SOME IMPACTS OF THE PERSONAL DATA PROTECTION LAW FROM 2026

LUU TUE DANG

The Law on Personal Data Protection 91/2025/QH15, which will officially take effect on January 1, 2026, is a law with a broad scope of regulation, applicable to all agencies, organizations, and individuals directly involved in or related to the processing of Vietnamese citizens' personal data. Notably, the Law supplements and tightens the responsibilities of data processing entities in several specific activities and sectors such as labor, insurance business, credit, media, and information technology. Therefore, readers should pay close attention to the points analyzed below, and proactively study and seek legal consultation to ensure full compliance with the Law from January 1, 2026.

First, the Law on Personal Data Protection continues to recognize two groups of personal data, namely *basic personal data and sensitive personal data*, similar to Decree 13/2023/ND-CP. However, the Law only provides principle-based definitions of these two categories, specifically: (i) *Basic personal data* refers to personal data reflecting common personal and identity factors that are frequently used in transactions and social relations; (ii) *Sensitive personal data* refers to personal data associated with individuals' privacy rights that, if infringed upon, directly affect legitimate rights and benefits of agencies, organizations, and individuals; and (iii) The specific list of these two data types will be promulgated by the Government. This approach ensures consistency and avoids conflicts with available laws, particularly Decree 13/2023/ND-CP, which is still in force, specifying personal data categories. However, organizations and individuals should note two additional issues:

- Currently, a new draft decree detailing the implementation of the Law on Personal Data Protection is being developed. The draft tends to expand the list of sensitive personal data as compared to Decree 13/2023/ND-CP by adding several categories such as: electronic identity information, data on telecommunications subscriber activities and history, behavioral tracking data, and usage data of telecommunications, social media, online communication services, and other cyberspace services; as well as information on financial, securities, and insurance transactions of customers at credit institutions, foreign bank branches, intermediary payment service providers, securities companies, and insurance organizations. Businesses operating in these sectors should pay particular attention as these provisions are likely to be officially adopted soon.
- The Law also contains separate provisions on personal *location data and biometric data* (The aforementioned draft decree detailing the implementation of the Law on Personal Data Protection also classifies "personal location data" and "biometric data" as sensitive personal data). Personal location data refers to data determined through positioning technology that indicates the location and identification of a specific person, and

biometric data refers to data on a person's unique and stable physical attributes or biological characteristics used to identify such person. The responsibilities of organizations and individuals processing such data will be tightened. Specifically, organizations and individuals that provide mobile application platforms must (i) notify users of the use of their personal location data, (ii) adopt measures to prevent unauthorized organizations or individuals from collecting such location data, and (iii) provide users with options to track their personal locations. Meanwhile, agencies, organizations, and individuals collecting and processing biometric data must (i) adopt physical confidentiality measures for their biometric data transmission and storage devices, (ii) restrict rights to access to biometric data, (iii) establish monitoring systems to prevent and detect acts of infringement on biometric data, and (iv) notify data subjects when the processing of biometric data causes them any damage.

Second, compared to Decree 13/2023/ND-CP, the Law introduces several new prohibited acts, including: (i) Using personal data of others and/or letting others use one's personal data to violate the laws; (ii) trading personal data, unless otherwise prescribed by law; and (iii) appropriating, intentionally leaking, or causing the loss of personal data. Violations of these prohibitions or other data protection regulations may result in administrative sanctions, criminal liability, or civil compensation, depending on the nature, severity, and consequences of the act. Regarding administrative sanctions, organizations and individuals should note that: Illegal trading of personal data may be fined up to 10 times the amount of revenue gained from the violation; Violations of cross-border personal data transfer regulations may be fined up to 5% of the violator's previous year's revenue; Other violations related to personal data protection may incur fines of up to VND 3 billion. These stricter sanctions are necessary to address the growing number of cases involving the theft and public sale of personal data online that have not been effectively handled.

Third, similar to Decree 13/2023/ND-CP, the Law affirms the general principle that personal data may only be processed with the consent of the data subject, except for certain cases where consent is not required, such as when data processing is: (i) to perform agreements between the data subject and relevant entities as prescribed by law; (ii) to serve the operations or state management activities of competent authorities; (iii) to respond to emergencies threatening national security or to prevent and combat crimes or legal violations (e.g., filing a criminal complaint under criminal procedure law); or (iv) to record or film public activities or events (such as conferences, seminars, sports competitions, art performances, and other public activities), provided that such data collection does not harm the dignity or reputation of data subjects. However, to ensure flexibility and reduce procedural burdens during the transition period when the Law first takes effect, the Law provides that organizations and individuals who have already obtained consent or entered into agreements with data subjects under Decree 13/2023/ND-CP before January 1, 2026 may continue processing data without having to obtain consent or re-negotiate with the data subjects again.

