Business Software Alliance

5 August 2026

BSA COMMENTS ON THE DRAFT 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 Draft 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] We submitted comments on Policy Dossier for the DSL in July 2026[5] and sought meetings with the MPS to discuss the same.

Consultation Period and Process

The DSL interacts extensively with existing legislation, such as the Data Law, the Personal Data Protection (**PDP**) Law, the Cybersecurity Law, the AI Law, and their implementing decrees. One of the stated purposes of the DSL is to close gaps in and to rationalize Vietnam's data governance framework. Assessing whether the DSL achieves that purpose requires extensive cross-checking against existing regulations and the current consultation window does not provide enough time to do so. As such, the comments in this submission identify the most pressing and apparent concerns. They are not exhaustive, and further issues are likely to emerge in future.

We therefore respectfully urge MPS not to proceed with the passage of the DSL on the current timeline and in its current form. A law intended to rationalize the data governance framework will only succeed if the duplication, overlap, and gaps in the existing framework are first identified systematically, and that exercise has not yet taken place. The premature enforcement of the new

[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] 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.

[5] 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.

Cybersecurity Law, lacking necessary implementing regulations, has also resulted in operational gaps and business disruption. Proceeding before the rationalization process is completed risks furthering the very fragmentation the DSL is meant to resolve. As drafted, the DSL does not meet the objective within the policy dossier to rationalize requirements across existing laws — it merely overrides existing obligations where contradictions with existing laws arise (see Article 58.2). This means that companies still need to navigate a patchwork of data governance laws and continue to meet all existing obligations, including overlapping and duplicated obligations, unless there is contradiction with the DSL.

Across the DSL, the Data Law, the PDP Law, the Cybersecurity Law, and the AI Law, organizations face overlapping obligations that have different thresholds and timelines which apply to different categories of data, with responsibilities placed on differing entities. The DSL's volume-based classification thresholds in Articles 6.2 and 6.3 do not map onto the PDP Law's risk-based assessment thresholds under Decree 356, and the DSL's annual reporting requirement for cross-border transfers in Article 32.4 is at odds with reporting required only once during the operating period under Decree 165 and Decree 356. Further, the DSL's training data obligations in Article 26.1(a) apply to a different set of entities than the equivalent obligations under the AI Law; and the DSL's post-approval suspension power in Article 32.2 operates independently of, and without reference to, the administrative remedy procedures under the Cybersecurity Law. While Article 58.2 states that the DSL prevails in cases of contradiction, it does not address areas of overlap, inconsistent definitions, and misaligned thresholds.

Recommendation: Defer further movement of the DSL until a systematic review of duplication, overlap, and gaps in the existing data governance framework has been completed in consultation with industry. Extend the public consultation period to at least 60 days and conduct further rounds of consultation, including technical workshops with industry, before the DSL proceeds to the next stage. To support meaningful consultation, we encourage MPS to publish a mapping of how each provision of the DSL interacts with the Data Law, PDP Law, Cybersecurity Law, AI Law, and their implementing decrees. This mapping should specifically identify provisions where compliance thresholds across laws are inconsistent and where different definitions of roles and responsibilities result in conflicting and/or overlapping obligations. We also encourage MPS to provide opportunities to comment on draft implementing regulations, where the DSL will be operationalized.

Allocation of Roles and Responsibilities

Although Article 3.10 refers the definitions of data controller and data processor to the PDP Law and the Data Law, the obligations throughout the DSL are placed on the “manager of the information system” or on “organizations operating the data storage and processing information system” (e.g., Articles 6.3, 10.1, 20.2, 21.3, 35.2, and 55). This assigns obligations such as data classification, risk assessment, log retention, and monitoring connections to the party operating the infrastructure, who in enterprise computing is frequently a data processor. These data processors are typically cloud or software providers with no visibility into, or control over, the customer data processed on its systems. The data controller, who determines the purposes and means of processing and is best placed to classify data and assess risk, decides these matters

under the PDP Law, yet may carry no corresponding duty under the DSL. The result is that responsibilities under the two laws are assigned to different parties for the same data, creating obligations that the operator cannot practically discharge and may duplicate, overlap, or conflict with the allocation of responsibility already established under the PDP Law.

Recommendation: Align the allocation of roles and responsibilities in the Draft Law with the controller and processor framework under the PDP Law and the Data Law. Obligations that depend on knowledge of the data and the purposes of processing, including classification, risk assessment, and transfer decisions, should lie with the data controller, while data processors should be responsible only for the security measures within their actual control, consistent with the shared-responsibility model on which enterprise cloud services operate. Each obligation in the DSL should be reviewed to identify the party best placed to discharge it, so that the same data is not subject to duplicate, overlapping, or conflicting duties assigned to different parties under different laws.

