

CROSS-BORDER PERSONAL DATA TRANSFERS: WHAT BUSINESSES SHOULD KNOW

PART 1: IDENTIFYING CROSS-BORDER PERSONAL DATA TRANSFER ACTIVITIE

Authors:



Ha Lu Chi Đạt
Senior Associate



Pham Thi Hoai
Senior Paralegal

CROSS-BORDER PERSONAL DATA TRANSFERS: WHAT BUSINESSES SHOULD KNOW



With the rapid advancement of technology and the increasing adoption of digital transformation initiatives among Vietnamese enterprises, the use of outsourced servers and third-party cloud computing platforms, as an alternative to on-premises servers or traditional paper-based storage systems, has become commonplace. According to statistics published by Vietnam's Ministry of Information and Communications in 2022, foreign cloud computing service providers accounted for nearly 80% of the cloud services market share in Vietnam. Among these providers, Amazon Web Services ("AWS") held approximately 33% of the market, while Microsoft Azure and Google Cloud each accounted for approximately 21%¹. Among these major providers, AWS is currently the only provider that has publicly announced plans to deploy servers and infrastructure in Hanoi, Vietnam by 2026², while Google has announced plans to establish a data center in Ho Chi Minh City³. To date, no official information has been released regarding the establishment of servers or data centers in Vietnam by the remaining providers. This demonstrates that a significant portion of server and cloud computing services available to users in Vietnam continues to be delivered through infrastructure located outside Vietnam.

This raises important compliance considerations for Vietnamese enterprises that utilize outsourced server services and cloud computing solutions. A key question is whether storing data through services provided by AWS, Google Cloud, or Microsoft Azure constitutes a cross-border transfer of personal data under Vietnamese law. This article aims to provide readers with an overview of circumstances that may be classified as cross-border personal data transfers, as well as the legal obligations applicable to organizations operating in Vietnam that engage in such activities.

1. Which Activities Constitute Cross-Border Personal Data Transfer?

Vietnamese law does not provide a standalone definition of the term "cross-border transfer of personal data." Instead, the concept is identified through specific personal data processing activities. Pursuant to Article 20.1 of the Law on Personal Data Protection 2025 and Article 17.1 of Government Decree No. 356/2025/ND-CP guiding the implementation of the Law on Personal Data Protection, cross-border personal data transfer encompasses the following circumstances:

Scenario 1: Transferring Personal Data Stored in Vietnam to Storage Systems Located Overseas

CROSS-BORDER PERSONAL DATA TRANSFERS: WHAT BUSINESSES SHOULD KNOW



Examples: A Vietnamese company collects and stores customer information on a server system located in Vietnam, and subsequently transfers such data to AWS servers in Singapore for storage and backup purposes; A hospital in Vietnam stores patient records on domestic systems but utilizes cloud computing services provided by a foreign vendor to automatically back up data on servers located in Japan.

In these circumstances, **the Vietnam-based agency, organization, or individual** responsible for the cross-border transfer is required to prepare and maintain a Cross-Border Personal Data Transfer Impact Assessment Dossier in accordance with applicable regulations.

Scenario 2: Transferring Personal Data to Foreign Organizations or Individuals

Examples: A Vietnamese company collects customers' personal data and sends such information to its parent company in Japan for business operations; A Vietnamese enterprise engages a payroll service provider in Japan and periodically transmits employees' personal data to that service provider for payroll administration purposes.

In these circumstances, **the Vietnam-based agency, organization, or individual** is required to conduct and maintain a Cross-Border Personal Data Transfer Impact Assessment Dossier.

Scenario 3: Using Overseas Platforms to Process Personal Data Collected in Vietnam

Example: A Vietnamese company collects customer information through its website. The collected data is then automatically transferred to a Salesforce CRM system hosted in the United States for purposes such as customer segmentation, consumer behavior analysis, transaction history management, and marketing activities.

For this scenario, both the Vietnamese entity and the foreign organization or individual involved in the personal data processing activities are required to prepare and maintain a Cross-Border Personal Data Transfer Impact Assessment Dossier.

CROSS-BORDER PERSONAL DATA TRANSFERS: WHAT BUSINESSES SHOULD KNOW



2. Does the Use of AWS, Google Cloud, or Microsoft Azure Constitute Cross-Border Personal Data Transfer?

The use of cloud computing services provided by AWS, Google Cloud, or Microsoft Azure may involve cross-border personal data transfer activities. To determine whether such activities fall within the scope of cross-border personal data transfer, businesses should assess whether there exists a flow of personal data originating from Vietnam and being transferred abroad based on the following three criteria:

(i) Does the Service Usage Involve the Processing of Personal Data?

Cloud computing services may be used for various purposes, including the storage and processing of different categories of information. Accordingly, a business should first determine whether any personal data is being processed through the relevant service.

(ii) Does the Personal Data “Originate” from Vietnam?

In all three scenarios described in Section 1 above, the point of origin of the personal data is Vietnam. Specifically, the personal data may be data stored in Vietnam as described in Scenario 1, personal data held by agencies, organizations, or individuals in Vietnam as described in Scenario 2, or personal data collected in Vietnam but subsequently processed through a platform located overseas.

(iii) Is the “destination” a foreign server, platform, organization, or individual?

A common element among all three cross-border personal data transfer scenarios described in Section 1 is the existence of a destination outside Vietnam. Such destination may be an overseas server used for data storage as described in Scenario 1, a foreign organization or individual receiving the personal data, or an overseas platform used to process personal data collected in Vietnam.

