law.

- Master storage infrastructure: issue mandatory technical standards for domestic infrastructure service providers to meet data protection standards.
- Study a mechanism for "digital post-auditing" and replace licenses with online monitoring and inspection based on signs of violations.

BSA supports Vietnam's ambition to strengthen resilience, trust, and innovation. However, genuine digital sovereignty is not achieved by restricting global cooperation or limiting technology choices — it is built on internationally-recognized standards, transparent governance, and the ability to operate confidently in an open and interconnected digital ecosystem. The challenge for policymakers is to reconcile Vietnam's legitimate desire for control with the realities of an interdependent global digital economy.

Recommendation: Sovereignty controls should only be applied according to the risk, in full knowledge of the trade-offs, such as innovation, security, and feature availability. Ultimately, it should be up to the individual organization, whether public sector body or critical infrastructure operator, to determine where controls are required and how trade-offs are made, according to the risk and potential impact.

Ensuring Data Security

The DSL proposes to ensure data security based on a four-level risk classification system, i.e.:

- Level 1: Data that directly impacts the independence, sovereignty, national defense, security and the stability of the regime. Level 1 Data is also known as Core Data.
- Level 2: Data that directly impacts the operation of the national information infrastructure, social order and security, and the macroeconomic economy.
- Level 3: Data that directly impacts the privacy and honor of citizens and the legitimate interests of organizations on a large scale.
- Level 4: Public and commercial data with low impact level but still must be managed and protected according to the law.

Levels 1 and 2 require special technical measures, including the mandatory application of "data shield" technology, physical isolation of top-secret data, and access controls based on national biometric identification. Levels 1 and 2 will use dedicated infrastructure, domestic encryption, and special multi-factor access control. Levels 3 and 4 will use shared infrastructure that is highly flexible and prioritizes connection speed and sharing. The Policy Dossier states that "[d]ividing data into 4 levels allows for extremely fast flow of level 3 and 4 data, promoting the digital society and digital economy." Further, the DSL looks to prioritize the use of domestic hardware, software, and cryptography solutions to eliminate the risk of "backdoors" from foreign suppliers.

If a significant amount of data held by private sector entities may be classified as Level 1 or 2, e.g., financial sector or healthcare sector data, there will be a bottleneck in the transfer and use of such data, which will slow commercial activity, degrade security, and harm innovation.

Vietnam has already enacted the Data Law which categorizes data into three categories: Core, Important, and Other data. The DSL should clarify the interaction between the categories in the Data Law and the proposed four-level classification system under the DSL. Rather than pass the

DSL as a separate and potentially overlapping law, Vietnam should amend its current laws to rationalize existing data governance requirements, avoid duplicative obligations, and establish a single coherent framework for data classification, protection, and cross-border transfers.

Recommendation: The DSL should adopt a narrowly defined and risk-based approach to data classification to avoid overclassification and unintended restrictions on economic activity. Levels 1 and 2 should be clearly defined and limited primarily to government-owned or government-controlled data that directly affects national defense, national security, public safety, or the operation of genuinely critical national infrastructure. They should not automatically include data that is widely held by the private sector, such as financial or healthcare data, or classify data as core or important because of the mere volume of data. Broadly classifying entire sectors or ordinary commercial, operational, or customer datasets as Level 1 or 2 data would create the very data bottlenecks the Policy Dossier seeks to avoid. Additionally, we recommend scoping Level 1 and 2 data narrowly, such as defining Level 1 data as those that directly implicate military or sensitive national security matters and remove broad terms such as "independence" and "social order."

Recommendation: The DSL should not mandate a preference for domestic hardware and software as this will reduce Vietnamese organizations' access to best-in-class technology solutions that will provide cutting edge security capabilities and allow Vietnamese organizations to integrate seamlessly into the international digital economy. Instead, the DSL should mandate internationally recognized standards that provide high levels of interoperability and security.

Recommendation: The DSL should prioritize the transition to post-quantum cryptography (**PQC**) by aligning with internationally recognized standards and global transition efforts. Vietnam should support the development of global standards and internationally interoperable quantum-safe policies, technical standards, and transition timelines while avoiding country-specific approaches that undermines interoperability, innovation, and security.

Ensuring Security in Cross-Border Data Transfers

The Policy Dossier states the policy objective of implementing digital sovereignty and ensuring national security, further stating that the requirement to store sensitive data in Vietnam "ensures that the managing agency always has the ability to access, control, and protect this resource from external interference or sanctions." The Policy Dossier further states the intent to establish a "controlled open" data flow management mechanism and to shift from a "prohibition" mindset to a "risk-based coordination" mindset. The Policy Dossier envisages "green lanes" for ordinary data to promote economic development, and "red lanes" to tightly control core and critical data, which together will create flexibility for the data economy without sacrificing national security. The restrictions on data flows and transfers may inadvertently also reduce the system redundancies built into best-in-class cloud services that may put critical data at greater risk of loss due to unforeseen circumstances[5] affecting locally mandated data storage.