Data Classification

Article 6 classifies data into four levels: Ordinary (Level 1), Internal (Level 2), Important (Level 3), and Core (Level 4). Article 6.4 identifies Core and Important data as those with direct and immediate impact on national defense, security, social safety, finance and banking, energy, telecommunications, and emergency administration, and subjects them to the strict localization treatment, prohibiting any transfers outside Vietnam. However, the broad framing of any data with potential to impact finance and banking, energy, telecommunications is problematic and risks elevating the ordinary business or operational data of such sectors as Core and Important data, regardless of actual impact on national security or defense. Articles 6.2 and 6.3 further require that lower-level data when accumulated at scale shall be subject to a higher level of protection, with system operators required to deploy automated monitoring to detect and report threshold crossings. Additionally, the classification, inventorying, mapping, and risk assessment obligations in Articles 10 to 21 apply across all four levels, imposing a compliance baseline on every organization, including for low-risk data, that is disproportionate to the risk presented.

Articles 24.1-2 require data on the operation of technical infrastructure in the "*key national domains*" — Finance-Banking, Energy, Health, Education, Telecommunications and Transport — to be classified and protected at Important (Level 3) or Core (Level 4) level as a minimum and for all information systems in those domains, when connecting and interconnecting, to integrate technical solutions for real-time connection monitoring with the centralized monitoring system of the MPS. Article 35.2 requires Important Data managers to connect to and share alert information with that system. This results in a wide range of ordinary commercial and operational data attracting the most stringent tier of obligations, together with a permanent technical monitoring connection, because of the sector in which the customer operates rather than the sensitivity of the data itself.

As highlighted in our previous submissions, these provisions affect significant volumes of data held within the private sector and will result in a bottleneck in the transfer and use of such data, which inevitably 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 four-level classification system under the DSL.

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 3 and 4 should be clearly defined, cross-referenced against the Data Law, 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, transport, or healthcare data, or classify data as Core or Important because of its affiliation to a sector or the mere volumes of such data. Broadly classifying entire sectors or ordinary commercial, operational, or customer datasets as Level 3 or 4 data unnecessarily restricts the development of the digital economy, would create the very data bottlenecks the Policy Dossier of the DSL sought to avoid and cause significant disruption on ongoing businesses. The sectoral lists used across Articles 6.4, 16.2, 24.1 and 28.1 should be deleted outright. If retained, sectoral lists should only refer to those have a direct connection to critical national security functions.

Recommendation: Remove the volume aggregation mechanism in Articles 6.2 and 6.3. If retained, the quantitative thresholds should be established through consultation, published in advance, and set at levels that do not capture routine commercial data processing. In particular, thresholds for lower-level data categories, such as Ordinary and Internal data, must be calibrated to avoid penalizing companies that process large volumes of such data in the ordinary course of business; a volume-based trigger is an inappropriate proxy for security risk where the underlying data carries a low impact classification. Similarly, revise Article 6.4 to remove broad references to specific industry sectors, i.e., finance and banking, energy, and telecommunications. Further, the requirement to deploy automated threshold monitoring should not apply to private-sector systems processing Ordinary or Internal data. As Decree 165 implementing the Data Law already contains a volume-based rule for cross-border transfers; the two mechanisms should not overlap.

Recommendation: Article 24.1 should apply to the operational data of the physical infrastructure managed by a designated operator, rather than to a sector as such, and should expressly exclude commercial service data and customer data processed by technology providers on behalf of entities in those sectors. Where any automated monitoring of threshold crossings is retained (Articles 24.2, 35, and 38), access obligations to privately held data should be confined to aggregated alert metadata or system-log telemetry rather than raw data content, with explicit safeguards against government access to personal data or trade secrets. It should not confer any access or capability of access to systems shared with customers in other jurisdictions. Providers of multi-tenant platforms should be allowed to discharge these obligations through an interface operated by the Vietnamese customer rather than by direct connection to shared infrastructure.

Data Localization and Restrictions on Cross-Border Data Transfers

Article 28.1 requires Core and Important Data in the named sectors to be stored in data centers in Vietnam and permits the use of international cloud services only where a real-time backup is maintained in Vietnam under the "supreme control" of Vietnamese state agencies. Articles 28.3 and 28.4 compel foreign enterprises that violate Vietnam's data security or personal data protection law to establish local infrastructure and storage and any violations may subject such foreign enterprises to technical measures such as bandwidth restrictions and suspension of access to data flows within Vietnam.

Article 32.2 requires prior appraisal and written approval by MPS for transfers of both Important and Core Data. Article 6.4 prohibits outright the transfer of Important and Core Data with direct impacts on the named sectors, save for Government-approved exceptions. Articles 32.3 and 32.4 exempt trade secret data from prior appraisal where a whitelisted destination, standard contract, or conformity certification applies, but still require self-assessment dossiers and annual reports to MPS.

