CDLAF
YOUR CONFIDANT

/2025

INTERNAL GUIDELINES ON IMPACT AND RISK ASSESSMENT UNDER VIETNAMESE DATA LAW

Head Office: Room 7.01, TMS Building, 172 Hai Ba Trung Str., Tan Dinh Ward, Ho Chi Minh City, Vietnam.

Branch Office: 330 Nguyen Van Troi, 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 (28) 3636 5486
cdlaf.vn

/cdlaflawfirm

INTERNAL GUIDELINES ON IMPACT AND RISK ASSESSMENT UNDER VIETNAMESE DATA LAW

This material is designed to provide detailed and consistent guidance for internal Enterprises on conducting four types of material compliance assessments under the Data Law and related decrees, and is based on the time when Decree 13/2023/ND-CP on personal data is in effect. Strict compliance with the procedures outlined below is a mandatory requirement to ensure that all activities of the organization are in accordance with the law, protect strategic data assets and minimize legal risks.

Key Definitions

To effectively use this guide, Enterprises need to understand the following legal definitions:

- **Important Data**: Data that may affect national defense and security, foreign affairs, macroeconomic situations, social stabilization, and community health and safety, included in the list promulgated by the Prime Minister. *(According to Article 3 of the Data Law)*

- **Core Data**: that directly impact national defense and security, foreign affairs, macroeconomic situations, social stabilization, and community health and safety, included in the list promulgated by the Prime Minister. *(According to Article 3 of the Data Law)*

- **Personal Data Controller**: Is an organization or individual that decides the purpose and means of processing personal data. *(According to Article 2 of Decree 13/2023/ND-CP)*

- **Personal Data Processor**: An organization or individual that processes data on behalf of the Data Controller, via a contract or agreement with the Data Controller. *(According to Article 2 of Decree 13/2023/ND-CP)*

How to Use This Guide

Before undertaking any data processing activity, Enterprises must undertake a data classification step to determine the respective compliance obligations. An activity may involve multiple data types, so it is necessary to check against all relevant definitions (Personal Data, Important Data, Core Data). The summary table below provides an overview for quick comparison of requirements.

Assessment Type	Legal Documents	Applicable Data Types	Subject of Implementation	Time of Filing	Filing/Notification Obligation	Frequency
I. Assessment of cross-border transfer and processing impacts	Data Law & Decree 165/2025/ND-CP	Core Data, Important Data	Data owner, data governing bodies	**Before** performing	**Core**: Submit and wait for approval. **Important:** Submit notice **15 days in advance.**	Once, updated when changes occur
II. Internal processing risk assessment	Data Law & Decree 165/2025/ND-CP	Core Data, Important Data	Data governing bodies	Periodic	Prepare documents for inspection.	Annual
III. Assessment of the impact of processing Personal Data	Decree 13/2023/ND-CP	Personal Data	Controller, Processor, Controller and Processor party	**Since** start processing	Submit within **60 days** of processing start date.	Once, updated when changes occur
IV. Assessment of the impact of cross-border transfers of Personal Data	Decree 13/2023/ND-CP	Personal Data of Vietnamese Citizens	The party transferring data abroad	**Before** performing	Submit within **60 days** of processing start date.	Once, updated when changes occur

Note on Overlapping Obligations: A data processing activity may be subject to multiple regulations at the same time. For example, the transfer of customer financial data abroad may be both a "cross-border transfer of personal data" (Section IV) and a "cross-border transfer of important data" (Section I). In this case, Enterprises must prepare and submit **two separate sets of dossiers** as required by both Decree 13/2023/ND-CP and Decree 165/2025/ND-CP, complying with the specific timelines and requirements of each process.

I. ASSESSMENT OF CROSS-BORDER DATA TRANSFER AND PROCESSING IMPACTS (FOR CORE DATA & IMPORTANT DATA)

The transfer of core and important data out of Vietnam is a strategic activity, fraught with risks and strictly regulated by law. Impact assessment is a core requirement of the Law on Data, which is designed to protect the country's national interests, security and strategic information assets. Strict compliance with this process is not only a legal obligation but also an essential enterprise risk management measure.

1. Compliance Obligation Analysis

Based on Article 23 of the Data Law and Article 12 of Decree 165/2025/ND-CP, the obligation to assess the impact is stipulated as follows:

- **Subject of implementation**: Responsibility for implementation belongs to "Data owner, Data administrator".

- **Time of implementation**: An impact assessment must be completed **before** any cross-border transfer or processing of core, important data occurs.

