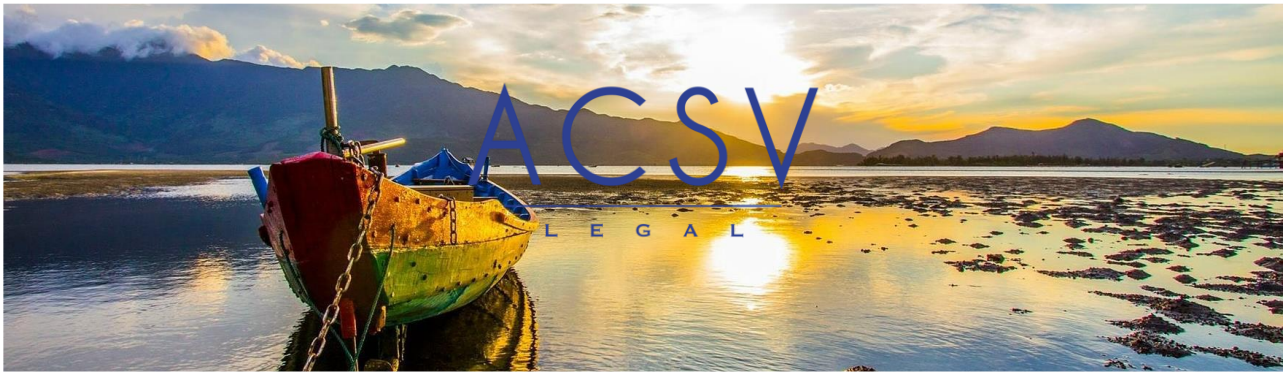


LEGAL UPDATE

DECREE DETAILING THE IMPLEMENTATION OF THE LAW ON PERSONAL DATA PROTECTION

On 31 December 2025, the Government of Vietnam officially issued Decree No. 356/2025/ND-CP ("**Decree**"), which provides detailed guidance on the implementation of the Personal Data Protection Law (Law No. 91/2025/QH15) ("**PDP Law**"). Both the Decree and the PDP Law took effect from **1 January 2026**, marking the formal transition from Decree No. 13/2023/ND-CP ("**Decree 13**") to a higher-level statutory framework. This transition reflects a significant improvement of Vietnam's personal data protection regime, shifting from a sub-law instrument to a comprehensive law, with stricter enforcement mechanisms and more specialised rules addressing the employment of advanced data processing technologies.

Below are the remarkable changes introduced by the Decree.

1. Refinement of the Classification of Basic and Sensitive Personal Data

While the overall structure of personal data (**PD**) classification remains broadly consistent with Decree 13, the Decree introduces important refinements that significantly elevate the level of protection for the PD commonly processed in daily business activities.

In particular, the PD relating to behavioural tracking and usage of telecommunications services, social networks, online media services, and other services in cyberspace has been reclassified from **basic PD** to **sensitive PD**. In addition, the Decree expressly expands the scope of sensitive PD to include, among others:

- Bank account information, bank cards and transaction history;
- Usernames and passwords for electronic identification accounts; and
- Images of identity cards, citizen identity cards, and identity documents.

Such reclarification addresses ambiguities under Decree No. 13, where certain high-risk data types were not expressly classified, resulting in inconsistent levels of protection in practice. Additionally, when processing sensitive PD, businesses are required to implement restricted access controls, strict processing procedures and robust security measures to ensure adequate data protection.

