

[Vietnam] Draft Law on Personal Data Protection

– Major upgrades of the current legislation on personal data protection that could potentially increase compliance costs –

Asia & Data Protection Newsletter

September 27, 2024

Author:

[Tomonobu Murata](mailto:to.murata@nishimura.com)
to.murata@nishimura.com

[Nguyen Tuan Anh](mailto:n.t.anh@nishimura.com)
n.t.anh@nishimura.com

1. Introduction

On September 24, 2024, more than six months after the Ministry of Public Security of Vietnam (“**MPS**”) publicly announced its proposal to draft a law on personal data protection (“**PDPL**”) in late February 2024, the Government of Vietnam disclosed the full text of the draft PDPL on its official portal. The draft will be open for public opinion until the end of November. The PDPL is expected to be adopted by the National Assembly of Vietnam during the first half of 2025 and to take effect on January 1, 2026.

At a glance, the draft PDPL is comprised of 68 articles, which are based significantly on the current legislation, specifically, Decree No. 13/2023/ND-CP (“**PDPD**”), with some modifications and numerous additions. This newsletter highlights key takeaways from the draft PDPL, to provide a snapshot of the latest updates to privacy law in Vietnam.

2. Key takeaways

- (1) Major modifications. The drafter (i.e., MPS) generally respects the spirit of the PDPD, but made some modifications, including:
- Expanding the scope of governed subjects to include entities and individuals that collect and process the personal data of foreigners in the territory of Vietnam. The draft PDPL does not clarify the current scope of governed subjects, and introduces another type that might cause further ambiguity.
 - Modifying key definitions of “basic personal data,” “sensitive personal data,” and “outbound transfer of personal data.” Along with the modification of “outbound transfer of personal data,” the draft PDPL adds more specific situations that fall within this definition. This might include subsequent outbound transfers of personal data between offshore entities and individuals.
 - Revising the principles for data protection by clarifying the independence of group companies for purposes of compliance with personal data protection regulations. Consent granted to one entity does not empower other companies within the same group to process personal data without further consent.
 - Enhancing the conditions for valid consent. Notably, the draft DPDL still contains a heavily consent-oriented approach, and continues to include the same non-consent based cases in the PDPD. It means that it does not include “legitimate interest” as one of lawful bases for data processing.
 - Clarifying the requirements for collection of personal data via CCTV in public places. The draft PDPL seems to expand the scope of applicability of these requirements, to enable normal entities to process data collected via CCTV without consent.
 - Improving the requirements for personal data protection in marketing and advertising. The draft DPDL

includes two separate sets of requirements for data protection in marketing and behavioral and targeted advertising, with some supplemental obligations (e.g., compliance with anti-spam regulations, immediate opt-outs, and prohibitions on outsourcing/subcontracting).

- Revising the components of the personal data processing impact assessment (“**DPIA**”) dossier, notably by requiring that a credit rating document for personal data protection be provided as a supporting document.
- Clarifying the frequency of updates to approved DPIA dossiers and outbound transfer impact assessment dossiers. The draft DPDL requires that these two dossiers be updated every six months in the event of changes, and immediately in some specified situations (e.g., corporate restructuring, change to nature of business).
- Imposing more protection requirements on the processing of basic and sensitive personal data. Appointment of a data protection entity (“**DPE**”) and a data protection officer (“**DPO**”) is now compulsory regardless of the sensitivity of data to be processed, and a data protection credit rating now also is required in the event of processing sensitive personal data.

(2) Notable additions. While retaining a significant number of regulations from the PDPD (with certain modifications), the draft DPDL introduces new concepts and regulations aimed at creating a more stringent set of rules. Some of the most noteworthy include:

- Introducing many new definitions, such as “developers,” “DPE,” “DPO,” “DPE service,” “DPO service,” “service of personal data protection qualification certification service,” “credit rating for personal data protection,” “credit rating organizations,” “data processing service,” and “personal data non-compliance.” Notably, the definition of “personal data non-compliance” is unexpectedly broad, and burdens businesses with data breach notification obligations.
- Providing specific requirements for personal data protection in specific areas and services (such as big data, Artificial Intelligence (AI), cloud computing, recruitment and employee monitoring, banking and finance, social networking services (SNS), and OTT services), and for special categories of data (such as health, insurance, location, and biometric data).
- Adding detailed requirements and qualifications for provision of DPE/DPO services, DPE/DPO certification services, credit rating services, and data processing services. One of the requirements is to obtain a certificate or approval (which is valid for 5 years) from the MPS (A05) or a designated entity to be eligible to provide those services.
- Including a credit rating mechanism, to be conducted by licensed rating entities, containing four levels (high credibility, credibility, pass, and fail).

3. Conclusion

The draft PDPL currently is in a preliminary stage, and is expected to undergo significant changes after the public consultation process, due to vagueness, incompleteness, and inconsistencies across various articles. Our initial impression is that the draft PDPL does not adequately address existing concerns stemming from the enactment and implementation of current legislation. Instead, it introduces more stringent regulations, which could lead to increased compliance costs for enterprises. These costs may include retaining qualified DPEs and DPOs, obtaining credit ratings for personal data protection, and modifying current data processing systems and contracts to meet the new, stringent requirements. Given the law’s importance and its considerable impact on the majority of businesses involved in personal data processing, it is crucial for all businesses to stay vigilant

and prepared for potential changes arising from developments in the draft PDPL.

Please feel free to reach out to us, should you want to know more about the draft PDPL or related topics.

In order to respond to the business needs of our clients, we publish newsletters on a variety of timely topics. Back numbers can be found [here](#). If you would like to subscribe to the N&A Newsletter, please fill out [the N&A Newsletter subscription form](#).

This newsletter is the product of its authors and does not reflect the views or opinion of Nishimura & Asahi. In addition, this newsletter is not intended to create an attorney-client relationship or to be legal advice and should not be considered to be a substitute for legal advice. Individual legal and factual circumstances should be taken into consideration in consultation with professional counsel prior to taking any action related to the subject matter of this newsletter.

Public Relations Section, Nishimura & Asahi newsletter@nishimura.com