[5] See for example: https://www.straitstimes.com/asia/east-asia/up-in-smoke-work-documents-of-191000-civil-servants-lost-in-data-centre-fire-in-south-korea

We welcome MPS' focus on promoting international integration and compatibility, such as internalizing international commitments on the Data Free Flow with Trust (**DFFT**) and through new generation free trade agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (**CPTPP**), EU-Vietnam Free Trade Agreement (**EVFTA**), and the ASEAN Digital Economy Framework Agreements (**DEFA**).

Although we recognize some utility in MPS' proposed "whitelisting" mechanism (i.e., a list of countries or organizations with data protection legal systems equivalent to Vietnam where businesses transferring data to these entities only need to notify the state and do not need to obtain prior approval from the authorities), we still have concerns with the state notification mandates, the whitelisting process, and with the treatment of non-whitelisted entities. For example, if the state notification requirements mean continued application of current requirements to submit extensive dossiers, such as current requirements under the Personal Data Protection (**PDP**) Law and the Data Law, the whitelisting mechanism will not meet its desired outcome of reducing the compliance burden on businesses. Likewise, if whitelisting procedures are overly restrictive or time-consuming, the whitelisting approach could ultimately impose more restrictions on cross-border data transfers than necessary.

Vietnam is also looking to move from digital "pre-audit" to "post-audit" by introducing Standard Contractual Clauses for businesses and international interoperability mechanisms such as certifications like the Global Cross-Border Privacy Rules (**Global CBPR**) system so that Vietnamese data can be transferred within economic alliances without renegotiating from scratch. Similarly, if businesses are nevertheless required to fill in extensive dossiers for each data transfer, the desired outcomes will not be met.

BSA strongly supports the importance of facilitating cross-border transfers, including of personal data. We appreciate the acknowledgement in both the Draft Policy Impact Report and the Draft Report on the State of Personal Data Protection of the importance of international data transfers, such as in relation to Vietnam's commitments in the CPTPP and EVFTA.

Recommendation: We strongly recommend that the DSL refrain from introducing any new cross-border data transfer requirements. Instead, the DSL should serve as an opportunity to rationalize and consolidate the overlapping transfer obligations that already exist between the PDP Law and the Data Law. The DSL should establish a single, coherent framework rather than adding another compliance layer. The Policy Dossier has identified legal fragmentation and overlapping obligations as "one of the biggest limitations" of the current data governance landscape. Introducing more transfer requirements — even with refinements — risks compounding exactly the fragmentation that the DSL seeks to resolve. Businesses that have already invested in building transfer compliance systems under the PDP Law should not face a second, potentially conflicting set of obligations for the same data transfers.

The DSL should clarify that the mere technical routing or transitory processing of data through infrastructure located outside Vietnam does not, by itself, constitute a regulated cross-border transfer. The DSL should also state that original data processing on Vietnamese territory is not required if remote access to sensitive data can satisfy Vietnam's policy objective of implementing digital sovereignty and ensuring national security. In addition, if data processing and cross-border

transfer impact assessments are imposed for particular circumstances, they should be required to be submitted to the MPS only upon request, as opposed to being required in every case. This would be consistent with international best practice and would help both companies and regulators better focus their resources on material instances.

This is a valuable opportunity for Vietnam to adopt internationally recognized personal data transfer mechanisms without additional requirements, such as the mandatory Data Transfer Impact Assessment under the PDP Law. Such mechanisms include the EU Standard Contractual Clauses (**EU SCCs**), the ASEAN Model Contractual Clauses (**ASEAN MCCs**), and the Global CBPR. Recognizing these mechanisms reduce regulatory burdens on businesses and regulators alike, facilitate trusted cross-border data flows, and further Vietnam's objectives of international integration and digital economic growth.

Should Vietnam choose not to adopt this approach, it should remove duplicative reporting requirements and avoid adding additional reporting obligations for cross-border data transfers. The DSL should include an explicit non-duplication clause providing that where a data transfer is already subject to requirements under the PDP Law, the Data Law, or any other law, only a single reporting needs to be made for that transfer.

Ensuring Security in AI and New Technology Applications

One of the policy objectives of the DSL is to promote the application and development of AI and new technologies, specifically to encourage the development of large-scale language models and purely "Vietnamese" AI systems and reduce dependence on foreign algorithms. Creating such domestic AI systems — including customization on local languages to deliver enhanced services, as an example — is a laudable goal. However, restricting the use of technologies to only domestic or homegrown businesses will limit Vietnam's sovereign innovation efforts.

For instance, the DSL should consider how Vietnam's current legal regime could inadvertently restrict domestic AI innovation, such as within the Intellectual Property (**IP**) regime and the recent Implementing Decree of the IP Law. BSA recently submitted comments[6] in which we recommend: (1) ensuring that Vietnam's text-and-data mining exception applies to both commercial and non-commercial uses; and (2) eliminating the requirement that the model developer must ensure that the "output" of an AI system does not compete with the rights holders' content, among others.

