

Special Alert

DECREE NO. 356/2025 - A NEW PROTECTIVE SHIELD FOR PERSONAL DATA IN VIETNAM

January 2026

On 31 December 2025, the Government officially promulgated Decree No. 356/2025/ND-CP detailing a number of articles and measures for the implementation of the Law on Personal Data Protection (“**Decree 356**”). Decree 356 takes effect from 1 January 2026 and replaces Decree No. 13/2023/ND-CP on personal data protection (“**Decree 13**”).

Accordingly, together with the Law on Personal Data Protection (the “**PDPL**”), Decree 356 is expected to serve as a new protective shield for personal data in Vietnam, contributing to the effective implementation of the PDPL. At the same time, both PDPL and Decree 356 aim to ensure human rights and the right to privacy, prevent acts of personal data infringement, raise awareness and foster a culture of personal data protection, and clearly define the responsibilities of agencies, organizations, and individuals in personal data processing activities.

Key Takeaways

- **Categories of Personal Data:** Decree 356 introduces significant adjustments to the categories of basic personal data and sensitive personal data.
- **Data Subject Consent and Responsibilities in Handling Data Subject Requests:** Decree 356 expressly prohibits “default consent” or misleading consent mechanisms. It also standardizes and clarifies response timelines and processing deadlines for data subject requests, which are now more specific and detailed than those under Decree 13.
- **Impact Assessment Dossiers for Personal Data Processing and Cross-Border Transfer of Personal Data:** The provisions on the Personal Data Processing Impact Assessment Dossier (the “**PDPIA Dossier**”) and the Cross-Border Personal Data Transfer Impact Assessment Dossier (the “**CPDTIA Dossier**”) continue to be

recognized under Decree 356, with adjustments and changes derived from the practical implementation of Decree 13.

- **Regulations on Personal Data Transfers:** Decree 356 clarifies cases where data transfer agreements are required, the minimum mandatory contents of such agreements, and additional security requirements applicable to the transfer of sensitive personal data.
- **Requirements for Personal Data Protection Personnel:** Decree 356 sets out specific requirements regarding qualifications, experience, and training for personal data protection personnel, thereby emphasizing the role of the human factor in the personal data protection compliance framework.
- **Personal Data Protection in Specific Sectors:** Sectors such as finance and banking, big data processing, AI, metaverse, blockchain technology, and cloud computing are subject to distinct technical requirements and data protection principles, reflecting their specific technological characteristics and associated risks.

This article highlights the most notable provisions of Decree 356, analyzes its key regulatory developments, and identifies practical issues that agencies, organizations, and individuals should carefully consider when implementing personal data protection measures.

Categories of Personal Data

With respect to the **Basic Personal Data**, in the context of Viet Nam's ongoing efforts to promote comprehensive and coordinated digital transformation across multiple sectors, with a view to achieving national data interoperability while ensuring data security and safety in cyberspace, Decree 356 introduces a number of notable changes to the category of basic personal data compared to Decree 13, as follows:

- **National identity card numbers, personal tax identification numbers, social insurance numbers, and health insurance card numbers** have been removed from the category of basic personal data, as such information has been replaced by the personal identification number.
- **Family relationship information** has been expanded to include "spouse" (husband and wife), whereas Decree 13 previously only covered "parents" and "children"; and
- **Personal data reflecting activities and activity history in cyberspace** is no longer classified as basic personal data under Decree 356, but has been reclassified as sensitive personal data.

As regards the **Sensitive Personal Data**, Decree 356 further expands and clarifies the scope of sensitive personal data, with a view to comprehensively covering data categories that require heightened attention during processing activities, while at the same time enhancing data subjects' awareness of sensitive personal data relating to them.

- **View of beliefs** have been added to the category of sensitive personal data, alongside views of politics and

religion. The fact that the Decree 13 did not recognize beliefs as sensitive personal data may be regarded as a notable shortcoming, given that religion and belief are separately and specifically regulated under the Law on Belief and Religion, particularly in light of Viet Nam's religious and belief diversity. Accordingly, this adjustment contributes to better safeguarding the freedom of belief and religion of data subjects.

- **Data relating to violations of law by individuals** is now classified as sensitive personal data, whereas previously only data relating to violations reaching the level of criminal liability (such as crimes or criminal acts) was regarded as sensitive personal data.
- **Banking-related data**, such as login credentials and passwords for bank accounts, bank card information, transaction histories, as well as transaction data in securities and insurance sectors held by securities firms and insurance companies, are now deemed sensitive personal data. This reflects an expanded scope that goes beyond traditional banking transaction data.
- **Data relating to the tracking of behaviors and usage activities of telecommunications services, social networks, online media services, and other services in cyberspace** has been added to the category of sensitive personal data. This revision under Decree 356 is particularly necessary in light of the increasing prevalence of personal data infringements in the online environment.

