CDLAF
YOUR CONFIDANT

/2026

CROSS-BORDER PERSONAL DATA TRANSFERS:

WHAT ENTERPRISES SHOULD KNOW

PART 2: WHAT SHOULD ENTERPRISES DO WHEN ENGAGING IN CROSS-BORDER PERSONAL DATA TRANSFERS?

Authors:

Ha Lu Chi Đat
Senior Associate

Pham Thi Hoai
Senior Paralegal

info@cdlaf.vn +84 909 668 216 cdlaf.vn | /cdlaflawfirm

PART 2: WHAT SHOULD ENTERPRISES DO WHEN ENGAGING IN CROSS-BORDER PERSONAL DATA TRANSFERS?

In **Part 1**, we clarified the technical and legal criteria for determining when the use of cloud computing services provided by foreign service providers (AWS, Azure, Google Cloud, etc.) gives rise to the obligation to carry out the impact assessment procedure for cross-border personal data transfers, as well as the applicable exceptions. Once an enterprise has accurately determined its compliance obligations, what personnel, technical, and internal governance documentation should it prepare to meet the requirements of the competent authorities? Will an enterprise incur any penalties if it delays compliance? CDLAF will address all of these issues in Part 2 below.

1. What Should an Enterprise Do When Engaging in Cross-Border Personal Data Transfers?

In general, the law requires agencies, organizations and individuals engaged in cross-border personal data transfers to prepare an impact assessment report within 60 days from the date on which such activities commence. Accordingly, once an enterprise determines that it engages in cross-border personal data transfers, it may refer to the following basic steps:

Step 1: Establish a Data Flow Map and Determine the Legal Status of the Parties Involved in Data Processing Activities

This is the foundational step that determines the accuracy of the entire dossier. If the data flows are incorrectly identified or the legal roles of the parties are misunderstood from the outset, the enterprise will have to revise its entire risk assessment system and contractual commitments. The enterprise should address the following three core matters:

- Scope and Establish the Data Flow Map: The enterprise needs to identify in detail each type of personal data that may be transferred across borders, including whether any sensitive personal data are involved, the origin of the data, the physical means or platforms and software through which the data will be transferred across borders, the geographical location of the servers receiving and processing the personal data, etc.
- What is the purpose of transferring personal data across borders? This is necessary to determine whether the cross-border transfer of personal data falls within the scope of the applicable procedural requirements. The enterprise should determine whether the Vietnamese company transfers personal data across borders to provide information to its parent company, provide information to business partners for other business-related purposes, store data such as through secure backups on cloud computing infrastructure, operate an international ERP system, or for other purposes.

- Accurately Determine the Legal Status of the Relevant Parties: The enterprise needs to identify and assess, against applicable personal data protection laws, whether the Vietnamese party is the Personal Data Controller, Personal Data Processor, or both the Personal Data Controller and Processor. At the same time, the enterprise must determine whether the foreign recipient receiving personal data from the Vietnamese enterprise is an independent third party, a parent or subsidiary within the same group, and what role the foreign party assumes under personal data protection laws.

Step 2: Prepare the Impact Assessment Dossier

The enterprise needs to prepare the impact assessment dossier for cross-border personal data processing in accordance with the law. One matter that should be prepared at an early stage is information concerning the person or department in charge of personal data protection. Such person or department may be appointed internally by the enterprise or outsourced to a qualified organization or individual. The enterprise should also take note of the requirement that the responsible personnel receive training and further education in personal data protection. At this stage, the enterprise should focus on two core components:

Decision on the Selection of Personnel / Personal Data Protection Department (DPO Setup): *Accordingly, the enterprise may choose one of the following two models:*

- **In-house DPO Model:** Issue an official appointment decision by the Legal Representative. Such personnel must complete a training and further education program on personal data protection as prescribed by law.
- **Outsourced Model (DPO-as-a-Service):** Enter into a service agreement with an organization, law firm, or specialized service provider. This option optimizes the enterprise's operating costs and ensures objectivity and independence in compliance monitoring.

Standardize the Technical Contents of the Impact Assessment Dossier:

- **Identification of the Legal Status and Information of the Parties:** Fully identify the legal information of the Vietnamese Data Exporter and the foreign Data Importer (the parent company or an international SaaS/Cloud service provider).

