Business Software Alliance

6 November 2026

BSA COMMENTS ON THE UPDATED DRAFT LAW ON DATA SECURITY

Respectfully to: The Ministry of Public Security
Copy to: The Committee for National Defense, Security and External Relations of the National Assembly

The Business Software Alliance (**BSA**)[1] respectfully submits the following comments on the updated Draft Law on Data Security (**DSL**) dated 28 September 2026, as submitted to the National Assembly. 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.

BSA has engaged with the Ministry of Public Security (**MPS**) throughout the development of the DSL, including through our comments on the Policy Dossier and the draft DSL in July and August 2026.[2] We also appreciated the opportunities to discuss our views with Minister Luong Tam Quang in Hanoi in August 2026 and at the US Chamber of Commerce delegation meeting on the sidelines of Singapore International Cyber Week on 14 October 2026, and with Lieutenant General Le Xuan Minh at the Digital Policy Dialogue on 15 October 2026.

BSA welcomes the improvements in the updated draft, especially the effort to reduce duplication and apply requirements proportionate to the level of risk involved. As the National Assembly considers the draft, the next step is to ensure these improvements produce a coherent framework across Vietnam's data, privacy, cybersecurity, and AI laws, with clear responsibilities and fewer overlapping compliance requirements.

Positive Developments in the Updated Draft

The revisions address several concerns raised during the public consultation, and we appreciate the time the MPS has taken to consider them.

The updated draft clarifies the relationship between the DSL and existing laws. Personal data protection remains under the Personal Data Protection (**PDP**) Law, data governance and classification under the Data Law, and the cybersecurity of information systems under the

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

[2] BSA Comments on the Development of a Law on Data Security on 13 July 2026 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-development-of-a-law-on-data-security, and BSA Comments on the Draft Law on Data Security on 5 August 2026 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-law-on-data-security.

Cybersecurity Law, while the DSL focuses on the security of data itself (Article 3.2). Where obligations overlap, the draft provides for a single dossier and procedure (Article 3.3).

The revisions strengthen the risk-based approach. Data administrators determine the risk level of their data, and obligations increase with that level (Articles 4.5 and 8). Level 1 data requires no dossier. Level 2 data requires a simplified data security protection plan, from which household businesses, micro enterprises, small enterprises, and innovative start-ups are exempt (Articles 10.1-10.3). Data that is considered Core Data solely because it meets the threshold for the number of data subjects or data volume is treated as Level 3, except in certain cases prescribed by law (Article 8.3). A data administrator that follows official guidance from the specialized data security authority on determining risk levels is also protected from sanctions for misclassification of levels in respect of the matters covered by that guidance (Article 8.8).

The draft adopts a risk-based framework for storing and transferring data abroad (Article 19):

- data at Levels 1 and 2 requires no procedure under the DSL;
- data at Level 3 requires solely a self-assessment; and
- approval for Level 4 and 5 data may continue to apply to repeated transfers within the same data flow, without a new approval for each transfer, provided there is no change in purpose, type of data, recipient, or safeguards.

We also welcome the protection of source code and model weights during appraisals and inspections (Article 11.7), the voluntary use of security cryptography for data that is not a state secret (Article 16.3), and the continued validity of existing transfer approvals and assessments (Article 29.2).

We welcome the removal of fines calculated as a percentage of revenue, and the principle that a violation covered by several laws is sanctioned only once (Article 26.12). Restrictions on cross-border services are subject to procedural safeguards and a 90-day limit (Article 20).

Completing the Rationalization of Overlapping Obligations

The Policy Dossier for the DSL identified legal fragmentation and overlap as one of the biggest limitations of Vietnam's data governance framework. The updated draft makes significant progress. It redirects the Data Law's procedures for transferring Core and Important Data, and its risk assessment requirements, to the DSL (Article 27.2). It also recognizes valid results of assessments, appraisals, inspections, audits, and certifications lawfully conducted under other laws (Article 3.3b) and allows a single incident report to satisfy reporting and notification obligations to the MPS for the same incident under the Cybersecurity and Personal Data Protection Laws (Article 3.3c). The value of these changes will depend on Decree 165, Decree 356, and the implementing decrees of the Cybersecurity Law being amended consistently before the DSL takes effect, and on addressing remaining overlaps in supply chain assessments, volume thresholds, and impact assessments.