One point that requires particular attention in the provisions on the category of personal data is that only personal identification numbers are classified as basic personal data, while login credentials for electronic identification accounts and images of identity cards or citizen identity cards are classified as sensitive personal data.

This specific distinction stems from the fact that the aforementioned information and images, if compromised, may directly and seriously affect the lawful rights and interests of agencies, organizations, and individuals. Specifically, the risks may include unauthorized access to electronic identification accounts, the use of images of national identity cards / citizen identity cards to obtain loans via applications, register postpaid mobile subscriptions, create fictitious tax identification numbers, or carry out other unlawful activities. In addition, the QR code embedded in citizen identity cards contains a substantial amount of personal data, which may be exploited by cybercriminals for illicit gain.

Accordingly, Decree 356 emphasizes the obligation of agencies and organizations to establish access control mechanisms, processing procedures, and enhanced security measures when handling sensitive personal data.

Data Subject Consent and Responsibilities in Handling Data Subject Requests

Data subject consent is always a key requirement in personal data processing activities. However, under the PDPL, there are certain exceptions under which agencies and organizations are permitted to process personal data without the data subject consent. One notable exception is the processing of personal data for the purpose of performing an agreement of the data subject with relevant agencies, organizations, or individuals in accordance with law, such as the performance of an employment contract between an employer and an employee. Although Decree 356 has not yet provided more detailed

guidance on this provision of the PDPL, this remains an aspect that agencies and organizations may consider and assess for application in their practical operations.

Notably, Decree 356 further clarifies the responsibilities of the Data Controller and the Data Controller-cum-Processor in relation to the collection, management and demonstration of the data subject consent. Accordingly, these entities are required to retain records of data subject consent and are prohibited from implementing “default consent” mechanisms, as well as from creating unclear or misleading instructions that may cause confusion between consent and non-consent for data subjects.

In addition, in order to safeguard the lawful rights and interests of data subjects, Decree 356 provides more specific and detailed timelines and deadlines concerning the responsibility to receive and handle data subject requests, replacing the relatively general 72-hour time limit stipulated under Decree 13.

Accordingly, Data Controller and Data Controller-cum-Processor are required to establish clear procedures, processes, and standardized forms for the implementation of data subject requests, and to comply with the corresponding response and processing time limits applicable to each type of request, as detailed below:

No.	Data Subject Requests	Response Deadline	Processing Deadline
1	Requests to withdraw consent / restrict processing / object to processing	2 working days	15 days (20 days if involving Data Processor / Third Party)
2	Request to access / rectify / provide personal data		10 days (15 days if involving Data Processor / Third Party)
3	Request for erasure of personal data		20 days (30 days if involving Data Processor / Third Party)
4	Request for implementation of personal data protection measures, solutions		15 days

Although Decree 356 sets out specific statutory timelines for handling requests, data subjects should be aware that, in order for such timelines to apply, they must comply with the procedures agreed upon and prescribed by the Data Controller or the Data Controller-cum-Processor. Where a data subject fails to follow these procedures, the response and processing of the request may be prolonged, potentially affecting the data subject’s lawful rights and interests.

Decree 356 also permits a one-time extension of the processing deadline, depending on the nature and complexity of the request, subject to an obligation to provide a reasonable and necessary justification for such extension.

Impact Assessment Dossiers for Personal Data Processing and Cross-Border Transfer of Personal Data

One of the matters of particular concern to agencies and organizations upon the effectiveness of Decree 356 is the set of provisions governing the obligations and responsibilities to prepare the PDPIA Dossier and CPDTIA Dossier.

Pursuant to the PDPL, where an agency's or organization's dossiers have been received by the Specialized Authority for Personal Data Protection in accordance with Decree 13 prior to 1 January 2026, such dossiers shall remain valid and no new dossiers are required to be prepared. However, where an agency or organization updates or amends the contents of the previously submitted dossiers, or has not fulfilled the obligation to prepare such dossiers under Decree 13, then as from 1 January 2026, the preparation of the dossiers must comply with the procedures, processes and templates prescribed under PDPL and Decree 356.