2. Extended Timelines for Responding to Data Subject Requests

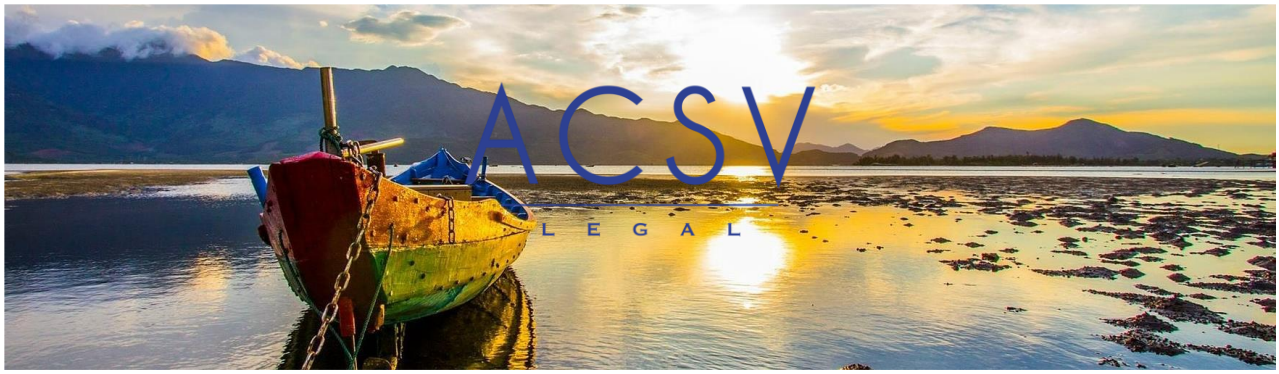
Under Decree 13, the widely debated "72-hour principle" applied to most data subject rights, requiring data controllers and controller-cum-processors to respond within 72 hours after receiving the data subject's request. In practice, this timeline is challenging for implementation.

The Decree substantially extends these timelines. In summary:

i. Withdrawal of consent, restriction and objection
- Response: within 2 business days.
- Implementation: within 15 days (with a one-time extension only, for a period not exceeding 15 days) for controllers and controller-cum-processors; and within 20 days for processors and third parties.

ii. Access, rectification, and provision
- Response: within 2 business days.
- Implementation: within 10 days (with a one-time extension only, for a period not exceeding 10 days) for controllers and controller-cum-processors; and 15 days for processors and third parties.

iii. Erasure
- Response: within 2 business days.
- Implementation: within 20 days (with a one-time extension only, for a period not exceeding



20 days) for controllers and controller-cum-processors; and 30 days for processors and third parties.

This adjustment reflects a more pragmatic approach, balancing the protection of data subject rights with operational practices of enterprises.

3. Stricter Requirements for Obtaining Consents

Compared with Decree No. 13, the Decree provides clearer and more detailed guidance on acceptable consent methods, while at the same time raising the compliance threshold. Specifically, controllers and controller-cum-processors must ensure that consent mechanisms allow verification of:

- the timing of consent;
- the contents to which the consent is applied; and
- the identity of the data subject.

Permissible methods include written consents, recorded phone calls, SMS-based messages, emails, websites, platforms or applications with technical consent-capture functions, and other verifiable methods.

Importantly, the Decree expressly prohibits default consent mechanisms or misleading designs that confuse the data subjects as to the distinction between consent and non-consent. Default settings must comply with personal data protection (**PDP**) principles and respect data subject rights.

4. Detailed Rules on Personal Data Transfer

The Decree provides comprehensive rules governing the PD transfers, including:

i. **Mandatory written agreements** are required for PD transfers based on (i) the data subject's consent, (ii) corporate restructuring, or (iii) transfers by controllers or controller-cum-processors to processors or third parties for data processing. Such agreements must clearly specify the transfer purpose, data subjects, types of the PD transferred, legal basis for the transfer, processing duration, and the respective responsibilities for PDP and the exercise of data subject rights.

ii. **Enhanced security measures** apply to the transfer of sensitive PD. These include physical security measures for storage and transmission devices, encryption, anonymisation, and other appropriate technical and organisational safeguards during the transfer process.

iii. **Internal data sharing** within the businesses, where consistent with the established processing purposes, must be governed by internal measures and control procedures to ensure the lawful sharing and use of personal data, and to prevent unauthorised disclosure of the PD by internal personnel to third parties.

iv. **Anonymisation** of the PD is required prior to any trading of the PD on data exchanges.

These provisions significantly raise the compliance threshold for data sharing and monetisation activities.

