GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

November 2026

COMMENTS ON VIETNAM'S UPDATED DRAFT LAW ON DATA SECURITY

The Global Data Alliance (GDA) offers the following position paper on Vietnam's Draft Law on Data Security (DSL) dated September 28, 2026. The GDA is a cross-industry coalition of companies headquartered around the world that are committed to high standards of data responsibility and rely on the ability to transfer data across borders to innovate and create jobs. Members operate in sectors including the agriculture, aerospace, automotive, advanced manufacturing, finance, insurance, health, media, telecommunications, and transportation sectors. The GDA supports measures that strengthen data security without imposing unnecessary restrictions on trusted international data flows.

The GDA's recommendations focus on consistent, risk-based requirements; avoiding regulatory duplication; and ensuring that the DSL's treatment of private-sector data (such as health, financial and logistics data) does not inadvertently impede essential cross-border services, research, and innovation.

We recognize that the Ministry of Public Security (MPS) has made several important changes to this draft. The draft clarifies the respective roles of the DSL, Data Law, Personal Data Protection (PDP) Law, and Cybersecurity Law, and provides for recognition of assessments and a unified procedure where requirements overlap (Article 3).

The draft now also: (1) allows private sector entities to determine risk levels; (2) generally reserves advance reviews for higher-risk data, and (3) avoids additional DSL transfer procedures for Levels 1 and 2. At the same time, Level 3 transfers require self-assessment, while Levels 4 and 5 require approval that may cover recurring transfers for the same data flow (Articles 4, 8, 10, and 19). The draft also contains safeguards for confidential source code and AI model weights (Article 11.7) and permits voluntary use of security cryptography for non-state secret data (Article 16.3). The draft removes revenue-based fines, the rule against multiple sanctions for the same violation (Article 26.12), and the procedural protections and 90-day maximum for service restrictions under Article 20.

The GDA offers the following recommendations:

1. Clarify Relationship to Other Vietnamese Measures and Clarify Roles

The value of Article 3's streamlined procedures will depend on corresponding amendments to Decree 165, Decree 356, and other implementing instruments. Article 18.3(c) could otherwise require repeated cybersecurity reviews of the same shared cloud platform for different customers. Separate volume thresholds for sensitive personal data, large-scale processing, and Core Data (Articles 8.1(c), 14.1, and 8.3) could also produce inconsistent classifications. Accordingly, the relationship among these implementing instruments should be more fully clarified, as should the allocation of controller and processor responsibilities, which should better reflect who controls data and systems – a common feature of other economies' data governance frameworks (Article 18.2).

Recommendations:

- Align implementing instruments before the DSL takes effect;
- Publish a map of superseded and retained obligations;
- Recognize prior assessments, certifications, and relevant PDP impact-assessment content;
- Harmonize thresholds and incident reporting;
- Clarify that data administrators shall undertake classification and transfer decisions for the data and systems they control;
- Delete Article 8.6, which would require administrators to treat data not yet on the official Important or Core Data lists as if listed, notwithstanding the list-based classification regime and the authorities' powers to update it under Articles 8.7–8.9.

2. Avoid Excessively Broad Transfer Restrictions on Certain Types of Private Sector Data, including Health and Financial Data

Given impacts on the ability to transfer and share data for purposes of supporting governmental policy objectives relating to health and finance, the data classification provisions merit particular attention.

Under Article 8.1(c), sensitive personal data processed at or above a prescribed scale enters Level 3; under Article 8.3, Core Data identified solely by volume or number of data subjects is ordinarily treated as Level 3. However, biometric and genetic data are excluded from that special treatment. This exclusion does not independently make such data Core Data, but where such datasets are separately designated Core Data they could face Level 4 requirements. Financial records could likewise receive heightened treatment based on their volume or designation. These factors may justify proportionate safeguards, but do not by themselves establish that routine healthcare, research, banking, or insurance processing presents a national-security risk warranting Level 4 or 5 treatment.

Classification directly affects international transfers. While Article 19.3 provides no additional DSL procedure for Levels 1 and 2, it mandates self-assessment for Level 3 and prior appraisal and approval for Levels 4 and 5. (Article 19.5 prohibits transfers only of specified Level 5 data of special importance to national defense, national security, or territorial sovereignty.) Overly broad higher-risk designations, impractical approvals, or restrictions on remote access could produce comparable effects in practice.

More broadly, Vietnam could facilitate trusted data flows by replacing prescriptive cross-border transfer approvals with a risk-based safeguards framework similar to GDPR Article 46, under which transfers may proceed using enforceable contractual commitments, binding corporate rules, or approved certification and other accountability mechanisms. At a minimum, Article 19 should avoid duplicative Level 3 assessments where an organization has already completed a comparable transfer assessment under another recognized framework.

The practical effect of over-classification would not be limited to transfer procedures. Level 3 datasets carry inventory, impact-assessment, audit, and technical-control requirements under Article 10; Level 4 brings additional appraisal and oversight requirements. Such obligations may be justified for genuinely high-risk systems, but become inefficient when routine hospital administration, clinical research, payment processing, or insurance operations are captured solely by the number of records handled.[1]

Where data are adequately segmented, the classification of a high-risk element should not automatically attach to unrelated processing on a shared platform. Nor should derived models or research outputs be assigned elevated controls without regard to whether they can actually disclose or reconstruct protected source information.