Overall, Decree 356 introduces fundamental changes to both the form and content of the above-mentioned dossiers, adopting an integrated approach and revising and supplementing technical requirements. At the same time, Decree 356 no longer specifically designates the Department of Cybersecurity and Hi-Tech Crime Prevention (A05) as the focal point authority for receiving and handling matters related to personal data protection, but instead generally refers to the Specialized Authority for Personal Data Protection.

In addition, while Decree 13 did not clearly specify the responsibilities of the Specialized Authority for Personal Data Protection in assessing and responding to the results of the above PDPIA Dossier and CPDTIA Dossier, Decree 356 now expressly addresses this issue. Accordingly, the Specialized Authority for Personal Data Protection is responsible for assessing such dossiers and notifying whether they meet or fail to meet the prescribed requirements within 15 days from the date of receipt of a valid dossier.

Another noteworthy aspect of Decree 356 that agencies and organizations should take into account in order to ensure effective implementation and avoid unnecessary compliance costs is that the Decree 356 expressly prescribes the cases in which the CPDTIA Dossier is not required. Notable examples include:

- The cross-border transfer of personal data for the purpose of cross-border human resources management in accordance with internal regulations, labor rules and collective bargaining agreements that are compliant with applicable laws; or
- The provision of personal data across borders for the purpose of entering into contracts or carrying out procedures related to cross-border transportation, logistics, remittances, payments, hotel bookings, visa applications or scholarship applications.

In these cases, agencies and organizations are not required to prepare the CPDTIA Dossier in accordance with Decree 356.

Regulations on Personal Data Transfers

PDPL provides for a total of seven (7) cases of personal data transfer and delegates to the Government the authority to prescribe detailed responsibilities and corresponding obligations. On that basis, Decree 356 stipulates that, in the following three (3) cases of personal data transfer, organizations and individuals are required to establish a personal data transfer agreement, which must at a minimum include the following elements: purpose; categories of data; duration; legal

basis; data protection responsibilities; responsibilities for facilitating the exercise of data subject rights; and coordination mechanisms in the event of a violation:

- Transfer of personal data based on the consent of the data subject;
- Transfer of personal data for the purpose of continuing the processing of personal data in the event of the division, separation or merger of agencies, organizations or administrative units, etc.; and
- Transfer of personal data by Data Controller or Data Controller-cum-Processor to Data Processor or Third Party for the processing of personal data in accordance with applicable regulations.

Where the personal data being transferred constitutes sensitive personal data, in addition to entering into a data transfer agreement, the transferring parties are required to implement physical security measures for data storage and transmission devices, as well as encryption, anonymization of personal data, and other appropriate security measures.

In the case of internal sharing of personal data among departments within the same agency or organization for the purpose of personal data processing, Decree 356 does not require the establishment of a transfer agreement as in the three cases mentioned above. Instead, agencies and organizations are required to develop internal control procedures governing the lawful sharing and use of personal data.

For transactions conducted on data exchanges, personal data must be de-identified prior to trading. With respect to this requirement, further guidance and more detailed regulations on personal data de-identification are still expected.

It should also be noted that where agencies, organizations, or individuals provide personal data in response to a specific request from the data subject, such provision does not constitute a personal data transfer and is therefore not subject to the above requirements. This approach appears to reflect the practical reality that data subjects seek to exercise their rights in relation to their own personal data, including the right to monitor and supervise how their personal data is being processed, as well as to identify which personal data relating to them is being collected and processed.

Requirements for Personal Data Protection Personnel

Decree 356 requires organizations to appoint personnel responsible for personal data protection who meet the following qualifications:

- Possess at least a college-level degree or higher;
- Have a minimum of two (2) years of professional experience (calculated from the date of graduation) in one or more of the following fields: legal affairs, information technology, cybersecurity, data security, risk management, compliance control, human resources management, or organizational and personnel management; and

- Have received training and professional development in personal data protection laws and relevant technical skills.

This provision of Decree 356 grants agencies and organizations autonomy in recruiting and appointing personnel responsible for personal data protection, while also assigning them the responsibility for providing training and capacity building on personal data protection knowledge and skills. This approach offers greater flexibility and convenience for agencies and organizations in the course of compliance. However, the absence of a formal mechanism for inspection, assessment and ex post review of such personnel, agencies and organizations may give rise to certain practical risks to the rights and interests of data subjects.

Personal Data Protection in Specific Sectors

In addition to the general provisions governing personal data protection, Decree 356 devotes considerable attention to regulating personal data protection in certain specific sectors, thereby requiring relevant parties to apply more cautious and stringent measures.

