July 9, 2026

GLOBAL DATA ALLIANCE COMMENTS ON THE POLICY DOSSIER FOR THE DRAFT LAW ON DATA SECURITY

The Global Data Alliance (**GDA**)[1] thanks the Ministry of Public Security (**MPS**) for the opportunity to comment on the Policy Dossier for the draft Law on Data Security (**DSL**).

The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. The GDA supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine data security, cybersecurity, innovation, economic development, and international trade. Given the GDA's focus on cross-border data, we comment specifically on the cross-border data aspects of the Policy Dossier.

The GDA has provided comments on numerous Vietnamese proposed requirements to localize data or restrict data transfers over the years, including with respect to the Data Law, the Cybersecurity Law, and the Law on Personal Data Protection. Those comments can be found here.[2]

GDA member companies are significant investors in Vietnam, investing millions of dollars and supporting thousands of jobs. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output.

We hope these suggestions will assist the MPS as it develops the DSL. We hope to be a resource for the MPS as Vietnam continues to build a comprehensive and robust data governance framework that is interoperable with international best practices — especially in relation to cross-border data transfers — and that supports the growth of a vibrant and innovative digital economy.

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

[1] For more information on the Global Data Alliance, please see www.globaldataalliance.org

[2] *See* Global Data Alliance, GDA Comment to the Government of Vietnam (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-vietnam&sector=&language=&posts_filtered=1

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.
- 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.

GDA 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, feature availability, etc. 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.

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[3] affecting locally mandated data storage.

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

[3] 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

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.

Conclusion

The GDA appreciates the opportunity to provide these comments. The Policy Dossier for the DSL reflects several encouraging principles — including a risk-based approach to data classification, a commitment to

facilitating ordinary commercial data flows, and an acknowledgment of Vietnam's international trade commitments. The GDA urges Vietnam to implement these principles faithfully in the draft law and its implementing measures. Please do not hesitate to contact us with any questions regarding this submission.

Thank you for the opportunity to provide comments.

Sincerely,

Joseph P. Whitlock
Executive Director
Global Data Alliance
josephw@bsa.org