Atsumi & Sakai Newsletter
JAPAN
NEW YORK
LONDON
FRANKFURT
BRUSSELS
HO CHI MINH

April 2026
No.VNM_048

Key Points of the New Personal Data Protection Regime in Vietnam

1. Introduction

Vietnam's personal data protection framework has reached a major turning point with the enactment of the Law on Personal Data Protection (No.91/2025/QH15, hereinafter referred to as the "New Law") on June 26, 2025, and Decree No.356/2025/ND-CP (hereinafter referred to as the "New Decree") on December 31 of the same year. Both the New Law and the New Decree came into effect on January 1, 2026. At the same time, Decree No.13/2023/ND-CP (hereinafter referred to as the "Former Decree"), which had established the basic framework for personal data protection in Vietnam, expired.

The Former Decree played an important role as Vietnam's first direct comprehensive regulation on personal data protection. However, in practice, some of its provisions were considered ambiguous and difficult to interpret. By elevating personal data protection to the level of law enacted by the National Assembly, the new legislation is expected to enhance the clarity and effectiveness of the regulatory framework, while also ensuring consistency with the Data Law (No. 60/2024/QH15), which came into effect on July 1, 2025[1].

Against this background, this paper introduces the new personal data protection framework, focusing on its key features and practical implications.

2. Limitation of applicability

(1) Scope of extraterritorial application and subjects of application

The New Law introduces certain changes to the scope of extraterritorial application compared with the Former Decree.

Under the Former Decree, the scope of application included "Foreign agencies, organizations and individuals directly engaged or involved in personal data processing activities in Vietnam," which was interpreted broadly to cover the processing of personal data of individuals in Vietnam, including foreign nationals (Article 1.2(d) of the Former Decree).

In contrast, the New Law revises this provision to apply to "Foreign agencies, organizations and individuals directly involved in or related to the processing of personal data of Vietnamese citizens and people of Vietnamese origin whose nationality remains unidentifiable and who are living in Vietnam and have been issued identity certificates" (Article 1.2(c) of the New Law).

[1] One of the key drivers behind this legislation has been the increasing number of large-scale personal data breach incidents that have recently emerged in Vietnam. For example, Vietnamese authorities announced that, in the first half of 2025 alone, they uncovered 56 cases of illegal data trading involving more than 110 million records, highlighting the growing social problem of the sale and illicit circulation of personal data (https://bocongan.gov.vn/bai-viet/bao-ve-du-lieu-ca-nhan-quyen-va-trach-nhiem-trong-ky-nguyen-so-1767197198). Against this backdrop, the need for the state to strengthen the protection of citizens' rights has become increasingly evident.

Accordingly, for example, a foreign company located abroad that collects and processes only the personal data of foreign nationals stationed in Vietnam, and does not process personal data falling within the scope of the New Law, would not be subject to Vietnam's personal data protection regime.

(2) Definition of personal data

Like the Former Decree, the New Law classifies personal data subject to regulation into two categories: "Basic Personal Data"[2] and "Sensitive Personal Data"[3] (Article 2.2 and 2.3 of the New Law). These categories are further defined in detail in Articles 3 and 4 of the New Decree.

In addition, the New Law goes one step further than the Former Decree by expressly providing that properly de-identified personal data is excluded from the scope of the Law (Article 2.1 of the New Law)[4].

(3) Exempted entities

Under Article 38.2 and 38.3 of the New Law and Article 41 of the New Decree, certain entities are granted exemptions or transitional relief from specific obligations under the personal data protection regime.

In particular, business households, micro-enterprises, small-sized enterprises, and startups (excluding entities that provide personal data processing services, directly process sensitive personal data, or process personal data of 100,000 individuals or more in total) are exempted from the obligation to prepare and submit/update a Data Protection Impact Assessment dossier (Articles 21 and 22 of the New Law) and to appoint a Personal Data Protection Officer (Article 33.2 of the New Law), or are granted a five-year deferral.

Specifically, business households and micro-enterprises are fully exempted, while small-sized enterprises and startups are entitled to choose whether or not to comply within five years from the date when the New Law comes into effect. The New Law has increased the exemption period to 5 years, compared to the 2-year exemption period stipulated in the Former Decree.

However, the New Law and the New Decree do not define directly the criteria for determining whether a business qualifies as a business household, micro-enterprise, or small-sized enterprise, thus, the criteria for identifying these entities will be based on Decree 80/2021/ND-CP. In addition, definition of startups will be based on the Law on Support for Small and Medium-sized Enterprises.

3. Main Obligations

(1) Consent of personal data subject

In principle, personal data processing must be based on the explicit and voluntary consent of the personal data subject (Article 9 of the New Law). Companies are required to clearly notify the type of personal data to be processed, the purposes of processing, the personal data controller or the personal data controlling and processing party, and the rights and obligations of the personal data subject, obtain consent in a lawful manner, and establish mechanisms to demonstrate that such consent has been obtained.