- **Distinguishing processes:**

+ **For Core Data:** It is mandatory to send the Impact Assessment dossiers to the Ministry of Public Security (or the Ministry of National Defense for data in the military, defense, and cryptographic fields) for assessment and to receive written results. The transfer activity can only be carried out after the assessment result is "Passed".

+ **For Important Data:** The Impact Assessment File must be prepared and 01 original copy must be sent to the Ministry of Public Security (or Ministry of National Defense) 15 days before the expected date of data processing. This is a mandatory prior notification obligation, not subject to approval.

This distinction is extremely important from an operational strategy perspective. For Core Data, the **pre-approval** process can significantly impact project timelines. In contrast, for Important Data, **the pre-notification process** allows for faster implementation but still requires thorough documentation and timely submission.

2. Assessment dossiers

Pursuant to Clause 4, Article 12 of Decree 165/2025/ND-CP, the Dossier for assessing the impact of cross-border data transfer and processing includes the following mandatory components:

Dossier Components	Detailed Description
Impact Assessment Report	This is the central document of the dossier, prepared according to **Form No. 02** issued with Decree 165/2025/ND-CP.
Written Agreement	A copy of the contract or other legally enforceable agreement signed between the data transferor and the data recipient.
Legal Documents	Documents proving the legal status of the parties, including: Certificate of business registration (for organizations) or valid personal identification documents (for individuals) of both the sender and the recipient.

3. Content to be evaluated

When drafting dossiers, Enterprises must ensure thorough analysis and response to the points specified in **Clauses 2 and 3, Article 12 of Decree 165/2025/ND-CP.**

- **Contents of Impact Assessment Report (Clause 2):**

+ The legality, necessity, scope and method of the transfer activity.
+ Analyze potential risks to national defense, security, economy, society and legitimate rights and interests of organizations/individuals.
+ Assess the data protection measures that the data recipient undertakes to implement.
+ Other issues related to the transfer operation.

- **Mandatory contents of the Written Agreement (Clause 3):**

+ Purpose, method and scope of data processing.
+ Location and duration of data storage abroad.
+ Requires the recipient to take responsibility for not providing the data to any other third party.
+ Remedial measures, compensation for damages and dispute resolution.

4. Periodic assessment

According to **Clause 1 and Clause 8, Article 12 of Decree 165/2025/ND-CP:**

- Impact assessment only needs to be conducted once (01) for the entire period of operation.

- However, the organization must update and supplement the dossier when there are changes in:

+ Purpose, method, scope, type of data transferred.
+ The recipient's purposes or methods of processing the data.
+ Data retention period abroad.
+ Changes in policy, law, or the physical control of the parties may impact data security.

5. Disclaimer

Clause 11, Article 12 of Decree 165/2025/ND-CP stipulates certain exemptions from the approval obligation (for core data) and the prior notification obligation (for important data), including:

- Emergency situations to protect the life, health and property of individuals.
- Conduct cross-border human resource management in accordance with labor regulations or collective labor agreements.
- Carry out contracts related to cross-border transportation, logistics, international payments, bank account opening, visa application, inspection services.

Important Note: Even in the above-mentioned exemption cases, the organization is still obliged to submit the Impact assessment dossier to the competent authority (Ministry of Public Security or Ministry of National Defense) within **15 days** from the date of data transfer, as prescribed in **Clause 12, Article 12.**

In addition to managing data as it leaves borders, assessing the risk of handling data internally is also an important compliance requirement that needs to be focused on.

II. RISK ASSESSMENT FOR CORE DATA & IMPORTANT DATA PROCESSING

The purpose of internal risk assessments is to proactively identify, analyze and manage threats to an organization's most important data assets, as required by **Article 25 of the Data Law**. It is a foundational governance activity to ensure the integrity, confidentiality and availability of data, thereby protecting business operations and complying with the law.

1. Compliance Obligation Analysis

Pursuant to Clause 4, Article 25 of the Data Law and Clause 11, Article 17 of Decree 165/2025/ND-CP, "Owners of core data and important data" are obliged to periodically conduct risk assessments for activities of processing these types

of data within their scope of management.

2. Evaluation dossier

The required record to be prepared and stored is the "Report on risk assessment of core data and important data processing activities" according to Form No. 06 issued with Decree 165/2025/ND-CP. This record must always be available to serve the inspection activities of competent state agencies.

