Client Alert

01-2026

VILAF

VIETNAM INTERNATIONAL LAW FIRM

VIETNAM'S NEW PERSONAL DATA PROTECTION DECREE: KEY COMPLIANCE REQUIREMENTS EFFECTIVE IMMEDIATELY

ESKO CATE AND NHAN HO, VILAF

On 31 December 2025, the Vietnamese Government issued Decree No. 356/2025/ND-CP ("Decree 356"), implementing the Law on Personal Data Protection. Decree 356 sets out detailed guidance on personal data governance, accountability duties, and regulatory supervision.

Decree 356 took effect immediately on 1 January 2026, and introduces extensive compliance obligations for all organizations and individuals that control or process personal data in Vietnam, replacing the previous key guiding regulation, Decree No. 13/2023/ND-CP.

This update focuses on the key components of Decree 356, highlighting the regulatory changes and compliance obligations that organizations should prioritize immediately from an implementation and risk-management perspective.

A. Exercise of data subjects' rights

Decree 356 requires controllers and controller-processors to maintain clear procedures and methods by which data subject can exercise their rights. It sets a multi-tiered requirement that data controllers and data controllers-processors respond to requests for the exercise of rights by data subjects within 02 working days, then carry out the relevant procedure to observe the data subject's rights within an additional specified timeframe. Details relating to the specific timeframes are set out in the table below.

Request from data subjects	Obligations of data controllers/processors	Extension of timeline
Withdraw consent, restrict or object to processing	• Respond within 2 business days • Provide full information on procedures and fulfill the request within 15 days • If third party is involved, fulfill the request within 20 days	• One extension allowed, maximum 15 days • Must notify data subject and justify necessity
View, edit, or request correction or provision of personal data	• Respond within 2 business days • Provide full information on procedures and fulfill the request within 10 days • If third party is involved, fulfill the request within 15 days	• One extension allowed, maximum 10 days • Must notify data subject and justify necessity
Request deletion of personal data	• Respond within 2 business days • Provide full information on procedures and fulfill the request within 20 days • If third party is involved, fulfill the request within 30 days	• One extension allowed, maximum 20 days • Must notify data subject and justify necessity
Request protection measures for personal data	• Respond within 2 business days • Provide full information on procedures and fulfill the request within 15 days	• One extension allowed, maximum 15 days • Must notify data subject and justify necessity

From a practical standpoint, organizations must implement structured, trackable request-handling workflows capable of meeting both the initial acknowledgement requirement and the separate completion deadlines.

B. Contractual and internal control requirements for Personal Data transfers

Decree 356 requires that any transfer of personal data by a data controller, controller-processor, or processor to another organization or individual for further processing (External Transfers) must be conducted under a written transfer agreement with the recipient. The transfer agreement must address the key compliance terms for the transfer, including purpose, data scope, retention and deletion, legal basis, security responsibilities, handling of data subject rights, and breach coordination. Where sensitive personal data is transferred, Decree 356 requires additional safeguards for the transfer, including physical security measures and technical protections such as encryption and anonymization.

For internal sharing of personal data between departments within the same organization (Internal Transfers), Decree 356 requires that organizations have internal control procedures governing the sharing of the personal data, and measures to prevent personnel from unlawfully disclosing personal data to third parties.

To ensure compliance, organizations should review any data flows where personal data is currently being sent outside the organization and ensure each transfer is covered by a compliant written transfer agreement. Additionally, organizations should work with their IT departments to ensure that suitable safeguards are applied for any transfers involving sensitive personal data. In parallel, organizations should review and enforce internal procedures for sharing personal data between departments, to ensure that sufficient controls exist to prevent unauthorized disclosure to third parties.

C. Data processing & outbound transfer impact assessment dossiers

Decree 356 provides extensive clarity on the obligations of organizations and individuals in relation to the preparation and submission of impact assessments. Additionally, it expands the content requirements and provides new forms for preparation and submission.

As before, organizations controlling or processing personal data must prepare and retain a data processing impact assessment dossier from the start of personal data processing activity. The dossier must be submitted within 60 days from the start of personal data processing and must be available for inspection by the data protection authority.

In addition, under Decree 356, an organization must prepare and submit a cross-border transfer impact assessment dossier in the following scenarios:

a. Transfer of personal data collected or stored in Vietnam to servers located outside of Vietnam or to foreign cloud service providers;

b. Transfer of personal data from Vietnamese organizations or individuals to foreign recipients; or

c. Processing of personal data collected in Vietnam on platforms outside of Vietnam.

The cross-border transfer impact assessment dossier must be available for inspection by the data protection authority and must be submitted within 60 days from the date of transfer of personal data.