For example, Article 18.3c requires products and services that connect to or access data at Level 3 or above to undergo cybersecurity assessment and examination before connection. For enterprise software deployed across many customers, this could lead to repeated reviews of the

same product or shared platform unless existing assessments and certifications are recognized. The draft also relies on several separate volume measures:

- the large-scale threshold for sensitive personal data (Article 8.1c);
- the threshold for large-scale processing (Article 14.1); and
- the thresholds for the number of data subjects or data volume used to determine Core Data under Decision No. 20/2025/QĐ-TTg (Article 8.3).

Recommendation: Amend Decree 165 and other affected implementing instruments consistently with Article 27 before the DSL takes effect. Publish a policy map to show which existing obligations are replaced, retained, or supplemented, and align incident reporting deadlines and content across the unified reporting system.

Recommendation: Recognize existing assessments and relevant certifications for the purposes of Article 18.3c, so that a product or shared platform assessed once does not need to be reassessed for each customer, with supplementary assessment only for distinct risks. Publish workable criteria for recognizing certifications under Article 10.7b. Align the volume thresholds and counting methods under Articles 8.1c, 8.3, and 14.1 with each other and with Decision No. 20/2025/QĐ-TTg, in consultation with industry. For personal data, confirm under Articles 3.3b and 10.7a that the security content of a PDP Law impact assessment is recognized for the data security impact assessment under Article 10.4, with supplementary information required only for security matters it does not cover.

Obligations Should Be Aligned with Risk and Control

The practical effect of the risk-based approach will depend on how data is assigned to each level. Certain types of data may be classified as Level 3 due to the volume processed, such as sensitive personal data processed at large scale, and data classified as Core Data under the Data Law because of its volume. Data at Level 3 is subject to requirements for a data inventory, impact assessments, and periodic audits, as well as access control and logging. This is especially relevant for enterprise software providers serving customers in the financial, healthcare, and human resources sectors, whose routine business-to-business services involve processing large volumes of such data. If the criteria are broad, a large share of ordinary commercial processing could be classified as Level 3 without such data presenting a higher security risk.

Similarly, the requirement to immediately disconnect and revoke the provider's data access rights upon detecting a data security risk or incident, including for Level 1 and 2 data (Article 18.4.c and 18.5), could inadvertently undermine incident response and prevent authorized security teams from deploying patches, containing attacks and restoring services. This is particularly significant for enterprise cloud and software providers, who operate and secure infrastructure or applications that customers cannot administer themselves. The law should require restricted access to allow proportionate containment and remediation of the affected connection or processing activity.

We welcome the draft's approach of placing responsibility for determining risk levels on the data administrator. Article 18.2 allocates responsibility according to role. A data processor is

responsible for the tasks assigned to it, while the data administrator remains responsible for matters within its own management and decision-making. Enterprise cloud and software providers typically process data on behalf of their customers and may have limited visibility into customer content and limited authority over its use. As the DSL does not define "data administrator," these providers could be treated as data administrators and become responsible for classifying, assessing, and protecting customer data they do not control.

Recommendation: Delete Article 8.6. Under the Data Law, Important and Core Data are the data on the lists issued by the Prime Minister. Requiring data administrators to identify unlisted data as Important or Core Data, and to apply the corresponding measures pending an update, creates uncertainty that is inconsistent with this list-based approach and with Article 8.2. The competent authorities' powers to review and update the lists (Article 8.7) and to re-determine levels (Article 8.9) are sufficient to address new categories of sensitive data.