- **Description of the Purpose and Data Flow:** Clearly explain why the data processing activity must be carried out on servers located outside the territory of Vietnam and cannot be processed entirely within Vietnam.
- **Technical and Information Security Measures Statement:** Provide a detailed description of technical measures for data protection, including encryption standards for data in transit and at rest, encryption key management mechanisms, least-privilege access control policies, and System Log recording procedures.

One of the current challenges for most enterprises may be the financial cost of compliance. In implementing personal data protection requirements, the first cost to consider is the cost of DPO personnel. An enterprise cannot simply assign any employee to concurrently perform the DPO role pursuant to an internal decision; such personnel must have completed specialized DPO training. Nevertheless, even when a company arranges for an employee to attend relevant training courses, it may still be difficult to have that employee concurrently assume the DPO role. This stems from the significant responsibilities attached to the position, particularly where data leakage incidents occur or where the company is found to have violated personal data protection compliance requirements, in which case the DPO may bear a certain degree of responsibility.

Step 3: Finalize Relevant Documents and Policies

The Impact Assessment Dossier is merely an administrative procedural document submitted to A05. Along with the report, the enterprise must ensure that it has all policies and procedures required by law in order to be duly qualified to process personal data. In principle, the following key documents are required:

- **Personal Data Protection Policy:** The policy is set out in the company's internal regulations, which allocate data access rights, establish endpoint security standards, and define the confidentiality responsibilities of internal personnel, etc. For documents entered into between the enterprise and third parties, such as employees, customers, and partners, additional contractual clauses or annexes should be included to record the company's commitments and agreements regarding the relevant personal data processing. Enterprises operating e-commerce platforms should also note that they will need to revise their Terms of Use, Privacy Policy, user consent provisions, etc.

- **Data Flow Diagram:** Digitize the data flow map, from the data collection point in Vietnam, through secure transmission protocols (API, TLS-encrypted connections), to the geographical location of the primary data storage server (Primary Server), etc. Establish a list of specific data fields (basic or sensitive personal data) corresponding to each data receiving point overseas.
- **Standard Forms and Operating Procedures:** A set of forms for receiving and processing requests from data subjects (withdrawal of consent, requests for deletion, restriction of processing, or provision of copies of data). An emergency data security incident response and handling procedure (Incident Response Plan), clearly allocating the roles of the DPO, IT/Security Department, and Executive Management in the event of data leakage or exposure risks.

Step 4: Submit the Dossier to the Competent Authority

After finalizing the dossier, the enterprise shall submit it accordingly. Specifically, the enterprise must submit one official dossier to the Department of Cybersecurity and Hi-Tech Crime Prevention (A05 – Ministry of Public Security) within 60 days from the date on which the data transfer activity commences. The originals of the entire impact assessment dossier, supporting documents, and DPA must always be maintained at the enterprise's premises for inspection and post-inspection purposes.

Step 5: Monitor the Processing Results, Coordinate in Providing Explanations, and Maintain Post-Inspection Compliance Status

After submitting the dossier, the enterprise's obligations do not end upon receipt of the submission acknowledgment, but move to the stage of coordinating with the assessment process and managing actual operational risks: proactively monitor the status of dossier processing and ensure that dedicated personnel are ready to respond when requests for clarification are received.

Establish and Maintain the Dossier at the Enterprise's Headquarters: The enterprise is required to retain one original dossier (in both hard-copy and electronic form) at its head office, including the official impact assessment dossier, a copy of the DPA, evidence of user consent, and internal security policies. The competent authority may conduct ad hoc or periodic inspections. The dossier retained by the enterprise must always accurately reflect the

actual infrastructure and data flows in operation.

The enterprise should note that the dossier must be periodically updated upon changes such as: changes to or addition of Cloud/SaaS providers; changes to server infrastructure configurations or the geographical location of data centers; expansion of the scope of collection or transfer of additional sensitive personal data fields (payment data, biometric data, health records); corporate restructuring, mergers, or changes to the data recipient within the foreign parent group, etc.

