9 November 2026

Senior Lieutenant General Le Tan Toi
Chairman
Committee for National Defence, Security and Foreign Affairs
National Assembly of the Socialist Republic of Viet Nam
Hanoi, Viet Nam

RE: ***Comments of the Association for Competitive Technology to the Committee for National Defence, Security and Foreign Affairs of the National Assembly of Viet Nam re: Draft Law on Data Security***

Dear Chairman Le Tan Toi:

The Association for Competitive Technology (ACT) appreciates the opportunity to share its views on the revised draft Law on Data Security (Draft Law), which the Government presented to the National Assembly on 26 October 2026 and which the Committee has found eligible for consideration and adoption at the current session.[1]

I. Introduction and Statement of Interest

ACT is a not-for-profit trade association representing the global small business technology developer community. Our members build software, mobile apps, connected devices, and cloud-based services. They include developers based in Viet Nam and companies around the world that serve Vietnamese consumers and businesses. Small developers depend on secure and affordable cloud services, strong encryption, and the ability to move data across borders to reach their customers and compete with larger firms.

ACT supports Viet Nam's goal of protecting data that bears on national security and public order, and we recognize the real progress in the revised draft. We appreciate the Committee's support for an approach to cross-border data that focuses on security controls instead of requiring data to be stored in Viet Nam. Our comments aim to help the Draft Law meet its security goals without placing obligations on small developers that they cannot meet or that would cut them off from the services and customers they rely on. We hope they can inform the final text and, after enactment, the implementing decrees.

II. Coherence with Viet Nam's Existing Data Laws

Small developers rarely have dedicated compliance staff, so when data is subject to the Data Law, the Law on Personal Data Protection, the Cybersecurity Law, the Law on Artificial Intelligence, and

[1] Minister of Public Security Luong Tam Quang presented the Government's submission, and the Committee presented its verification report, at the National Assembly's plenary session on 26 October 2026. See "Hoàn thiện hệ thống pháp luật, tạo điều kiện phát triển kinh tế dữ liệu," Tạp chí Thị trường Tài chính Tiền tệ (26 October 2026) (in Vietnamese), https://thitruongtaichinhtiente.vn/hoan-thien-he-thong-phap-luat-tao-dieu-kien-phat-trien-kinh-te-du-lieu-86576.html.

the Draft Law, each with its own classification scheme, thresholds, and reporting cycle, the cost of compliance falls hardest on the smallest firms. We ask the Committee to make sure that the classification levels in the Draft Law map onto the categories in the Data Law, that a single impact assessment can satisfy each law where the same dataset is covered more than once, that assessments are prepared once and updated when circumstances change materially, as under Decree 165 and Decree 356, instead of being refiled each year, and that a business does not face separate storage or retention obligations for the same data under different laws.

The Draft Law should also follow the allocation of roles already set out in the Law on Personal Data Protection and the Data Law. Obligations that depend on knowing what the data is and why it is processed, such as classification, risk assessment, and transfer decisions, should rest with the data controller. A cloud or software provider acting as a data processor, which often has no visibility into its customers' data, should be responsible for the security measures within its actual control.

III. Risk-Based Data Classification

We ask that the higher risk levels, and Levels 4 and 5 in particular, be defined by objective criteria set out in the law or in a decree issued after public consultation. These levels should be limited to data whose compromise would directly affect national defence, national security, public order, or the operation of critical national infrastructure. Data should not move to a higher level only because a company in a particular sector, such as finance, health, or telecommunications, holds it, or because a dataset has reached a certain size. The customer records of a small health app or a payments startup should not attract the obligations intended for data with a direct bearing on national security. Published criteria would give the agencies that apply the law a consistent basis for their decisions and give businesses the certainty they need to invest.

IV. Cross-Border Transfers

We share the view of Vice Chairman Nguyen Hong Dien that cross-border transfer rules should take account of the risk of a particular transfer as well as the classification of the data.[2] The purpose of a transfer, the recipient, the scope of processing, the encryption used, and the ability to retrieve the data all bear on that risk. A transfer of encrypted data for technical processing, with restricted access and the ability to retrieve it, presents very different risks from a transfer of unencrypted data for long-term storage abroad. Routine activities such as payment processing, cloud hosting, software updates, customer support, and the operation of centralized systems should be able to proceed with only internal assessment and recordkeeping. We therefore ask the Committee to take the following steps:

1. Limit prior evaluation and approval to transfers of narrowly defined Level 4 and Level 5 data, with a fixed review period and a written decision that states its reasons.

[2] Remarks of Vice Chairman Nguyen Hong Dien at the sixth session of the National Assembly Standing Committee. See "Thiết lập khung pháp lý bảo vệ tài nguyên dữ liệu quốc gia từ sớm, từ xa," Đại biểu Nhân dân (27 September 2026) (in Vietnamese), https://daibieunhandan.vn/thiet-lap-khung-phap-ly-bao-ve-tai-nguyen-du-lieu-quoc-gia-tu-som-tu-xa-10431931.html.