These provisions introduce new restrictions on cross-border data transfers that have wide impact. For instance, the DSL would now require prior approval for the overseas transfer of Important Data, introduce an outright transfer prohibition, and impose localization on privately held data in some cases. Instead of reporting once per operating period under the Data Law (see Decree 165) and the PDP Law (see Decree 356), the DSL now requires annual reports of data transfers abroad. Such measures are in contradiction to the post-audit approach envisioned in the Policy Dossier, and with Vietnam's commitments on data transfers and localization under the agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (**CPTPP**), European Union-Vietnam Free Trade Agreement (**EVFTA**), and the upcoming Digital Economy Framework Agreement (**DEFA**).

Recommendation: Remove the localization mandate for privately held data. Security outcomes, rather than storage location, should be the regulatory objective, and organizations should be permitted to use international cloud services that meet defined security requirements benchmarked by internationally recognized standards such as standard contractual clauses, binding corporate rules, or certifications the Global Cross Border Privacy Rules or those by the International Standards Organisation (**ISO**). The "supreme control" requirement should be replaced with clearly defined access, audit, and cooperation arrangements. If any localization obligation is retained under Article 28, it should be limited to data with a direct nexus to national security and should not apply to data held within the private sector.

Recommendation: Align the transfer regime with the existing framework under the Data Law and Decree 165: retain notification-only treatment for Important Data, reserve prior appraisal for narrowly defined Core Data, and remove the outright prohibition of overseas transfers in Article 6.4. If a prohibition is retained for a narrow category of state-held defense and security data, the law should set out clear criteria, procedures, and timelines for the exception mechanism, and in any case should not prohibit the transfer of data that is held within the private sector, such as finance and banking, energy, transport, and telecommunications.

Recommendation: Replace the annual reporting obligation in Article 32.4 with a single self-assessment dossier prepared once for the organization's operating period and updated upon material change, consistent with Decree 165 and Decree 356, and preserve the non-duplication principle established by Article 42.3 of Decree 356 so that a single assessment suffices where a dataset falls under multiple regimes. If the obligations in Article 32.4 are retained, the DSL should specify the conditions, notice requirements, and maximum duration for any post-approval suspension of data flows. Suspension should require a written, reasoned decision and take effect only after a defined and reasonable notice period.

Recommendation: Develop whitelisting, standard contract, and certification mechanisms in consultation with industry, and recognize internationally accepted transfer mechanisms, including the EU Standard Contractual Clauses, the ASEAN Model Contractual Clauses, and the Global Cross-Border Privacy Rules system, as valid bases for transfer without additional requirements for submitting reports or obtaining approval from MPS or similar competent authorities.

AI-related Requirements

Article 26 requires AI providers to verify and clean training data, integrate labelling solutions for AI-generated content, develop technical filters against harmful false information, and respond to requests from MPS to explain transparency of algorithms and training data sources. Article 26 further gives MPS the power to suspend AI services when an AI system seriously violates the provisions of the Law. These obligations substantially duplicate requirements already established under the existing AI Law, including those on training data governance, labelling of AI-generated content, and transparency. It also overlaps with obligations under the Intellectual Property (**IP**) Law and its implementing decree on the issue of IP and AI inputs and outputs. Again, while Article 58.2 states that the DSL takes precedence where other prior legal documents are in contradiction, it does not address overlap. The scope of the DSL extends beyond data security into domains already governed by the recently enacted AI Law and the recently updated IP Law, resulting in significant regulatory confusion.

Further, the DSL does not distinguish between AI model developers and enterprise application providers. Article 26.1(a) imposes the obligation to "establish a process for verifying and cleaning training data" and Article 26.2(b) imposes the obligation to explain the "training data sources" on all organizations and enterprises "researching, developing, operating and providing artificial intelligence services." This is fundamentally inconsistent with the architecture of enterprise AI deployment. Most enterprise applications, such as customer relationship management, productivity, and analytics platforms, embed third-party large language models (**LLM**s) whose training data was selected, assembled, and processed entirely by the foundation model developer, not the application provider. Providers of these enterprise applications do not have the contractual right, technical access, or practical ability to audit, verify, or clean the training datasets of a third-party LLM; that information is typically held as a trade secret by the model

developer. In contrast, the AI Law places training data obligations on the developer.[6] Articles 26 26.1(a) and 26.2 of the DSL impose responsibilities on entities that are not in a position to discharge, and risks penalizing downstream deployers for characteristics of a model they did not build and have no control over.

In addition, similar to Article 23 which contemplates disclosure of source code in MPS appraisals, the provision under Article 26.2 allows MPS to require explanations from AI providers, on the underlying logic of algorithms and compelling disclosures of proprietary training data sources upon request, does not contain protections for source code, model weights, trade secrets, or other confidential business information, which could seriously deter digital and AI innovation in Vietnam. Further, problems related to false information arise principally on consumer-facing platforms, hence the DSL should distinguish obligations and protections towards such consumer-facing platforms rather than a blanket requirement that also includes enterprise AI systems that carry low risk of misinformation.

