LEGAL UPDATE
April 2025

ON THE NEW DRAFT LAW ON PERSONAL DATA PROTECTION

KEY TAKEAWAYS

- The Vietnamese government is currently drafting a new Law on Personal Data Protection, which represents a significant step forward by establishing a higher legal framework compared to the Government's Decree No. 13/2023/ND-CP. The Draft Law is scheduled to be debated and ratified at the upcoming National Assembly session in May 2025, and will take effect on 1 January 2026.

- The Draft Law introduces more detailed and specific regulations across various aspects of personal data protection, including the requirement for establishment or hiring of Personal Data Protection Organization and Personal Data Protection Expert, regulations for employees' information, AI systems, cloud computing, and social networks, etc.

- However, certain provisions in the Draft Law may require further clarification through implementing regulations.

OVERVIEW

The Vietnamese government is currently drafting a new Law on Personal Data Protection ("**Draft Law**"). The Draft Law on personal data protection represents a significant step forward by establishing a higher legal framework and introducing more detailed and specific regulations across various aspects of personal data protection compared to the Government's Decree No. 13/2023/ND-CP dated 17 April 2023 ("**Decree 13**"). We discuss below the key changes in the Draft Law (version dated 10 March 2025) compared to Decree 13.

KEY CHANGES

DEFINITIONS

The Draft Law provides some new or modified definitions. Notably, the Draft Law:

(a) Defines "the right to personal data protection" as the right of the data subjects to perform or demand others to respect and protect their data. This right is not explicitly defined in Decree 13;

(b) Defines "Personal Data Protection Organization" as an organization certified by the Personal Data Protection Authority[1] and designated by the Controller, the Controller and Processor, the Third Party, the Party Transferring Personal Data Abroad, and the Party Receiving Personal Data of Vietnamese citizens. Enterprises in Vietnam in collecting, processing and/or transferring data are required to set up this organization within their own enterprises or hire a professional provider engaging in the Personal Data Protection Service

[1] It is likely the Department of Cyber Security and High-Tech Crime Prevention (A05) under the Ministry of Public Security.

Business as defined below;

(c) Defines "Personal Data Processing Services" are conditional business lines for enterprises that provide personal data processing solutions on behalf of the Personal Data Controller, Personal Data Controller and Processor;

(d) Defines "Personal Data Protection Service Business" as the provision of services by organizations and enterprises with sufficient capacity (legal and technology) to protect personal data to meet the needs of the Controller, the Controller and Processor, the Third Party, the Party Transferring Personal Data Abroad, and the Party Receiving Personal Data of Vietnamese citizens;

(e) Defines "Personal Data Protection Expert" as a person appointed by the Controller, the Controller and Processor, the Third Party, the Party Transferring Personal Data Abroad, the Party Receiving Personal Data of Vietnamese Citizens with sufficient capacity (legal and technology) to protect personal data. Enterprises in Vietnam in collecting, processing and/or transferring data are required to have their own Personal Data Protection Expert(s) or hire those experts from an enterprise which engages in the Personal Data Protection Expert Service Business as defined below;

(f) Defines "Personal Data Protection Expert Service Business" as the provision of services by organizations, enterprises, and individuals with technological and legal capacity to protect personal data to meet the needs of the Controller, the Controller and Processor, the Third Party, the Party Transferring Personal Data Abroad, the Party Receiving Personal Data of Vietnamese Citizens; and

(g) Defines "Organization Certifying the Capacity to Protect Personal Data" as an organization certified by the Personal Data Protection Authority and capable of training and granting certificates of capacity to Personal Data Protection Experts.

DATA PROCESSING WITHOUT CONSENT

Both Decree 13 and the Draft Law outline exceptions where consent of a data subject is not required. However, the Draft Law adds an article on the mechanism for supervising the processing of personal data in such case. More specifically, under this article relevant agencies, organizations and individuals need to establish a monitoring mechanism when processing personal data in cases where the consent of the data subject is not required, including:

(a) Establishing clear and transparent personal data protection procedures and policies;

(b) Fully applying personal data protection measures; Implementing regulations on reporting and handling when violations of personal data protection regulations occur; Establishing a multi-dimensional monitoring mechanism from the authorities and data subjects on the processing of personal data and ensuring that relevant parties also comply with regulations on personal data protection; and

(c) Ensuring the rights of data subjects and the accountability of the parties in the process of processing personal data; Having a mechanism to receive and handle feedback and recommendations from relevant people and organizations.

