FRASERS
LAW COMPANY
Established 1994

Vietnam’s Draft Law on Data Security

Legal Update | September 2026

The Ministry of Public Security (***MPS***) has prepared a draft Law on Data Security (***Draft Law***), which establishes a new framework for protecting data throughout its life cycle. The Draft Law is proposed to be submitted to the National Assembly for consideration in October 2026 and to take effect on 1 December 2027. It remains subject to amendment during the legislative process.

Vietnam already has legislation governing data, personal data protection and cybersecurity. However, according to the MPS, the current framework does not comprehensively regulate the security of the underlying data itself, from its creation and storage through to its use, transmission and destruction, whether the data is at rest or in motion. The Draft Law is intended to address that perceived gap by creating a risk-based regime focused on the confidentiality, integrity, availability, authenticity and resilience of data.

The Draft Law is not limited to personal data. It applies to data generally and introduces extensive organisational, technical, reporting and approval requirements. Some of its most significant implications for businesses are considered below.

1. Scope of data regulation

The Draft Law applies to Vietnamese organisations and individuals, foreign organisations and individuals in Vietnam, and foreign entities that directly participate in or are connected with data-processing activities in Vietnam. The scope, which is intended to cover offshore entities involved in or connected with data-processing activities in Vietnam, may therefore capture foreign cloud providers, technology suppliers and outsourced processors that have no conventional establishment in Vietnam.

Personal-data processing remains subject to personal-data-protection legislation. However, security, technical and technological matters not specifically regulated under that legislation are governed by the Draft Law. Cybersecurity similarly remains subject to cybersecurity legislation, while the Draft Law regulates the data itself throughout its life cycle. Businesses may consequently need to comply concurrently with the Law on Data No. 60/2024/QH15 (***Law on Data***), the Law on Personal Data Protection No. 91/2025/QH15 (***Law on Personal Data Protection***), the Law on Cybersecurity No. 116/2025/QH15 (***Law on Cybersecurity***) and the proposed Draft Law.

However, the Draft Law also states that security measures should be proportionate and should not excessively obstruct lawful business activities, and that security grounds should not be misused to obstruct lawful data flows. The intended approach is risk-based rather than uniform. These principles are important, but their practical effect will depend on how the implementing regulations define the categories, thresholds and approval procedures.

2. Data classification

The Draft Law classifies data into four risk levels: Ordinary Data (Level 1), Internal Data (Level 2), Important Data (Level 3) and Core Data (Level 4). Important Data and Core Data are aligned with the corresponding concepts under the Law on Data, while Ordinary Data and Internal Data are two additional regulatory categories. Specifically:

(i) Ordinary data (Level 1) means open data or data relating to ordinary civil or commercial activities; if compromised, it poses only a low risk to the lawful rights and interests of organisations or individuals.

(ii) Internal data (Level 2) means data serving the internal management and operation of an agency, organisation, or enterprise, or trade secrets; if leaked, it would cause losses to the normal operations of the organisation or to the competitive environment.

(iii) Important data (Level 3) means data belonging to key sectors and fields, which, if leaked, misappropriated, or misdirected, would cause serious harm to national security, macroeconomic security, or the public interest.

(iv) Core data (Level 4) means data directly related to national defence, national security, digital sovereignty, and the nation's supreme strategic interests; if compromised, it would cause harm to the country.

The risk-based classification of data is not static. Data initially classified at a lower level may become subject to a higher level of protection if its accumulated volume reaches a prescribed threshold and changes the nature of the associated risk. Operators of information systems are required to implement automated systems to monitor accumulated data volumes. If a threshold is exceeded, the operator must upgrade its protections immediately and, for Important Data and Core Data, report the change to the centralised monitoring system of the MPS. The Government will prescribe the quantitative thresholds and reporting periods.

This classification system is intended to direct regulatory and technical resources towards higher-risk data, rather than applying uniform requirements to all data in a manner that could unnecessarily hinder ordinary social and economic activities. Clear quantitative thresholds will therefore be important if businesses are to implement the proposed automated classification and monitoring requirements effectively.

3. Data governance obligations

Data-governing entities are required to maintain regular data inventories identifying, among other matters, the type, owner, location, processing location and importance of the data. Important Data and Core Data must also be mapped to show data flows, access and connection points, related systems and third-party dependencies.

A data-security impact assessment is required before deploying a new data system, processing critical data, materially changing system architecture, transferring data outside the organisation's management scope or using new technology that may create data-security risks. Entities operating systems that process Important Data or Core Data must also conduct annual risk assessments and report the results to the MPS.

Micro, small and medium-sized enterprises that do not process data on a large scale or do not process Important Data or Core Data would be exempt from the specific life-cycle protection obligations. However, this is not expressed as a general exemption from the remainder of the Draft Law.