Recommendation: If the objective of the DSL is to encourage the development of large-scale language models and domestic AI systems, Vietnam should ensure that its broader legal framework supports AI innovation. In particular, the Government of Vietnam should consider BSA's recommendations on the IP Law and its Implementing Decree, including permitting text-and-data mining for commercial purposes and removing restrictions that limit the practical development and deployment of AI systems. Restrictive text and data mining rules may inadvertently hinder the development of the very domestic AI capabilities that the DSL seeks to promote.

[6] BSA Comments on the Draft Decree for the Implementation of the Intellectual Property Law on Copyright and Related Rights, 12 March 2026 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-draft-decree-implementation-intellectual-property-law-copyright-related-rights.

The Policy Dossier states that the DSL will clearly define the responsibilities of the entities developing and operating AI for the consequences caused by algorithms protecting the ideological foundation and social security and the legitimate rights and interests of agencies, organizations and individuals. In addition, the Policy Dossier establishes four levels of AI risk, mandatory labelling requirements for AI-generated content, and other requirements. However, all these concepts are already established under the AI Law.

Recommendation: The DSL should not duplicate AI governance requirements that have already been established under the AI Law, including AI risk classifications, obligations relating to AI-generated content, and accountability frameworks for AI actors. Overlapping requirements across multiple laws create legal uncertainty, inconsistent implementation, and duplicative compliance burdens for organizations subject to oversight by different government agencies. The Government of Vietnam should avoid introducing the same type of regulatory overlap and fragmentation that the DSL seeks to address in the broader data governance framework.

Several AI-related measures proposed in the Policy Dossier raise concerns outside of potential overlap with the AI Law. These include requirements relating to the publication of algorithm standards, government access to source code or algorithmic logic, the mandatory retention of content creation logs, and requirements to conduct penetration testing of large AI systems for misinformation or public opinion manipulation risks. While BSA supports efforts to address harmful uses of AI, such measures may create significant risks for the protection of confidential business information, intellectual property, cybersecurity, and innovation. Moreover, concerns relating to misinformation, content moderation, and public opinion manipulation generally arise in the context of consumer-facing social media, search engines, and other business-to-consumer (**B2C**) platforms, rather than enterprise AI systems and business-to-business (**B2B**) applications that are designed for internal business use.

Recommendation: The DSL should avoid imposing requirements that mandate disclosure of source code, proprietary algorithms, model weights, or other confidential technical information. Any transparency, accountability, or risk management requirements should be proportionate to the risks presented and targeted at the categories of AI systems most likely to give rise to those risks. Obligations addressing misinformation, content moderation, and public opinion manipulation should focus on consumer-facing platforms and services rather than enterprise AI systems and B2B applications. A targeted, risk-based approach better addresses legitimate public policy concerns while maintaining innovation, cybersecurity, intellectual property, and investment incentives.

Transition Period

The DSL delegates significant authority to implementing regulations and to the National Data Security Management Unit, where the true scope of its obligations — including mandatory technical standards — will ultimately be determined. As such, the principles of stakeholder consultation and proportionality should be enshrined in the law itself, rather than left to the discretion of implementing agencies. Introducing obligations prematurely, especially where technical standards remain undefined, risks creating compliance uncertainty without corresponding security benefits.

Recommendation: Enshrine consultation and proportionality as statutory principles in the DSL, and establish a mandatory prior consultation mechanism requiring consultation with industry stakeholders before issuing or revising mandatory technical standards. Provide grandfathering provisions for existing system architectures and contractual arrangements structured in compliance with laws in force at the time of the DSL's enactment. Phase in compliance obligations with a minimum transition period of 12 to 18 months following the publication of implementing guidelines, giving organizations sufficient time to prepare, allocate resources, and build robust governance frameworks that align with both domestic requirements and international best practices.

BSA Resources

To support the MPS's deliberations on the DSL, we share the following relevant BSA position papers that may serve as useful references.

- **Keeping the Door Open: The EU's Path to Digital Sovereignty** provides BSA's recommendations for a practical and open approach to Europe's digital sovereignty,
- **Enterprise AI Adoption Agenda for ASEAN** provides policy recommendations for ASEAN member states to achieve the broad adoption of enterprise AI,
- **Principles for Government Cloud Security Laws and Policies** describes recommended approaches for cloud security laws and policies,
- **Quantum Computing and Encryption: Six Actions Governments Should Take to Secure Information** provides the steps for governments to transition to PQC, and
- **BSA 2026 Quantum Technologies Agenda** provides recommendations to government for long-term quantum leadership.

Conclusion

We would like to thank the MPS for considering our comments on the development of the DSL and hope that you will positively consider our recommendations. We urge the 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.

Yours sincerely,

Wong Wai San

Wong Wai San
Director, Policy – APAC