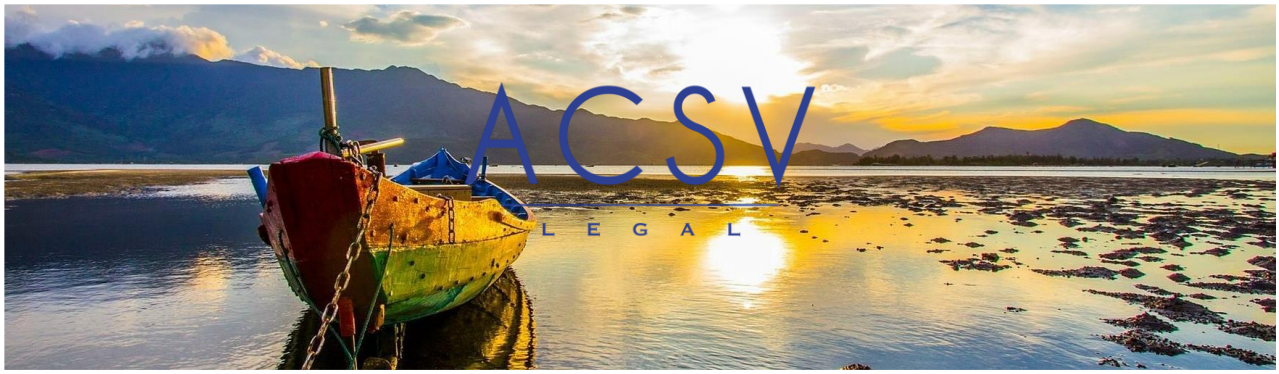
5. Standardisation of Requirements for Data Protection Officers and Departments (DPO/DPD)

The Decree formalises the appointment of DPO or DPD through an official written appointment decision issued by the businesses, which must clearly set out the scope of assignment, functions, duties, powers and other relevant requirements relating to the responsibilities of DPOs and DPDs.

In addition, the Decree **sets out specific qualification requirements** for DPO/DPD. These include appropriate educational background; relevant working experience in legal, information technology, cybersecurity, data security, risk management, compliance, or HR; and having been trained and equipped with knowledge and skills relating to PDP.

It appears that the Decree allows the DPO to be exempted from certain liabilities arising from the PD breaches, as long as those exemptions are included in an agreement with the appointing organization of the DPO.

Overall, this new point reflects a clearer organisational structure for the brand-new position of DPO or brand-new department of DPD in an enterprise.



6. Expanded Exemptions from Cross-Border Data Transfer Impact Assessments (DTIA) Report

In addition to exemptions already provided under the PDP Law, the Decree introduces additional circumstances in which businesses are not required to prepare DTIA reports, including journalism and media activities; publicly disclosed data; emergency situations where cross-border data transfers are necessary to protect life, health or property, or to fulfil statutory duties; cross-border human resource management in accordance with internal labour rules and collective labour agreements, and data transfers necessary for logistics, payments, travel, visas or scholarships.

These expanded exemptions provide greater operational flexibility for businesses engaged in cross-border activities, particularly in sectors such as human resources, logistics, travel, finance and international services. By narrowing the scope of cases requiring DTIA reports, the Decree helps reduce administrative burdens and compliance costs for many eligible enterprises.

7. Clarification of Timelines for Updating DPIA and DTIA Reports

Where the PDP Law requires PD Processing Impact Assessments (**DPIA**) or DTIA reports to be updated "immediately" in certain cases without specifying a concrete timeframe, the Decree addresses this ambiguity by introducing a **clear deadline of 10 days**, thereby improving legal certainty and consistency in implementation.

8. Exemptions for Micro, Small and Start-Up Businesses

The PDP Law provides that certain obligations, including the submission of DPIA report, updating of DPIA and DTIA reports, and the appointment of DPO/DPD, **may not be exempted** for micro and small enterprises and innovative start-up businesses where such companies provide the PD processing services, directly process sensitive PD, or process the PD of a large number of data subjects. However, it does not specify clear criteria for determining when such non-exemptions apply in practice.

To address this gap, the Decree introduces clear criteria. In particular, a business is deemed to process the PD on a large scale where it processes the PD of **100,000 data subjects or more**. In addition, the Decree identifies a clearer scope of what PD processing services should be to shed light on the definition of "PD processing service".

9. Enhanced Breach Notification Obligations on Location and Biometric Data

The Decree introduces a standalone provision governing PD breaches involving location data and biometric data, underscoring the heightened sensitivity and risk level of these categories of PD.