2. What Cases Are Exempt from the Cross-Border Personal Data Transfer Impact Assessment?

Not every cross-border personal data transfer is subject to an impact assessment dossier. Pursuant to Clause 6, Article 20 of the Personal Data Protection Law 2025 and Clause 3, Article 17 of Decree No. 356/2025/ND-CP, certain cases are not subject to the regulations on cross-border personal data transfer impact assessments, including:

- Cross-border transfers of personal data by competent state authorities;
- Agencies and organizations storing personal data of their employees on cloud computing services;
- Data subjects transferring their own personal data across borders;
- Press and media activities in accordance with the law;
- Cross-border personal data transfers that have been made public in accordance with the law;
- Emergency cases where it is genuinely necessary to provide personal data across borders to protect an individual's life, health, or property safety, or to perform duties and obligations as prescribed by law;
- Cross-border personal data transfers for cross-border human resources management in accordance with labor rules, regulations, and collective bargaining agreements as prescribed by law;
- Provision of personal data across borders for entering into contracts or carrying out procedures relating to cross-border transportation, logistics, remittances, payments, hotel services, visa applications, or scholarship applications.

Accordingly, enterprises should assess both the data transfer activities and applicable exemptions, rather than assuming that every overseas data transfer requires an impact assessment dossier.

However, an exemption from the impact assessment requirement does not exempt enterprises from other personal data protection and processing obligations, including data flow mapping, determining the legal status of relevant parties, and maintaining necessary policies.

3. Legal Risks and Business Losses for Failure to Submit the Dossier on Time

On 19 August 2026, the Government issued Decree No. 330/2026/ND-CP on administrative penalties for violations in cybersecurity and personal data protection, effective the same day.

Accordingly, preparing and submitting a cross-border personal data transfer impact assessment report is no longer optional or something enterprises can indefinitely postpone.

Under the Decree, penalties may be imposed as fixed amounts or percentages of revenue, depending on the violation.

Fine	Violation
VND 30,000,000 to **VND 50,000,000**	• Failure to prepare the impact assessment dossier for cross-border personal data transfers before or during the transfer of data; • Failure to periodically update the impact assessment dossier for cross-border personal data transfers or to update it when changes occur as prescribed by law; • Failure to maintain the impact assessment dossier for cross-border personal data transfers in a state of readiness for inspection by the specialized personal data protection authority ...

PART 2: WHAT SHOULD ENTERPRISES DO WHEN ENGAGING IN CROSS-BORDER PERSONAL DATA TRANSFERS?

Fine	Violation
VND 50,000,000 to **VND 100,000,000**	• Failure to establish a contract or transfer document binding the data exporter and data importer to personal data protection responsibilities, or failure to clearly determine responsibilities for exercising data subjects' rights after the data has been transferred; • Failure to ensure the data subject's consent to the purpose of the cross-border personal data transfer, or failure to notify the data subject that their data is being transferred overseas, the identity of the recipient, and the processing purpose; • Failure to apply appropriate security measures during the cross-border transfer of personal data or failure to have a plan to ensure personal data security after the transfer ...
1%–2% of the preceding fiscal year's annual revenue in Vietnam	• Conduct resulting in the disclosure or loss of personal data of 10,000 to fewer than 100,000 data subjects who are Vietnamese citizens.
2%–3% of the preceding fiscal year's annual revenue in Vietnam	• Conduct resulting in the disclosure or loss of personal data of 100,000 to fewer than 1,000,000 data subjects who are Vietnamese citizens.
3%–5% of the preceding fiscal year's annual revenue in Vietnam	• Conduct resulting in the disclosure or loss of personal data of 1,000,000 or more data subjects, or cross-border transfer of personal data after the specialized personal data protection authority has issued a decision requiring the transfer to cease, causing harm to national defense or national security, and certain other specific cases.

PART 2: WHAT SHOULD ENTERPRISES DO WHEN ENGAGING IN CROSS-BORDER PERSONAL DATA TRANSFERS?

Accordingly, where an enterprise has determined that its use of cloud computing services constitutes a cross-border personal data transfer activity, it must carry out the necessary compliance steps in accordance with the law to avoid penalties.

CDLAF

YOUR CONFIDANT

OUR ECOSYSTEM

invest

OFFICE LEASING

CFT

CORPORATE COMPLIANCE

Head Office: R7.01, Transimex Building, 172 Hai Ba Trung Str., Tan Dinh Ward, Ho Chi Minh City, Vietnam.

Branch Office: 330 Nguyen Van Troi Str., Phu Loi Ward, Ho Chi Minh City, Vietnam.

Transaction Office: 101/20 Street 11, Thu Duc Ward, Ho Chi Minh City, Vietnam.

info@cdlaf.vn +84 909 668 216 cdlaf.vn | /cdlaflawfirm