SPECIFIC DATA PROCESSING ACTIVITIES

The Draft Law includes new or more detailed articles for the protection of personal data in various specific contexts. In particular, the Draft Law:

(a) Add more detailed regulations on protecting children's personal data, including different consent requirements based on age;

(b) Add more specific rules for personal data protection in marketing and advertising, including the obligation to provide options for users to refuse marketing information;

(c) Provide for personal data protection in AI systems by outlining principles for transparency, oversight, and accountability;

(d) Provide for personal data protection in cloud computing;

(e) Provide for personal data protection in labor supervision and recruitment;[2]

(f) Provide for personal data protection in banking, finance, credit, and credit information activities;[3]

---

[2] Detailed regulations are in Article 29 of the Draft Law. Below are the notable requirements.

When recruiting workers, agencies, organizations and individuals must ensure the following:

(i) Only information in the list of publicly announced recruitment contents or employee profiles are required;

(ii) Information provided in employee profiles is processed in accordance with the provisions of law and must have the consent of the data subject;

(iii) Employee profiles are stored for a period of time as prescribed by law and must be deleted when no longer required or the prescribed period has expired, unless otherwise provided by law; and

(iv) When personal data of employees is updated to the global employee database system: agencies, organizations and individuals collecting and processing personal data must prove that the collection and processing of data is legal and are responsible for the legality of the information they provide.

For foreign companies recruiting and processing personal data of Vietnamese employees living and working in Vietnam, they must:

(i) Comply with the provisions of the law on personal data protection in accordance with the provisions of Vietnamese law;

(ii) Have a written document or contract with organizations and enterprises investing in Vietnam on the processing of personal data of employees; and

(iii) Provide organizations and enterprises investing in Vietnam with copies of data on Vietnamese employees living and working in Vietnam to comply with the provisions of the law when necessary.

[3] This new article (Article 30) requires relevant parties:

(i) Not to buy, sell credit information or illegally transfer credit information between financial, credit, and credit information institutions;

(ii) To fully apply regulations on the protection of sensitive personal data, safety and security standards in banking, financial, credit, and credit information activities as prescribed by law;

(iii) To not use credit information of data subjects to score credit, evaluate credit information, or assess the creditworthiness of data subjects without the consent of data subjects;

(iv) The results of credit information assessment of data subjects used in business activities with other

(g) Provide for personal data protection related to health and insurance information;

(h) Provide for regulations for location data;

(i) Add detailed obligations for personal data protection on social media platforms and online communication services;[4] and

(j) Add specific rules for biometric data.

REQUIREMENT FOR UPDATING THE PERSONAL DATA PROCESSING IMPACT ASSESSMENT DOSSIER AND THE PERSONAL DATA TRANSFER IMPACT ASSESSMENT DOSSIER

The Draft Law requires the Personal Data Processing Impact Assessment Dossier and the Personal Data Transfer Impact Assessment Dossier to be updated on a 6-month period when there is a change. However, an immediate update (and be reported to A05) is required in the following

parties must only be in the form of Pass or Fail, Yes or No, True or False, or a scale based on the database that financial, banking, credit, and credit information institutions collect directly from customers;

(v) To identify and clearly state the stages where personal data de-identification measures are required; and

(vi) To notify data subjects of incidents and loss of information on bank accounts, financial, credit, credit information.