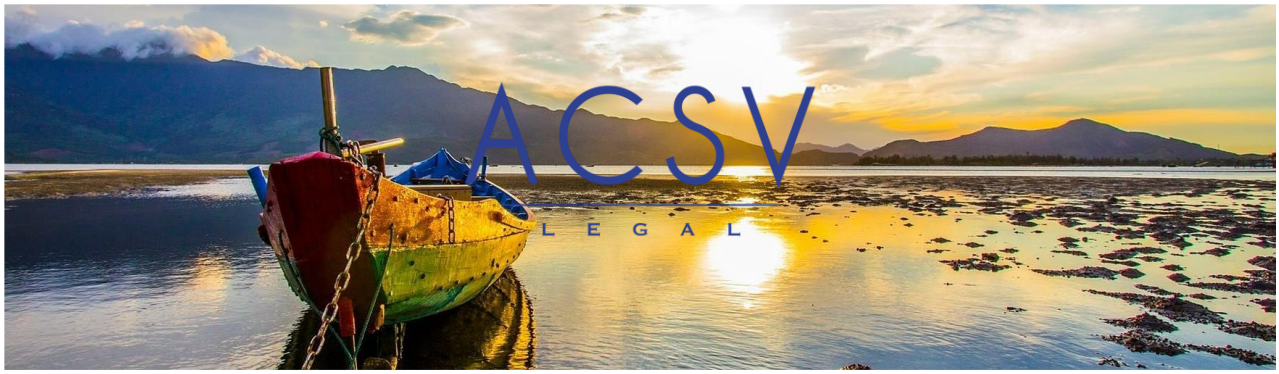
Compared with breaches involving other types of PD, businesses are subject to stricter notification obligations. In addition to notifying the competent PDP authority such as the Ministry of Public Security, businesses are required to notify affected data subjects. Such notification must, at a minimum, specify when and how the breach was detected, the type of PD affected (location data, biometric data, or both), the severity of the breach and associated risks to data subjects, the remedial measures taken or planned, guidance for affected data subjects, and the relevant contact points of the company responsible for PDP and incident handling.

Where a company is unable to notify all affected data subjects within the required timeframe due to technical constraints or emergency circumstances, it must instead issue a public notification via its official electronic communication channels, such as its website or application, and subsequently provide individualised notifications as soon as technically possible.

Failure to provide timely notification, or any intentional delay or avoidance of notification obligations, may result in administrative sanctions in accordance with applicable laws.

Records of PD breach incidents must be retained for a minimum period of 5 years from the date on which remediation of the incident is completed.

By introducing a dedicated breach notification regime for location and biometric data, the Decree signals a higher



compliance expectation for businesses handling these highly sensitive data types. Businesses should review and, where necessary, strengthen incident response procedures, notification workflows and internal escalation mechanisms to ensure timely and proper breach reporting.

10. Sector-Specific Requirements and Standardised Compliance Templates

The Decree introduces more specific and tailored compliance requirements for businesses operating in certain regulated sectors and technology-driven areas, including finance, banking, credit information services, and activities involving big data, artificial intelligence, blockchain, virtual environments and cloud computing.

Separately, the Ministry of Public Security has revised, supplemented and annexed a complete set of standardised reporting and compliance templates to the Decree, which are intended to support implementation of the PDP Law and the Decree in practice.

11. Conclusion

Overall, the Decree represents the great effort of the Vietnamese Government to introduce a more structured, enforceable and comprehensive PDP legal framework in Vietnam. Businesses should use the remaining transition period to reassess data classification, consent mechanisms, transfer arrangements and internal governance structures to ensure readiness for full compliance by 1 January 2026.

At the same time, it should be noted that the administrative sanctioning decree for PDP has not yet been issued. This provides businesses with some flexibilities to review, strengthen and complete their compliance frameworks before the issuance of the PDP sanctioning decree.

For further information or assistance in understanding the implications of the Decree, please contact:

Minh Nguyen / Special Counsel
minh.nguyen@acsvlegal.com

Ly Nguyen / Associate
ly.nguyen@acsvlegal.com