- **In financial, banking, and credit information activities:** Decree 356 requires the application of personal data protection standards and technical regulations, including technical standards for the de-identification and anonymization of personal data as promulgated and applied in Vietnam.
- **In big data processing:** Agencies, organizations, and individuals are required to implement strong authentication mechanisms, with a minimum requirement of multi-factor authentication (such as passwords, PINs combined with one-time passwords, digital signature devices, or biometric factors), as well as role-based access controls to ensure that only authorized persons are able to access personal data.
- **In AI systems and metaverse:** Decree 356 requires that data subjects be granted the right to edit, anonymize, or delete identity profiles, even in cases where the platform retains behavioral history data.
- **In blockchain technology:** Decree 356 requires that personal data must not be stored directly on the blockchain, personal data may only be stored where it has been de-identified or in the form of a hash value of the personal data. Current personal data protection laws recognize two (02) notable concepts: “**de-identification**” and “**encryption**”. The key distinction is that personal data that has been encrypted is still regarded as personal data and remains subject to the applicable legal requirements, whereas personal data that has been de-identified is no longer considered personal data.
- **In cloud computing:** Personal data must be encrypted both at rest and in transit, together with the implementation of strict access control mechanisms. Unlike blockchain technology, personal data in cloud computing must be encrypted, meaning that it is converted into an unreadable form without decryption, and personal data, even after encryption, is still regarded as personal data.

The differences in the requirements applicable to personal data in cloud computing and blockchain technology may stem

from the design characteristics of each technology. Specifically, cloud computing is designed to manage personal data in a controlled environment; therefore, the legal framework focuses on data security requirements. By contrast, blockchain technology is designed to store data in an immutable and decentralized manner, which accordingly necessitates the removal of identifying elements relating to individuals from the outset.

Conclusion

Personal data is a matter closely associated with human rights and citizens' rights, as well as safety and security in cyberspace, information security, data security, information technology, the Fourth Industrial Revolution, and the development of e-government, digital government, and the digital economy. Decree 356 is expected to further Vietnam's legal framework for personal data protection.

However, Decree 356 currently provides guidance on only certain provisions of the PDPL. Accordingly, in order to enhance the effectiveness of implementation and enforcement, as well as to fully realize the practical value and significance of the PDPL, in the time ahead, there is a basis for expectation and a shared anticipation of further guiding instruments in the field of personal data protection.

About Indochine Counsel

Established in October 2006, Indochine Counsel is a premier commercial law firm in Vietnam. We're ideally positioned to help international investors and foreign firms navigate the legal landscape in one of Asia's most dynamic and exciting countries. We also take pride in our services for domestic clients searching for opportunities abroad. With over 45 lawyers and staff in two offices, Ho Chi Minh City and Hanoi, Indochine Counsel offers expertise in a dozen practice areas assisting you throughout the entire life cycle of your business. We're your trusted partner in Vietnam for international and domestic legal solutions.

Indochine Counsel represents and advises clients on all legal aspects in the following major areas of expertise:

- Anti-trust & Competition
- Banking & Finance
- Corporate & Commercial
- Energy, Natural Resources & Infrastructure
- Intellectual Property
- Inward Investment
- Labour & Employment
- Litigation & Dispute Resolution
- Mergers & Acquisitions
- Real Estate & Construction
- Securities & Capital Markets
- Technology, Media & Telecommunications

Contact Us

For further information or assistance, please contact the following professionals at Indochine Counsel:



Dang The Duc
Managing Partner
E duc.dang@indochinecounsel.com



Thai Gia Han
Senior Associate | Head of IP & TMT
Practice Group
E han.thai@indochinecounsel.com



Nguyen Le Toan Phuoc
Legal Assistant
E phuoc.nguyen@indochinecounsel.com

Ho Chi Minh City

Unit 305, 3rd Floor, Centec Tower
72-74 Nguyen Thi Minh Khai, Xuan Hoa Ward
Ho Chi Minh City, Vietnam

T +84 28 3823 9640
F +84 28 3823 9641
E info@indochinecounsel.com

Hanoi

Unit 705, 7th Floor, CMC Tower
Duy Tan Street, Cau Giay Ward
Hanoi, Vietnam

T +84 24 3795 5261
F +84 24 3795 5262
E hanoi@indochinecounsel.com

This Special Alert is designed to provide our clients and contacts with general information of the relevant topic for reference only, without the assumption of a duty of care by Indochine Counsel. The information provided is not intended to be nor should it be relied upon as a substitute for legal or other professional advice.

© 2006 – 2026 Indochine Counsel. All Rights Reserved



You can reach us at
[Indochinecounsel.com](https://www.indochinecounsel.com)



LinkedIn



Facebook



YouTube