2. Refrain from an outright prohibition on transferring privately held data. If a prohibition is retained for a narrow category of state-held defence and security data, the law should set out the criteria, procedure, and timeline for authorizing exceptions.
3. Recognize internationally accepted transfer mechanisms, including the ASEAN Model Contractual Clauses, the Global Cross-Border Privacy Rules system, the EU Standard Contractual Clauses, and certification to ISO/IEC 27001, as valid bases for transfer without additional approval or reporting requirements.
4. Remove any remaining requirement to store privately held data in Viet Nam, so that the law focuses on security outcomes. This approach would also be consistent with Viet Nam's commitments on cross-border data flows and the location of computing facilities.[3]

V. Decryption Keys and Encryption

We understand that the revised draft would restrict the transfer outside Viet Nam of decryption keys and cryptographic parameters associated with Level 4 and Level 5 data. Encryption is one of the most effective security tools available to small developers. Many of them rely on key management services offered by international cloud providers, or on encryption designed so that only the end user holds the keys. So that the restriction on keys does not become a data storage requirement by another route or weaken the security of services that Vietnamese users rely on, we ask that the final text take the following steps:

1. Apply the restriction only to keys that protect data classified at Level 4 or Level 5 under objective criteria.
2. State that the law does not require any provider to create, hold, retain, or disclose decryption keys it does not otherwise hold, or to redesign end-to-end or device-based encryption in which the keys remain with the user.
3. Allow organizations to meet the requirement through key management arrangements they control, including customer-managed keys and hardware security modules certified to internationally recognized standards, without requiring a particular location or provider.
4. Exclude any requirement for a mechanism that would allow a third party to decrypt data without the involvement of the key holder. Any such mechanism creates a weakness that criminals and hostile actors can also exploit and would make Vietnamese data less secure. Viet Nam has also committed not to require manufacturers or suppliers of commercial products that use cryptography to transfer or provide access to private keys as a de facto condition of market entry, by making it a condition of the manufacture, sale, distribution, import, or use of those products.[4]

[3] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), arts. 14.11 (Cross-Border Transfer of Information by Electronic Means) and 14.13 (Location of Computing Facilities).
[4] CPTPP, Annex 8-B, Section A (Information and Communication Technology Products that Use Cryptography), para. 3.

VI. Technical Measures and Due Process

We welcome the Committee's support for a 90-day limit on technical measures applied to cross-border services. For a small developer, even a temporary block can mean losing customers it may not win back. We therefore ask that the final text take the following steps:

1. Require a written decision stating the grounds for any technical measure, with notice and an opportunity to remedy the issue before the measure takes effect, except in a genuine emergency.
2. Direct any measure at the specific service and party responsible for the violation, and not at platforms, cloud infrastructure, or other developers whose services share that infrastructure.
3. Treat 90 days as a maximum and provide a means to seek review of the decision.

VII. Artificial Intelligence and Confidential Business Information

The August draft included obligations on providers of artificial intelligence services concerning training data, labelling, and explanations of algorithms. To the extent the final text retains these provisions, we ask that they be left to the Law on Artificial Intelligence and its implementing decrees, which already address these matters, so that developers do not face two sets of rules for the same activity. Any request from the authorities for information about an algorithm or a system should protect source code, model weights, training data sources, and other trade secrets from disclosure, because for many small developers this intellectual property is their most valuable asset.

VIII. Proportionate Implementation

Finally, we ask that the Committee support the following measures so that small firms can realistically comply:

1. Harmonize incident reporting timelines and thresholds across Vietnamese laws and with international practice, which generally allows 24 hours for an initial notification and 72 hours for a fuller report.
2. Calculate percentage-based fines on the revenue in Viet Nam of the entity that committed the violation, and not on global group turnover, and define the violations that attract such fines in the law itself.
3. Publish the implementing decrees, together with simplified assessment templates and guidance for small businesses, for public consultation of at least 60 days, and provide a transition period after the law takes effect on 1 July 2027 so that small businesses have time to adjust their systems and contracts.

IX. Conclusion

ACT thanks the Committee for considering these comments. We would welcome the opportunity to meet with the Committee or the Ministry of Public Security to discuss them, and to contribute to the development of objective criteria for Levels 4 and 5 and the implementing decrees.

Sincerely,



Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Global Policy Counsel

Association for Competitive Technology
1401 K St NW (Ste 501)
Washington, DC 20005
United States

cc: Tran Thanh Man, Chairman of the National Assembly
Nguyen Hong Dien, Vice Chairman of the National Assembly
Luong Tam Quang, Minister of Public Security