Businesses are also responsible for data security across their data supply chains, including cloud providers, artificial intelligence service providers, data centres, brokers and outsourced processors. Before entering into cooperation and annually thereafter, the business must assess each relevant third party's technical capacity and data-protection measures, potential security risks and vulnerabilities, and risk-mitigation and incident-response arrangements. Data may be shared, transferred or made accessible only after the parties enter into a Data Security Agreement or include mandatory data-confidentiality provisions in the formal services agreement. The agreement must include an immediate notification obligation, within no more than 24 hours, if a data-leakage incident occurs or is at risk of occurring, and the business has a right and obligation to conduct periodic or ad hoc audits of the third party, or require a valid independent audit report.

4. Enhanced requirements for Important Data and Core Data

The Draft Law imposes increasingly stringent requirements as the data level increases. In particular, with regard to Important Data:

(i) Important Data generally has to be stored and processed in information systems meeting at least Level 3 security standards;

(ii) agencies and organisations processing Important Data or higher-level data must establish a risk-governance system, designate responsible data-security personnel and establish a dedicated data-security unit;

(iii) the Important Data-governing entity must retain securely protected system logs for at least six months; and

(iv) information systems containing Important Data must implement multifactor authentication, least-privilege access controls and encryption of data both at rest and in transit.

The MPS may conduct remote monitoring and require processing to be suspended where a serious risk of leakage or loss is identified.

For Core Data, the data generally must be stored and processed in information systems meeting Level 4 or Level 5 security standards. Core Data relating to national security, defence or critical infrastructure must be physically isolated or specially segmented from the public Internet and may not be transferred abroad, except in special cases serving the supreme interests of the State as decided in writing by the Prime Minister.

Information systems, investment projects and technology-transfer projects involving Important Data or Core Data are subject to a security appraisal by the MPS before operation or approval. The appraisal document constitutes a mandatory basis in the dossier for the relevant investment or technology-transfer decision.

Businesses using foreign experts or partners on Important Data or Core Data projects must also conduct personnel security vetting, enter into confidentiality undertakings and apply independent technical isolation measures when such personnel access the relevant systems. A foreign organisation or individual that violates Vietnam's data-security laws may be barred from system access or deported. This is a new and practically significant requirement for multinational groups that rely on offshore or seconded technical staff.

For an information system that is also subject to information-system security-level appraisal under cybersecurity legislation, the data-security appraisal is conducted concurrently and integrated into a single dossier and appraisal process led by the MPS, resulting in a single written approval.

5. Governance of algorithms and artificial intelligence systems

The Draft Law introduces specific obligations for organisations and businesses that research, develop, operate or provide artificial intelligence services in Vietnam, particularly generative artificial intelligence. Such entities must establish processes to verify and cleanse training data to ensure it is lawfully sourced and does not infringe intellectual property rights, integrate digital labelling of AI-generated content, and build technical filters to prevent the dissemination of information that is false or harmful to national security, public order or social safety.

The MPS may require an AI service provider to explain the transparency of its algorithms and the source of its training data where the provider's system generates false information concerning Vietnam's sovereignty, history, borders, culture or politics. Providers must maintain a channel for receiving violation reports and must block content that directly infringes national security immediately upon the MPS's urgent request. Where an AI system commits a serious violation causing particularly severe consequences, the MPS may decide to suspend the service or apply technical measures to block that system.

This is a new and significant compliance layer for technology and AI businesses operating in Vietnam, extending beyond data-specific obligations into algorithm transparency and content governance.

6. Cross-border transfers

Cross-border transfers of Important Data and Core Data are already regulated under the Law on Data and its guiding regulations, including the requirement of a data-transfer impact assessment. The Draft Law introduces additional data-security controls for certain outbound transfers.

According to the Draft Law, the transfer of Important Data or Core Data abroad requires prior appraisal and written security approval from the MPS. A transfer is generally prohibited where the data has a direct and immediate impact on national defence, national security, social order and safety, finance and banking, energy, telecommunications or emergency management, unless the Government permits an exceptional case serving the supreme interests of the State.

Data constituting an enterprise's trade secrets may be transferred without prior appraisal if:

(i) the receiving jurisdiction is recognised by the MPS as providing an equivalent level of data protection;

(ii) the parties execute the standard data-protection contract issued by the MPS; or

(iii) the transferring entity holds a conformity certificate for cross-border data security.

However, the transferring organisation must prepare a data-security impact-assessment dossier, report annually to the MPS and remain subject to post-transfer inspection. The MPS may suspend the outbound data flow if it detects a breach of the relevant confidentiality commitment.

7. Data localisation

Data localisation requirements already exist under the Law on Cybersecurity for certain enterprises providing telecommunications, Internet or value-added services in cyberspace that collect, exploit, analyse or process certain categories of user data in Vietnam. The Draft Law introduces a separate localisation regime based on the classification and strategic significance of the data.

In particular, Core Data and Important Data of national strategic significance that have a direct and immediate impact on national defence, national security, social order and safety, finance and banking, energy, telecommunications or emergency management must be stored in a data centre located in Vietnam. If an international cloud system is used, a continuously updated, real-time backup copy must be maintained in Vietnam, and the data-governing entity must ensure that ultimate control rests with the competent Vietnamese state authority. Other Important Data is subject to periodic synchronisation, backup or recovery requirements proportionate to its risk.