Decree 356 exempts certain activities from cross-border transfer impact assessment requirements, including cross-border personnel management, cross-border transfers to fulfill legal obligations, or cross-border transfers to execute contracts or conduct procedures related to cross-border transportation, logistics, remittance, payment, hotel booking, visa application, or scholarship application.

Decree 356 further clarifies the requirement set out in the Personal Data Protection Law that the dossiers must be reviewed and updated every six months from the initial submission if there are new purposes for data transfer or processing, or if there are changes in the data controller, processor, or third parties involved. Immediate updates are required within 10 days in cases such as organizational restructuring, dissolution, bankruptcy, changes in data protection service providers, or changes in registered business lines related to personal data processing.

Under the new forms included in Decree 356, it is clear that the authorities expect organizations and individuals to provide extensive information about their data flows, processes, and internal controls. Moreover, Decree 356 specifies that the applicable agency will now review the sufficiency of the submitted impact assessment dossier and issue an assessment result.

Organizations should immediately review their current impact assessment submissions and prepare to update them for compliance with the new forms under Decree 356. Where gaps are identified, organizations should immediately begin the process of rectification. Moreover, organizations that do not already have mechanisms in place to review and update on a regular schedule should develop and implement measures for continuing compliance.

D. Data breach notification

Personal data controllers and processors must notify the data protection authority within 72 hours of discovering any personal data breach that could harm the interests of Vietnam or of the data subjects. If a processor detects a breach, it must promptly inform the controller.

Notifications must be sent to the data protection authority either directly or via the national personal data protection portal, using the prescribed form. In addition, personal data controllers and processors must document the breach and cooperate with the authority in handling the incident.

Decree 356 sets out additional, exceptional notification requirements. Data controllers and processors in the fields of finance, banking or credit information must notify both:

a. the specialized agency responsible for personal data protection, and

b. the affected data subjects

within 72 hours after discovering any disclosure or loss of sensitive personal data. This requirement is extended to any data controller or controller-processor in cases of breaches involving biometric or location data, regardless of the field of operation. Additional requirements further apply in these cases.

E. Data protection officer (DPO) and data protection department (DPD)

Decree 356 introduces new requirements for data protection officers ("DPO") and data protection departments ("DPD"). Specifically, DPOs must have at least a college degree, a minimum of two years' experience working in fields of legal, IT, cyber security, data security, risk management, compliance, human resource management, or personnel organization, and must have completed training in personal data protection law and skills. If a DPD is established, all members must meet the requirements for DPOs.

Decree 356 expressly acknowledges the ability for organizations to engage outsourced DPOs or DPDs to satisfy personal data protection obligations and specifies requirements for individuals and organizations that provide these services.

An individual offering services as a DPO must have at least a college degree, a minimum of three years' experience in the fields of legal, personal data processing, cybersecurity, data security, risk management, or compliance control, and must have completed specialized training in personal data protection law and skills. Organizations offering PDP services must have either technology or legal business lines, must have relevant expertise, employ at least three qualified personnel, and have provided data protection-related services.

F. Data processing services and new, conditional business lines

Under Decree 356, data processing services are defined to include a wide range of activities, such as provision and operation of automated personal data processing systems and software, online data collection, data analytics and mining, and data encryption services. Service providers providing these services must meet requirements set out in Decree 356, including among others (a) being a Vietnamese entity, (b) obtaining a certificate for data processing services from the Ministry of Public Security, and (c) fulfilling various personnel, technical, and operational requirements.

G. Enforcement and supervisory powers under Decree 356

Decree 356 makes clear that personal data protection compliance will be supervised through regular and ad hoc inspections, including where there are grounds to suspect a violation, where an authorized body directs an inspection, or as part of routine state management. The inspection scope is broad and expressly includes an organization's current state of compliance, its preparation and maintenance of impact assessment (including cross-border transfer impact assessments), and the provision of personal data processing services.

Decree 356 substantially expands the legal framework for personal data protection in Vietnam, placing additional requirements on organizations and individuals that control or process personal data. Organizations must carefully review and implement data protection measures and ensure readiness for regulatory inspections. For guidance or questions regarding your obligations under Decree 356, please contact us at tung@vilaf.com.vn.

FOR MORE INFORMATION PLEASE CONTACT:

VILAF
VIETNAM INTERNATIONAL LAW FIRM

Esko Cate
Senior Associate
World Law Group Privacy & Data Protection Co-Chair
esko.cate@vilaf.com.vn

Nhan Ho
Associate
nhan.ho@vilaf.com.vn