In particular, Article 9.4 of the New Law requires that the consent of the personal data subject be obtained separately for each purpose of personal data processing. Accordingly, companies that collect

[2] Basic personal data means personal data reflecting common personal and background factors, which is frequently used in transactions and social relations and is on the list issued by the Government (Article 2.2 of the New Law).

[3] Sensitive personal data means personal data associated with the privacy of individuals which, when infringed upon, will directly affect lawful rights and interests of agencies, organizations and individuals, and is on the list issued by the Government (Article 2.3 of the New Law).

[4] Under the New Law, "de-identification of personal data" is defined as the process of changing or deleting information to create new data that cannot identify or cannot help identify a specific person (Article 2.11 of the New Law), and the process must ensure irreversibility. Accordingly, it should be noted that if the modification or deletion of information is insufficient, the resulting data may fall outside the scope of this provision.

personal data for multiple purposes must implement systems—such as through their privacy policies or related documents—to obtain consent for each purpose individually.

However, the New Law provides certain exceptions to the consent requirement. In the following cases, the consent of the personal data subject is not required (Article 19.1 of the New Law):

- To protect the life, health, honor, dignity, and lawful rights and interests of the personal data subject or other persons in urgent cases; to protect legitimate rights or interests of oneself or others or the interests of the State, agencies and organizations, when necessary, against acts of infringement of the above-mentioned interests. In this case, the burden of proof rests with the personal data controller, the personal data processor, the personal data controlling and processing party, and a third party;
- To resolve a state of emergency or a threat to national security which does not reach the extent of declaration of a state of emergency; to prevent and combat riots, terrorism, crimes and violations of law;
- To serve operation of state agencies and state management activities in accordance with law;
- To implement the agreement between personal data subjects and related agencies, organizations and individuals in accordance with law;
- Other cases as prescribed by law.

Among these exceptions, the provision allowing processing "To implement an agreement between personal data subjects and related agencies, organizations and individuals in accordance with law" (Article 19.1(d) of the New Law) may appear similar to the provision under the EU General Data Protection Regulation (GDPR) that permits the processing of personal data without the personal data subject's consent where it is necessary for the performance of a contract (Article 6.1(b)).

However, no implementing regulations or official guidance have yet been issued to clarify the scope of this exception under the New Law. Moreover, as noted above, the legislative background of the New Law emphasizes the establishment of a stricter consent mechanism, including the requirement to obtain separate consent for each processing purpose. In light of this context, the concept of "implement the agreement" is likely to be interpreted narrowly.

(2) Submission of various evaluation reports

(a) Data Protection Impact Assessment (DPIA) dossier

Personal data controllers and personal data controlling and processing parties are required to prepare a Data Protection Impact Assessment (DPIA) dossier from the commencement of personal data processing activities (the first day of conducting personal data processing) and submit it to the relevant department of the Ministry of Public Security within 60 days from the start of such processing activities (Article 21.1 of the New Law).

The New Law further requires that the DPIA dossier be updated whenever there are changes to its contents, and at least once every six months (Article 22.1 of the New Law). In addition, in the event of reorganization, dissolution, bankruptcy, or similar circumstances, the dossier must be promptly updated within 10 days (Article 22.2 of the New Law and Article 20.2 of the New Decree).

However, where an organization falls within the category of business households, micro-enterprises, small-sized enterprises, or startups, exemptions from the obligation to prepare and submit a DPIA dossier may be granted, either temporarily or permanently, subject to the conditions described in Section 2(3) above.

(b) Cross-Border Transfer Impact Assessment (CTIA) dossier

Like the Former Decree, the New Law requires the preparation and submission of a Cross-Border Transfer Impact Assessment (CTIA) dossier where personal data stored in Vietnam is transferred outside the country (Article 20 of the New Law).

The transferring entity must complete the CTIA dossier within 60 days from the commencement of the cross-border transfer and submit it to the relevant department of the Ministry of Public Security (Article

20.2 of the New Law). In addition, where there are material changes to the contents of the CTIA dossier, it must be amended and updated in a manner similar to the procedures applicable to the Data Protection Impact Assessment (DPIA) (Article 22 of the New Law).

However, the New Law and the New Decree provide exemptions from the obligation to submit a CTIA dossier in the following cases (Article 20.6 of the New Law and Article 17.3 of the New Decree):

- Cross-border transfer of personal data by competent state agencies;
- Agencies and organizations storing personal data of their employees with the use of cloud computing services;
- The personal data subject transferring his/her personal data across the border;
- Other cases as prescribed by the Government;
- Journalistic and communication activities conducted in accordance with the law;
- Cross-border transfer of personal data that has been publicly disclosed in accordance with the law;
- Emergency situations in which it is genuinely necessary to provide personal data across borders to protect the life, health, and property safety of an individual; or to perform duties and obligations as prescribed by law;
- Cross-border transfer of personal data for cross-border human resources management in accordance with labor rules, internal labor regulations, and collective labor agreements as prescribed by law;
- Provision of personal data across borders for the purpose of entering into contracts or carrying out procedures related to cross-border transportation, logistics, remittance, payment, hotel services, visa applications, or scholarship applications.