The overseas storage of significant volumes of Vietnamese data, together with reliance on foreign cryptographic standards, is said to create difficulties for the Vietnamese authorities in investigating and retrieving data. The localisation requirement is intended to prevent Vietnam from losing access to data where such data is entirely dependent on foreign infrastructure, including during geopolitical disruption.

The centralised monitoring system referred to throughout the Draft Law is the National Data Security Governance Center (Trung tâm Quản trị an ninh dữ liệu quốc gia), to be established under the MPS as the supreme command and monitoring infrastructure for Vietnam's critical data infrastructure. Operators of Core Data systems must transmit security logs to the Center through one-way transmission devices, while operators of Important Data systems must connect and share security-alert information according to prescribed technical standards. Monitoring activity must preserve operational confidentiality, and intervention in, or extraction of, specific data content is restricted to national-security emergencies or criminal investigations authorised by law.

8. Incident reporting and penalties

The Draft Law imposes strict incident-reporting deadlines. An incident involving Core Data must be assessed and reported within two hours of detection. For other data, an initial notification is required within 24 hours. A full report is due within 72 hours of detection, followed by a post-incident assessment within 30 days after remediation. Affected data subjects must also be notified where their lawful rights and interests are infringed. The two-hour reporting deadline may, however, be difficult to meet in practice.

Particularly serious violations concerning Important Data or Core Data may attract fines of up to 5% of the organisation's revenue in Vietnam for the preceding financial year. For a member of a multinational group whose Vietnamese revenue is not commensurate with the scale and severity of the violation, the fine may be calculated by reference to the group's global revenue for the preceding financial year and may not exceed 5% of that global revenue. Organisations and individuals committing violations may be subject to criminal prosecution, depending on the nature and severity of the violation; if damage is caused, they must provide compensation in accordance with the law.

The Draft Law also looks ahead to long-term cryptographic resilience. Core Data and Important Data of national strategic significance, and data containing state secrets, must be protected with long-term security measures capable of withstanding the development of quantum computing and other emerging technologies. Operators of the relevant information systems must periodically assess their readiness and follow a roadmap to transition to quantum-resistant cryptography under guidance from the competent state authority. As a transitional measure, from 1 January 2035, all information systems of Communist Party and State agencies, the armed forces, and the finance and banking, energy, telecommunications and education sectors that store or process Core Data or Important Data must have completed data migration and moved entirely to certified quantum-resistant cryptographic solutions. This gives affected businesses, particularly in regulated sectors, a specific long-term technology-migration deadline to plan for.

9. Data trading, insurance and emergency powers

The Draft Law treats the processing, analysis, brokering, storage and destruction of data as a conditional business line subject to security and public-order licensing standards. Trading or selling Core Data or Important Data that has a direct and immediate impact on national defence, security, social order and safety, finance and banking, energy, telecommunications or emergency management is prohibited outright, other than in special cases permitted by the Government, and data brokers or marketplace operators must register their operations, verify the lawful provenance of the data traded and retain transaction records for inspection. The State recognises and protects lawful ownership and exploitation of data assets, and prohibits the misappropriation of data, trade secrets or attacks on business data infrastructure.

Businesses are encouraged, though not required, to purchase data-security risk insurance appropriate to the level of data they store or process, to mitigate financial losses arising from incidents; the Government will prescribe applicable limits, conditions and related tax incentives.

In a national-security emergency that directly threatens data sovereignty, the MPS or the Ministry of National Defence, within their respective mandates, may issue special coordination orders and apply emergency technical measures against businesses providing relevant infrastructure or network services, including the requisition of infrastructure, assets and personnel in accordance with the law on requisition of property. These are significant state-intervention powers that businesses providing critical digital infrastructure should factor into their risk assessments.

The Draft Law is intended to fill gaps in Vietnam's existing data-regulation framework, protect the lawful rights of organisations and individuals and create a more trusted digital environment. The regime is intended to be risk-based, people- and business-centred, and implemented with minimal additional administrative procedures. Whether these objectives are achieved will, however, depend substantially on the implementing regulations. A coordinated implementation framework will therefore be important to ensure that the Draft Law improves confidence in Vietnam's digital economy without imposing unnecessary burdens on legitimate business activities.

Authors

Duong Thi Mai Huong
Partner
huong.duong@frasersvn.com

Bui Tho Kien
Associate
kien.bui@frasersvn.com

Ho Chi Minh City

19th Floor, Deutsches Haus
33 Le Duan Boulevard
Sai Gon Ward
Ho Chi Minh City, Vietnam
T: +84 28 3824 2733

Hanoi

15th Floor, Pacific Place
83B Ly Thuong Kiet Street
Cua Nam Ward
Hanoi, Vietnam
T: +84 24 3946 1203

Website www.frasersvn.com
Email legalenquiries@frasersvn.com