Recommendation: Remove AI-related obligations from the DSL since they are already covered in the existing AI Law and IP Law. If the DSL continues to contain obligations related to AI governance, explain the relationship between the DSL, the AI Law, and IP Law, including which law takes precedence. Further, exclude source code, proprietary algorithms, model weights, and confidential technical information from mandatory disclosure. Obligations addressing misinformation and content manipulation should be targeted at consumer-facing services rather than enterprise applications. If retained, Article 26.1(a) and 26.2 should be amended to confine training data verification and cleaning obligations to AI model developers.

Incident Reporting

Article 38.3 requires a data security incident affecting Core Data to be assessed and reported within 2 hours of detection, with initial notification of other incidents within 24 hours, a full report within 72 hours and a post-incident review within 30 days. The short timeframes do not give organizations sufficient time to investigate an incident nor assess whether it is an incident that requires reporting. These reporting requirements are neither practical nor feasible and are out of step with other countries. Organizations need sufficient time to investigate an incident, assess its impact, and respond to mitigate harm before reporting.

[6] See Article 15.2(b) of Decree 142/2026/ND-CP (Decree 142), which places responsibility for ensuring the quality, suitability, and representativeness of training data on the AI provider. See also Article 12.3 of Decree 142, which recognizes that providers using third-party AI models are responsible only for information within their lawful access and control, and are not required to obtain or disclose underlying training datasets of foundation models developed by third parties.

Recommendation: As discussed in our previous submissions,[7] BSA urges the Government of Vietnam to harmonize cyber incident reporting obligations with international best practices, including what constitutes a cyber incident, the timeframes and thresholds for notification, and the type of information that must be submitted to authorities. As highlighted in BSA's *10 Principles for Cyber Incident Reporting Harmonization Around the Globe*,[8] harmonized requirements create a set of consistent data points from which stakeholders can efficiently and effectively share information, enhance threat intelligence, improve vulnerability management, adjust security controls, and expedite incident responses. The DSL should specify an incident reporting timeframe that is aligned both intra-nationally across Vietnamese laws and with international best practices. The reporting timeframe and thresholds should be commensurate with the information required, for example, the EU Network and Information Security Directive (**NIS2**) provides a 24-hour timeframe for a notification[9] and the US Cyber Incident Reporting for Critical Infrastructure Act (**CIRCIA**) will provide at least 72 hours for a report.[10]

Financial Penalties

Article 57.2 provides for fines of up to 5% of an organization's revenue in Vietnam for "particularly serious violations" involving Important and Core Data, and further allows the Government to prescribe fines calculated on the basis of group global turnover, capped at 5%, for multinational corporations whose revenue in Vietnam is "not commensurate with the scale and seriousness of the violation." The violations attracting these percentage-based fines are undefined and are delegated to the Government (Article 57.4). A fine calculated on global turnover, triggered by a yet-to-be defined government regulation, makes jurisdiction-specific risk a global issue in worst-case scenario planning. This is out of line with other data governance regimes in the region and is likely to deter foreign investment in Vietnam.

Recommendation: Base percentage fines on revenue generated in Vietnam only, and remove the global turnover basis. If a broader basis is retained for exceptional cases, the triggering principles and criteria should be defined objectively, in a closed list, and in proportion to the severity of the violation. Fines should be calculated exclusively on the Vietnam-sourced revenue of the directly infringing entity, consistent with international proportionality principles and Vietnam's own commitments under the General Agreement on Trade in Services (**GATS**), CPTPP, and EVFTA.

---

[7] See BSA Comments on the Draft Decree Detailing a Number of Articles in the Cybersecurity Law dated 6 March 2026 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-draft-decree-detailing-articles-cybersecurity-law, and BSA Comments on the Draft Cybersecurity Law dated 8 August 2025, and 26 September 2025 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-cybersecurity-law-dated-8-august-2025.

[8] BSA's 10 Principles for Cyber Incident Reporting Harmonization Around the Globe, February 2025, https://www.bsa.org/policy-filings/global-10-principles-for-cyber-incident-reporting-harmonization-around-the-globe .

[9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union 27 December 2022 at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[10] Cyber Incident Reporting for Critical Infrastructure Act of 2022, March 2022 at https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

Conclusion

We would like to thank the MPS for considering our comments on the DSL and hope that you will positively consider our recommendations. We reiterate the necessity for more time to comprehensively assess the DSL's interaction with the broader regulatory framework of new and existing laws. It is critical that implementing regulations are finalized through transparent stakeholder consultation before the law comes into effect. We encourage the MPS to continue to engage in dialogue with the private sector, so as 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
Director, Policy – APAC