Accordingly, the New Law and the New Decree adopt a framework that provides practical exemptions for cross-border data transfers that are unavoidable in business practice or necessary from a social perspective.

(3) Appointment of Personal Data Protection Officer

Under the Former Decree, only entities that processed sensitive personal data were required to designate a personal data protection department and a responsible officer, and to notify the relevant department of the Ministry of Public Security (Article 28.2 of the Former Decree).

In contrast, the New Law requires companies—regardless of whether they process sensitive personal data—to either establish an internal personal data protection department and designate a responsible officer, or engage an external specialized service provider (Article 33.2 of the New Law). Where the function is outsourced to an external specialized agency, the arrangement must be formalized in a written contract, and information regarding the external agency must be disclosed to the personal data subject (Article 16.3 of the New Decree).

However, where an organization qualifies as a business households, micro-enterprises, small-sized enterprises, or startups, exemptions from the obligation to appoint a personal data protection officer may be granted either temporarily or permanently, subject to the conditions described in Section 2(3) above.

4. Penalties

The New Law provides for significant administrative penalties. In particular, violations relating to the cross-border transfer of personal data may be subject to fines of up to 5% of the entity's turnover in the preceding year. In cases where there is no revenue from the immediately preceding year, or the penalty calculated based on revenue is lower than the maximum fine, the maximum penalty for this offense is VND 3 billion for organizations and VND 1.5 billion for individuals.

In addition, for violations involving the sale or purchase of personal data, a penalty of up to ten times the amount of the unlawful gain may be imposed. In cases where there is no revenue generated from the violation, or the fine calculated based on the revenue generated from the violation is lower than the maximum fine, the maximum fine for this violation is VND 3 billion for organizations and VND 1.5 billion for individuals.

For other violations of personal data protection regulations, administrative fines of up to VND 3 billion may be imposed (Article 8 of the New Law).

5. Conclusion

The New Law and the New Decree have significantly strengthened the effectiveness of Vietnam's personal data protection regime by introducing clearer obligations, penalties, and exemptions. Given that the enforcement framework has been substantially reinforced, it would be risky to assume that the regulations will not be actively enforced in practice. Companies should conduct compliance assessments of their operations with current personal data protection regulations. If a DPIA or CTIA report is required, such filings should be completed in a timely manner, particularly in view of the significant penalties for non-compliance. Furthermore, companies should quickly review, issue new, or amend internal regulations or specific procedures on personal data protection, such as labor regulations, employment contracts, privacy policies, and confidentiality commitments.

Authors

Katsunori Irie
Partner
E: katsunori.irie@aplaw.jp

Taisuke Oikawa
Associate
E: taisuke.oikawa@aplaw.jp

Thi Phong Lan Nguyen*
Of Counsel
*Not Registered as a Foreign Lawyer in Japan
E: lan.nguyen@aplaw.jp

Contacts

E-mail: ipg_vietnam@aplaw.jp

If you would like to sign up for A&S Newsletters, please fill out the sign-up form.
Back issues of our newsletters are available here.

Related Articles

Vietnam Legal Update on LinkedIn:
[Legal Update] Vietnam's Evolving Commercial Landscape: Insights from the Draft Decree on Foreign Trading Activities

---

We are the only independent Japanese law firm with affiliated offices located in New York, London, Frankfurt, Brussels and Ho Chi Minh City which, together with our Tokyo office, Osaka affiliated office and Fukuoka affiliated office, enables us to provide real-time advice on Japanese law to our clients globally.

Atsumi & Sakai

www.aplawjapan.com/en/

Tokyo Head Office
Fukoku Seimei Bldg. (Reception: 16F)
2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011 Japan

Osaka Affiliate Office
Nakanoshima Festival Tower 16F,
2-3-18 Nakanoshima, Kita-ku, Osaka City, Osaka 530-0005 Japan

Fukuoka Affiliate Office
Tenjin Bldg. 10F
2-12-1 Tenjin, Chuo-ku, Fukuoka-shi, Fukuoka 810-0001 Japan

New York Affiliate Office
1120 Avenue of the Americas, 4th Floor, New York, New York 10036

London Office
85 Gresham Street, London EC2V 7NQ, United Kingdom

Frankfurt Affiliate Office
Barckhausstraße 1 (8th Floor), 60325 Frankfurt am Main, Germany

Brussels Office
CBR Building
Chaussée de la Hulpe 185, 1170, Brussels, Belgium

Ho Chi Minh Office
10F, The NEXUS building
3A-3B Ton Duc Thang Street,
Sai Gon Ward, Ho Chi Minh City, Vietnam