[4] Article 34 of the Draft Law provides that organizations and individuals providing social networking services and online communication services are responsible for:

(i) Protecting personal data of Vietnamese citizens when operating in the Vietnamese market or appearing on mobile application stores provided to the Vietnamese market;

(ii) Clearly announcing the content of personal data collected when data subjects install and use social networks and online communication services; not illegally collecting personal data and beyond the scope of the agreement with customers;

(iii) Not requesting images or videos containing full or partial identity, citizen identification, or identity card content as a factor in account authentication;

(iv) Providing options allowing users to refuse to collect cookies and share cookies;

(v) Providing a "do not track" option or only tracking the use of social networks and online communication services with the consent of the user;

(vi) Providing specific, clear, written notice of the sharing of personal data as well as the application of security measures when conducting advertising and marketing activities based on customers' personal data;

(vii) Not eavesdropping, wiretapping or recording calls and read text messages without the consent of the data subject;

(viii) Providing a mechanism for users to report violations of security and privacy;

(ix) Publishing a security policy, clearly explaining how personal data is collected, used and shared; provide users with the right to access, edit, delete data and set privacy for personal information; protect personal data of Vietnamese citizens when transferred outside the territory of Vietnam; establish a mechanism for users to report violations of personal data protection; develop a process for handling violations of personal data protection quickly and effectively; and

(x) Notifying data subjects of incidents and violations of regulations on personal data protection regarding social network accounts and online communication services within 72 hours of the occurrence of the violation or incident, along with the results of handling, remedying the consequences, assessing the severity of the incident and potential risks arising.

circumstances:

(a) When the company is dissolved or merged;

(b) When there is a change in information about the Personal Data Protection Organization or Personal Data Protection Expert; or

(c) When a new business line arises or the business related to personal data that has been described in the registered Personal Data Processing Impact Assessment Dossier or the Personal Data Transfer Impact Assessment Dossier is discontinued.

The update of the Personal Data Processing Impact Assessment Dossier and the Personal Data Transfer Impact Assessment Dossier can be done on the National Personal Data Protection Information Portal or sent by post or directly to the Personal Data Protection Agency.

UNCLEAR PROVISIONS

There are several areas where the provisions, while outlining principles and frameworks, may contain language that could be considered broad or require further clarification through implementing regulations. Here are some examples:

(a) Definition of "other related actions" in data procession: The definition of "personal data processing" includes a list of activities such as collection, recording, analysis, etc., or " other related actions". This phrase could be seen as broad and may require interpretation in specific contexts to determine what actions fall under the definition of processing.

(b) Conditions for Data Processing Without Consent: Article 19 outlines circumstances where consent is not required, such as "emergency situations" to protect the life or health of the data subject or others. The threshold and specific scenarios that qualify as "emergency situations" might be open to interpretation. Similarly, processing data for "national defense, national security, social order and safety" could be broadly defined.

(c) Conditions for Cross-border Data Transfer: Article 46 outlines cases of cross-border transfer and mentions that the Personal Data Protection Agency can order the cessation of transfer if the data is used in activities violating national interests. The definition of activities that violate "interests, national defense, national security" could be broad and might require further guidance to ensure consistent application.

(d) Update of the Impact Assessment Dossiers: Article 47 requires periodic updates to the Personal Data Processing Impact Assessment Dossier and the Cross-border Data Transfer Impact Assessment Dossier every six months or immediately upon changes. The nature and significance of changes that necessitate a 6-month update might require further clarification. Insignificant changes should not be required for an update and report.

TRANSITIONAL PROVISIONS

The Draft Law allows agencies, organizations and enterprises engaging in collecting, processing and/or transferring data to designate departments and personnel with the function of protecting personal data in place of the Personal Data Protection Organization and Personal Data Protection Expert required under the Draft Law within one year from the date the Draft Law becomes effective.

In addition, the Draft Law allows small businesses and startups to be entitled to choose to be exempted from the application of the provisions on Personal Data Protection Organizations and Personal Data Protection Experts for the first five years from the date of establishment of the business. For small businesses and startups directly engaged in the business of processing personal data, they are not subject to these provisions.

For the requirement on Personal Data Protection Expert, small businesses and startups are entitled to opt for an exemption for the first five years from the date of establishment. However, the requirement does not apply to micro-enterprises, small businesses and startups directly engaged in the business of processing personal data.

TIMELINE

The Draft Law is scheduled to be debated and ratified at the coming National Assembly's session in May 2025, and will take effect on 1 January 2026.

We hope our article has been helpful to you. Please feel free to contact us if you have any further inquiries.

Scientia