Vietnam's New Personal Data Protection Regime: Required Compliance Actions in 2026

Alitium
Ho Chi Minh City
Level 5, L'Mak Signature Building
147 Hai Ba Trung
Xuan Hoa Ward (District 3)
Ho Chi Minh City, Vietnam

Hanoi
51 Phan Boi Chau
Cua Nam Ward (Hoan Kiem)
Hanoi, Vietnam

P: +84 (28) 3535 6460
E: vietnam@alitium.com

Contact
Phuong Vo
Managing Partner
phuong.vo@alitium.com

Phung Nguyen
Accounting & Tax Partner
phuong.nguyen@alitium.com

Matthew Lourey
Chairman
mlourey@alitium.com

Vietnam | Singapore | Malaysia

[21 July 2026]

Required Investor Actions for Compliance with Vietnam's 2026 Personal Data Protection Regime

Article Authors:
Tram Pham – Senior Associate,
Thuan Dao – Associate,
Diem Bui – Legal Assistant,

Personal data is no longer merely an operational asset in Vietnam. From 1 January 2026, it has become a board-level legal risk. The Personal Data Protection Law No. 91/2025/QH15 (the "PDP Law") and Decree No. 356/2025/ND-CP ("Decree 356") establish Vietnam's first statute-level personal data protection framework, replacing Decree No. 13/2023/ND-CP and introducing more prescriptive compliance obligations for businesses and investors.

The key point for investors is simple: Vietnam's new regime may apply even where a business is headquartered outside Vietnam, if it directly participates in or is involved in processing personal data of Vietnamese data subjects. For foreign-invested enterprises, regional headquarters, shared service centres, cloud-based platforms, HR systems and cross-border group reporting structures, personal data compliance should now be treated as part of investment, M&A, market-entry and post-closing risk management.

1. Vietnam's personal data rules have extraterritorial reach

The PDP Law and Decree 356 apply not only to Vietnamese entities, but also to foreign organizations operating in Vietnam and foreign organizations directly participating in or involved in the processing of personal data of Vietnamese data subjects, including:

- Vietnamese agencies, organizations, and individuals;
- Foreign agencies, organizations, and individuals operating in Vietnam; and
- Foreign agencies, organizations, and individuals that directly participate in or are

involved in the processing of personal data of Vietnamese citizens and persons of Vietnamese origin with undetermined nationality residing in Vietnam who have been issued identity cards (collectively "Vietnamese Data Subjects").

This means that an offshore platform, regional HR hub, parent company, cloud service provider, CRM provider or overseas shared service centre may fall within Vietnam's compliance perimeter if it processes personal data linked to Vietnamese data subjects.

Investor takeaway: Compliance should be assessed across the whole data processing chain, not only at the level of the Vietnamese subsidiary.

2. Data classification now drives compliance exposure

The framework distinguishes between **Basic Personal Data** and **Sensitive Personal Data,** with Sensitive Personal Data being subject to more stringent protection requirements.

- **Basic Personal Data**, which includes identifying and identification information commonly collected in civil transactions and business activities, such as full name, date of birth, telephone number, email address, personal identification number or passport number, residential address, digital account information, etc.
- **Sensitive Personal Data**, which includes information that may significantly affect an individual's privacy, such as data relating to private life, health, biometric data (e.g., fingerprints and facial recognition data), bank account details, payment card information, credit history, income and asset information, political opinions, social media usage, and other categories of sensitive personal data prescribed by law.

Processing Sensitive Personal Data triggers heightened expectations, including notification to data subjects of its sensitive nature and implementation of enhanced safeguards such as access controls, internal processing procedures, appropriate security measures and, where relevant, additional transfer protections such as encryption, anonymization and physical security measures.

Investor takeaway: A data inventory and classification exercise should be completed before closing a transaction, launching a platform, or migrating data overseas.

3. Compliance is no longer a back-office exercise

The PDP Law and Decree 356 introduce a more structured compliance architecture. Core obligations include obtaining valid consent where required, appointing a Data Protection Officer (**DPO**), preparing Data Protection Impact Assessment (**DPIA**) and Cross-border Transfer Impact Assessment (**CTIA**) dossiers where applicable, and complying with statutory breach notification timelines.

(i) Obtaining valid consent

As a rule, personal data may only be processed with the data subject's consent, unless a statutory exception applies. Consent must be voluntary, clear and verifiable, and businesses must retain sufficient evidence throughout the processing lifecycle. Consent also may be recorded through mechanisms such as recorded calls, emails, websites or mobile applications, provided that the business can provide evidence of the consent. Data subjects may also withdraw consent in accordance with the law, making consent management a continuing obligation rather than a one-off formality.

Businesses should review their consent collection methods to ensure that they satisfy the legal requirements for valid consent.

(ii) DPO appointment

Organizations must appoint a DPO, either internally or through an external service provider that meets minimum qualification and experience requirements. In detail;

For internal appointments, the appointee must satisfy the minimum qualification and experience requirements below:

- Hold at least a college-level degree;
- Have a minimum of two years' experience (from the time of graduation) in one or more of the following fields: legal affairs, information technology, cybersecurity, data security, risk management, compliance, human resources, or personnel administration; and

- Have completed training in personal data protection laws and professional skills relating to personal data protection.

Where a DPO is outsourced, the external service provider, whether an individual or an organization, must satisfy certain qualification and competency requirements.