Recommendations:

- Do not restrict data transfers of certain types of data (e.g., by indiscriminately classifying health data or financial data as Core Data / Levels 4–5 based on a sectoral presumption of sensitivity);
- Clarify that the biometric/genetic exception in Article 8.3 does not itself designate such data as Core Data;
- Recognize effective data partitioning (Articles 3.2(e) and 12.2), preserve Article 14.3 for ordinary business and operational data, and allow appropriately safeguarded derived research outputs to be assessed on their demonstrable disclosure or reconstruction risks (Article 15.4);

[1] Cross-border health data is essential to clinical trials, pharmacovigilance, medical-device monitoring, specialist consultation, and biomedical research. Financial data flows support payments, anti-fraud and financial-crime detection, insurance, enterprise risk management, and cybersecurity. These services often require continuous processing through regional or global systems, not just emergency transfers. Article 19.7's emergency exception is welcome but is not a substitute for routine transfer mechanisms. Article 18.4(d)'s remote-access restrictions should also be read consistently with the authorized professional-access framework in Articles 19.1(c) and 19.10.

Potentially affected activities include cross-border clinical-trial coordination, comparative diagnostics, regional disease surveillance, real-time payment screening, sanctions and anti-fraud checks, and centralized security monitoring. A transfer approval system that is uncertain in scope or requires fresh approval each time a dataset is updated could interrupt services that are continuous by design. Article 19.4 already permits an approval to remain valid for an approved flow until changes occur in purpose, data type, recipient, or protections. In implementation, this should cover recurrent, automated transfers under stable arrangements rather than demand a separate authorization for each exchange. Transfers permitted under the PDP Law should be integrated, not subjected to a duplicative substantive or filing process.

- Confirm that the DSL and its implementing rules impose no categorical localization or residency obligations for specific types of data;
- Publish narrow criteria and predictable timelines for Level 4/5 approvals;
- Permit approvals for recurring transfers to affiliates, processors, research partners, and financial networks where purpose, recipients, and safeguards are unchanged;
- Clarify when authorized overseas professional access may continue, subject to appropriate controls;
- Deem an existing, substantively equivalent GDPR transfer assessment, Global Cross-Border Privacy Rules (CBPR) assessment or certification, or ASEAN transfer assessment using recognized mechanisms (including the ASEAN Model Contractual Clauses) sufficient to satisfy the Level 3 self-assessment under Article 19, subject only to narrowly tailored supplementation for material risks not already addressed;
  As a preferred longer-term approach, replace the current restrictive transfer procedures with an accountability-based transfer framework modeled on GDPR Article 46, recognizing appropriate contractual, intra-group, and certification-based safeguards while retaining proportionate controls for demonstrably exceptional national-security risks.

3. Limit Extraterritorial Application to Activities Targeting Vietnam

Articles 1.2(c) and 2.3 should be clarified so that the DSL does not automatically extend to all data processing conducted abroad merely because a foreign entity is affiliated with a business operating in Vietnam. Overly expansive application could impose overlapping or conflicting compliance obligations on global corporate groups, including for information created, collected, and processed entirely outside Vietnam with no meaningful connection to the Vietnamese market.

Recommendations:

- Apply the DSL to foreign entities only to the extent their relevant activities intentionally target individuals or customers in Vietnam, or otherwise have a substantial, direct nexus to Vietnam, rather than relying solely on corporate affiliation or incidental accessibility from Vietnam;
- Expressly exclude personal data independently created and collected abroad by foreign affiliates in connection with their non-Vietnam operations, absent a qualifying Vietnam-directed activity or other substantial territorial nexus.

4. Clarify Decryption Safe Harbor

Article 19.1(b) helpfully excludes certain encrypted Levels 3 and 4 data stored abroad from the definition of transfer when the administrator manages the decryption keys in Vietnam and the overseas provider cannot access them. That optional safe harbor should not be interpreted to require local key storage for all lawful transfers.

The law should also distinguish an actual cross-border disclosure of protected content from legitimate technical operations. Foreign-based incident response, vendor support, encrypted backups, and international fraud monitoring may necessarily involve remote interfaces of decrypted data sets without surrendering control over sensitive data.

Recommendations:

- Permit customer-controlled encryption and secure managed-key arrangements regardless of the keys' physical location, consistent with the applicable protection requirements;
- Articles 18.4(d) and 19.10 should be clarified so that authorized access can proceed under appropriate logging, contractual restrictions, and security controls, while the most sensitive prohibited data remains subject to Article 19.5;
- The specific domestic key-control rules for Level 5 infrastructure in Article 13.1(đ) should not be extended by implication to lower-level commercial datasets.

5. Implementation Timeframe

The practical operation of the DSL will depend heavily on forthcoming decrees and guidance. We recommend public consultations of at least 60 days and issuance of implementing instruments well before obligations begin. Transition periods under Article 29 should run from publication of the relevant requirements, rather than from the law's effective date.

The GDA thanks the MPS and the Committee for considering these comments and remains available to share international, cross-sector experience and best practices. Should you have any questions, please feel to reach out to Joseph Whitlock (jwhitlock@bsa.org)