As mentioned above, AWS is currently the only provider that has publicly announced the deployment of servers in Hanoi, Vietnam, while the remaining providers have not publicly disclosed any information regarding the establishment of servers or data centers in Vietnam. Accordingly, before and during

CROSS-BORDER PERSONAL DATA TRANSFERS: WHAT BUSINESSES SHOULD KNOW



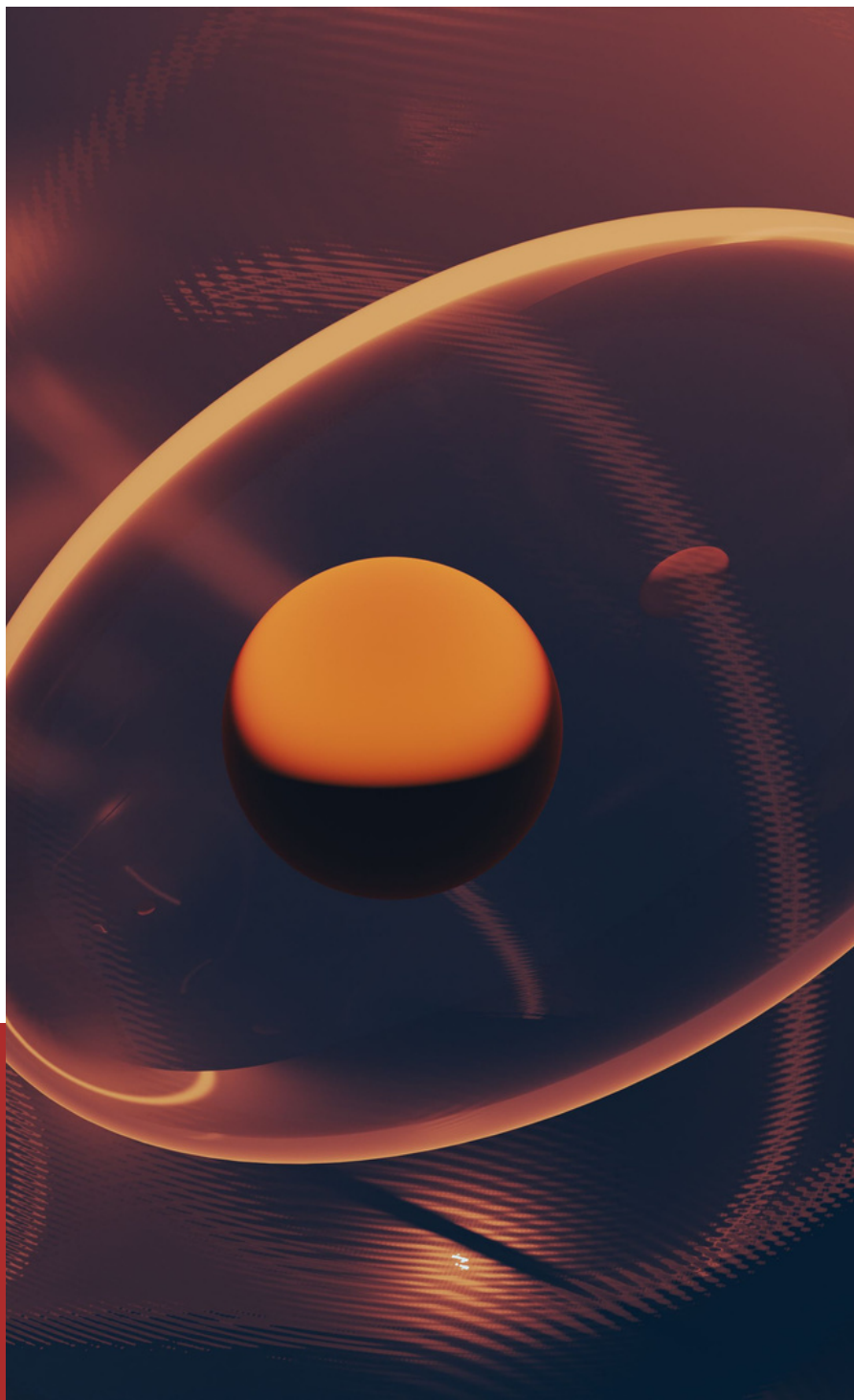
the use of such services, businesses should verify and obtain confirmation from the service provider regarding the location of the servers where the data will be stored and processed.

If the answer to all three criteria above is “yes” when using AWS, Google Cloud, or Microsoft Azure services, it may be concluded that a cross-border transfer of personal data is taking place.

For example, where personal data is collected and stored in Vietnam and is subsequently transferred to a server system located outside the territory of Vietnam, or to a cloud computing service provided by a foreign service provider whose servers are also located outside the territory of Vietnam, such activity falls within the scope of cross-border personal data transfer under Article 20.1 of the Law on Personal Data Protection 2025 and Article 17.1 of Decree No. 356/2025/ND-CP. Conversely, if a business uses cloud computing services provided by a foreign service provider but the data is stored and processed entirely on systems located in Vietnam, and there is no transmission of, or access granted to, such data outside the territory of Vietnam, such activity would not be regarded as a cross-border transfer of personal data.

Correctly identifying the nature of a cross-border personal data transfer, as discussed in Part 1, is an important first step. The real challenge, however, lies in determining what documentation businesses must prepare, how a Data Processing Agreement (DPA) should be negotiated and executed with business partners, and how a Data Protection Officer (DPO) function should be managed to obtain valid approval within the statutory 60-day period.

In **Part 2: What Should Businesses Do When Engaging in Cross-Border Personal Data Transfer Activities?** CDLAF will provide a detailed guide to a practical five-step compliance roadmap and analyze the risks associated with violations of personal data protection regulations under Decree No. 330/2026/ND-CP. Through this discussion, we aim to assist businesses in anticipating potential compliance issues and, in turn, reassessing their internal risk management frameworks.



OUR ECOSYSTEM



OFFICE LEASING



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