- An individual service provider must hold at least a college degree, have at least three years of relevant professional experience, and have completed specialized training in personal data protection.
- An organizational service provider must employ at least three qualified personnel meeting those requirements and have relevant experience in information technology, cybersecurity, information security, or personal data protection advisory services.

For SMEs, start-ups and newly established FDIs, this may be a practical bottleneck given the limited pool of qualified personal data protection professionals. DPO readiness should be included in post-investment integration and compliance budgeting.

(iii) DPIA and CTIA dossiers

- **CTIA**: Organizations engaging in cross-border transfers of personal data, including transfers to overseas systems or recipients and the use of overseas platforms to process personal data collected in Vietnam, may be required to prepare a CTIA.
- **DPIA**: Data controllers and controller-processors are required to prepare and maintain a DPIA from the commencement of their personal data processing activities. DPIA and CTIA dossiers must be updated when material changes occur, and certain changes must be reported and reflected within prescribed timelines.

Both the CTIA and DPIA must be updated within six months following their initial submission whenever there are material changes to the contents of such dossiers, including changes in data processing purposes or changes to the relevant data controller, data processor, controller-cum-processor, or third party. In addition, certain changes must be reported and reflected in the dossiers within 10 days, including the reorganization, dissolution, termination of operations, or bankruptcy of the relevant organization; changes to the personal data protection service provider; and changes to registered business lines or services relating to personal data processing that were previously registered in the DPIA or CTIA dossier.

Data flow mapping, server location review, intra-group transfer assessment and vendor contract review should be completed before transferring personal data overseas or integrating Vietnam operations into regional platforms.

(iv) Breach notification

Breach notification. A qualifying personal data breach may trigger notification to the Ministry of Public Security and related data subjects within 72 hours of awareness.

- **Notification to the Ministry of Public Security ("MPS")**: Where a data controller, controller-processor, or third party discovers a violation of the personal data protection regulations that may adversely affect national defence, national security, social order and safety, or infringe upon the life, health, honour, dignity, property, or other lawful rights and interests of data subjects, it must notify the MPS within 72 hours. Where such a violation is discovered by a data processor, the data processor must promptly notify the relevant data controller or controller-processor.
- **Notification to affected data subjects:** Where the breach involves location data or biometric data, the data controller or controller-processor must also notify the affected data subjects within the same 72-hour period, in addition to notifying the MPS.
  Records relating to the breach and remedial measures must be retained for at least five years following completion of the remediation process. Incident response procedures should be tested before a breach occurs. A 72-hour reporting window leaves little room for ad hoc decision-making.

Please note that household businesses and micro-enterprises are exempt from the DPIA, CTIA and DPO requirements, while small enterprises and start-ups may defer compliance with these requirements for five years from the effective date of the PDP Law. However, this relief does not apply to entities that provide personal data processing services, directly process sensitive personal data, or process personal data of 100,000 or more data subjects. Investors should therefore verify whether a target company qualifies for transitional relief before relying on the exemption or deferral.

What Should Investors do Now?

For foreign investors and companies operating cross-border data models, the priority is not to wait for enforcement. The immediate focus should be to identify exposure, close documentation gaps and build a defensible compliance trail:

- **Map data flows:** Identify what personal data is collected, where it is stored, who can access it, and whether it is transferred outside Vietnam.
- **Classify data correctly:** Distinguish Basic Personal Data from Sensitive Personal Data and apply the corresponding safeguards:
  - **Review consent mechanisms**: Ensure consent is voluntary, specific, verifiable and properly retained.
  - **Assess DPIA and CTIA requirements:** Determine whether impact assessment dossiers are required and whether cross-border transfer exemptions are genuinely available.
  - **Prepare governance documents:** Update privacy notices, internal policies, vendor contracts, intra-group data sharing arrangements and incident response procedures.

Investors should incorporate personal data protection into legal due diligence, transaction documentation, post-closing integration and ongoing corporate governance. Businesses already operating in Vietnam should conduct a gap assessment now, rather than waiting for a breach, an inspection or a cross-border transfer to expose compliance gaps.

Issues to Watch For

(i) **DPO qualification standards:** Further guidance may be needed on recognised training, certifications, accreditation bodies and assessment criteria.
(ii) **Controller and processor roles:** Complex SaaS, cloud, platform, IT outsourcing and intra-group arrangements may require careful role allocation.
(iii) **Cross-border transfer exemptions:** The practical application of exemptions for cloud services, HR management and intra-group transfers should be monitored closely.
(iv) **Extraterritorial enforcement**: Enforcement against overseas entities without a Vietnam presence remains an evolving area.

Businesses should continue monitoring future guidance and enforcement developments as Vietnam's personal data protection regime evolves.

Vietnam's PDP Law and Decree 356 mark a clear shift from general data management to legally accountable data governance. For investors, the message is direct: personal data compliance is now a transaction risk, an operational risk and a reputational risk. The companies that act early, by mapping data, documenting lawful processing, tightening cross-border transfers and preparing incident response protocols, will be better positioned to protect value in Vietnam's digital economy.

For any further questions you may have, please reach out to us at vietnam@alitium.com

****

his article is intended to provide an overview of recent updates and announcements. While it aims to present useful insights, it is important to note that the content shared here should not be considered as formal legal or compliance advice. For specific guidance on compliance obligations or legal matters related to your business, we strongly recommend consulting with a qualified professional, such as a qualified professional advisor or legal expert or directly reach out to us.