Recommendation: Explicitly define "data administrator" and "data processor" in Article 2, aligning them with existing definitions in the PDP Law and internationally recognized frameworks. Clarify that a party processing data on behalf of a customer is a data processor and not a data administrator. Confirm that, under Article 18.2, a data processor's responsibilities are limited to the processing tasks and technical controls agreed with the customer, while classification, impact assessment, and transfer decisions remain with the data administrator. An enterprise cloud or Software-as-a-Service provider that processes data on behalf of and under the instructions of its customers should be considered a data processor, regardless of the technical infrastructure it manages. Where a cloud provider offers the same service to multiple customers, it should not be required to independently classify or assess each customer's data. The customer, as data administrator, should be the party bearing that obligation.

Recommendation: Under 18.4 and 18.5, allow controlled access necessary to protect the service and for defined security operations. Wider disconnection of provider services should only be mandatory where continued access presents an unacceptable risk. These clarifications would align providers' security responsibilities with the operational authority needed to fulfil them, while preserving data administrators' oversight and safeguards against misuse.

AI systems. Article 15.2 places the same obligations on all organizations that research, develop, provide, or deploy AI systems processing data at Level 3 or above. These include ensuring the lawful origin of training data and preventing the extraction of training data from a model. An enterprise that deploys a third-party model cannot verify how that model was trained or change how the model responds to extraction attempts. These are matters solely within the model developer's control.

Recommendation: Allocate the obligations in Article 15.2 according to each party's role. Obligations relating to training data and model design should rest with model developers. Deployers should be responsible for how they configure and use the AI system, including the controls on autonomous AI systems in Article 15.2e. Clarify that the requirement within Article 9.4 to use de-identified or synthetic data when using data classified as Level 3 and above for AI

training does not apply to enterprise customers and their authorized service providers who fine-tune or configure AI features within a specific, contractually defined scope and purpose.

Cross-Border Data Transfers

Enterprise software and cloud services rely on secure international infrastructure, including geographically distributed systems for redundancy and disaster recovery, global threat detection, and encryption key management. The updated draft supports these operations by requiring prior approval only for transfers of the highest-risk data.

Encryption keys. Under Article 19.1b, encrypted Level 3 or Level 4 data stored abroad is not treated as transferred where the data administrator manages the decryption key in Vietnam and the foreign party neither holds nor controls it. To the extent this eases the ability to securely transfer and store data internationally, this is a welcome development. However, it should not become a de facto requirement to manage keys in Vietnam. Many organizations protect their data with customer-managed keys held in globally distributed key-management services. This approach maintains customer control of the encryption keys, and consequently the security of their data, while providing resilience and security of both the keys and the data.

Recommendation: Confirm that Article 19.1b offers an additional option and is not a condition for lawful transfer. Apply it wherever the data administrator controls the decryption keys and the service provider does not hold them, regardless of where the keys may be physically located. Preserve customers' ability to choose secure key-management arrangements, including managed services.

Recommendation: Recognize internationally accepted transfer mechanisms, such as the Global Cross-Border Privacy Rules system and the ASEAN Model Contractual Clauses, as satisfying the corresponding elements of the Level 3 self-assessment and as evidence of adequate safeguards in Level 4 and 5 appraisals. Any additional requirements should be limited to residual security risks that the mechanism does not address, such as encryption and access controls for the data transferred.

Implementation

Much of the DSL's practical effect will be determined by implementing decrees and guidance, including the criteria for determining risk levels and specifying the volume thresholds. Several obligations must be met within 12 months of the effective date (Article 29). Existing Level 4 and 5 systems must complete their first audits and put monitoring in place. Data administrators of Level 2 data must prepare protection plans. These deadlines may arrive before the relevant decrees and templates are available.

Recommendation: Conduct public consultations of at least 60 days on implementing decrees and guidance and issue them well before the DSL takes effect. Start the transition periods under Article 29 from the issuance of the relevant decrees and guidance rather than from the effective date of the law.

Conclusion

We thank the MPS and the Committee for considering our comments on the DSL and hope that our recommendations will be taken into account. We welcome the opportunity to continue our warm engagement with the MPS as it develops the implementing regulations. BSA remains ready to serve as a resource to the MPS, providing policy input and sharing global perspectives and international best practices regarding the enterprise software industry. 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
Director, Policy – APAC