Fourth, the Law continues to require an impact assessment of personal data processing and cross-border data transfer. Organizations and individuals must prepare and submit a set of original dossier to the personal data protection authorities (under the draft decree, it is expected to be the Department of Cybersecurity and High-Tech Crime Prevention – A05, Ministry of Public Security) within 60 days from the first day of data processing (for processing impact assessments) or from the first day of cross-border data transfer (for transfer impact assessments). These assessments are conducted once for their entire operation, but updates must be made every 6 months or immediately in the event of: (i) reorganization, operational termination, dissolution, or bankruptcy; (ii) changes to the information on the personal data protection service providers; or (iii) changes in business lines or business services concerning personal data processing arise that differ from those registered in the dossier on assessment of personal data processing impact and dossier on assessment of cross-border personal data transfer impact. To reduce compliance burdens, the Law provides that:

- In the cases where agencies, organizations, or individuals have already conducted a personal data processing impact assessment or a cross-border personal data transfer impact assessment in accordance with this Law, they are not required to repeat the risk assessment or impact assessment under other data-related legal instruments. This provision is introduced in the context that another legal document on data – the Law on Data 60/2024/QH15, which took effect on July 1, 2025 – has also imposed the obligations to assess the impact of cross-border transfer and processing of "core data" and "important data," which include personal data.
- With respect to the dossier of personal data processing impact assessments and cross-border personal data transfer impact assessments received by the competent authority under Decree 13/2023/ND-CP before January 1, 2026, organizations and individuals may continue to use them and are not required to resubmit or prepare a new dossier in accordance with the provisions of the

Law on Personal Data Protection.

Fifth, personal data protection in other specific sectors and activities is regulated as follows:

- In **labor relations**, employers must delete or destroy personal data of applicants who are not recruited, as well as the personal data of employees upon termination of employment contracts, unless otherwise agreed or provided by law. Accordingly, employers' data protection responsibilities are broadened - it arises not only during the recruitment stage prior to the conclusion of employment contracts but also continues at the point of termination of the employment relationship.
- In the **banking and credit sector**, organizations and individuals operating in this field must not use the credit information of a personal data subject to conduct credit scoring, credit ranking, credit information assessment, or creditworthiness evaluation without the prior consent of the data subject. This provision aligns with the principle of obtaining consent before processing data and contributes to protecting the personal data of borrowers. However, it also poses challenges for credit institutions in managing risks and assessing the feasibility of extending further credit to existing clients.
- In **online activities**, organizations and individuals providing social network services or online communication services are required to fulfill various obligations to protect the personal data of data subjects. These include: (i) refraining from requesting images or videos containing all or part of an identity document as an authentication factor for account verification; (ii) not eavesdropping, wiretapping, or recording phone calls or reading text messages without consent by the data subject, unless otherwise provided by law; and (iii) providing users with the option to refuse data collection and sharing, as well as a "do not track" option or only tracking users' social network or online communication activities with their consent. These regulations enhance the safety and control of users over their personal data in the online environment, which inherently carries a high risk of data theft, unauthorized access, or misuse, even when users have applied necessary technical security measures.
- Additionally, the Law also imposes stricter requirements for personal data processing activities in certain specialized sectors, such as advertising services, insurance business, and information technology fields, including big data processing, artificial intelligence, blockchain, metaverse, and cloud computing.

The promulgation of the Law on Personal Data Protection has contributed to better ensuring the rights of personal data subjects, establishing mechanisms to prevent acts that infringe upon personal data and affect the rights and interests of individuals and organizations more effectively, and enhancing the responsibility of agencies, organizations, and individuals in data processing. However, the Law also poses many challenges as it requires organizations and individuals to comply with stricter obligations and responsibilities in personal data processing. Therefore, enterprises, organizations, and individuals need to proactively study in detail the provisions of the Law on Personal Data Protection, together with any draft Decree guiding its implementation, to ensure full compliance in the near future. This will help prevent the risk of violations and avoid the imposition of any administrative, civil, or criminal sanctions in accordance with the law. In the case that our valued Clients and readers wish to learn more and seek consultation related to the new provisions of the Law on Personal Data Protection, as well as other issues related to personal data in general, NHQuang&Associates is ready to provide further explanations and relevant legal opinions.