3. Content to be evaluated

When drafting the report, Enterprises must ensure full coverage of the following main contents according to **Clause 11, Article 17 of Decree 165/2025/ND-CP:**

- **Basic information**: Details of the data owner and contact information of the department/person responsible for data protection.
- **Description of processing operations**: Purpose, type, amount, method, scope, time and location of data storage.
- **Security management system**: Technical and administrative measures have been implemented to protect data (e.g., encryption, access control, backups).
- **Risks and incidents**: Detailed analysis of detected data security risks, incidents that occurred (if any) and measures taken to address them.
- **Other contents**: Other reporting requirements as prescribed by specialized laws.

4. Periodic assessment

The mandatory assessment frequency is **annual**, as prescribed in **Clause 11, Article 17 of Decree 165/2025/ND-CP**.

5. Disclaimer

Clause 11, Article 17 of Decree 165/2025/ND-CP stipulates a single exemption: an organisation is exempted from preparing this Risk Assessment Report if it has prepared a "**Cross-border data transfer and processing impact assessment dossier**" under Article 12 for the same activity and the same type of data in that year.

In parallel with the national data privacy regulations, Vietnamese law also has separate and equally stringent impact assessment requirements for personal data.

III. ASSESSMENT OF THE IMPACT OF PROCESSING PERSONAL DATA

The protection of personal data is at the heart of Decree 13/2023/ND-CP. Accordingly, the establishment and maintenance of a "Dossier on assessment of impact of personal data processing", commonly known internationally as Data Protection Impact Assessment (DPIA), is a fundamental legal tool to ensure that all personal data processing activities of an organization are transparent, accountable and fully compliant with the rights of data subjects.

1. Compliance Obligation Analysis

Pursuant to **Article 24 of Decree 13/2023/ND-CP,** the following subjects are obliged to establish and maintain this record **from the time of commencement of processing of personal data**:

- Personal Data Controller Party.
- Controller and Processor of Personal Data Party.
- The Personal Data Processor (in case of performance under a contract with the Controller).

2. Assessment dossier

The required dossier is the "**Dossier on assessment of impact of personal data processing**". According to **Clause 4, Article 24 of Decree 13/2023/ND-CP**, the organization must send 01 original copy of this record to the **Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention and Control)**.

3. Content to be evaluated

The impact assessment dossier must include all the contents specified in **Clause 1, Article 24 of Decree 13/2023/ND-CP**:

- Information and contact details of the Controller / Data Controller and Processor.
- Name and contact details of the employee or department responsible for protecting personal data.
- Purpose of processing personal data.
- Types of personal data processed.
- Organizations and individuals receiving data (including parties outside of Vietnam).
- In case of transfer of personal data abroad.
- Processing time; expected time to delete or destroy data (if applicable).
- Detailed description of the personal data protection measures applied.
- Assess the level of impact, consequences, possible damage and measures to minimize or eliminate that risk.

4. Periodic assessment

Important milestones to comply with according to **Article 24 of Decree 13/2023/ND-CP**:

- **First submission**: The application must be submitted to the Ministry of Public Security within **60 days** from the date of commencement of personal data processing.
- **Update**: The dossier must be updated, supplemented and resubmitted if there is any change to the previously submitted content.

5. Disclaimer

Based on the provisions of **Article 24 of Decree 13/2023/ND-CP**, the law **does not stipulates** any exemption from the obligation to prepare and submit the dossiers on assessment of impact of personal data processing.

Where the processing of personal data involves a foreign element, a separate and more detailed impact assessment will be required.

IV. ASSESSMENT OF THE IMPACT OF CROSS-BORDER TRANSFERS OF PERSONAL DATA

The transfer of personal data of Vietnamese citizens abroad is a high-risk activity and is managed particularly closely by **Article 25 of Decree 13/2023/ND-CP**. The preparation and submission of an impact assessment dossier for this activity is a legal prerequisite for being allowed to carry out.

1. Compliance Obligation Analysis

Pursuant to **Clause 1, Article 25 of Decree 13/2023/ND-CP, the "Party transferring data abroad"** (which may be the Controller, Controller and Processor, Processor, or Third Party) is obliged to prepare a Record of assessment of the impact of transferring personal data abroad.

2. Evaluation dossier

The required dossier the **"Dossier on assessment of impact of outbound transfer of personal data"**. Similar to the internal assessment, **Clause 3, Article 25 of Decree 13/2023/ND-CP** requires sending 01 original copy of this document to **the Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention and Control)**.

3. Content to be evaluated

The dossier must include all required contents according to **Clause 2, Article**

25 of Decree 13/2023/ND-CP:

1. Information and contact details of the Data Transferring Party and the Data Receiving Party.
2. Full name and contact details of the responsible organization/individual of the Data Transfer Party.
3. Describe and justify the objectives of the data processing activities after they have been transferred abroad.
4. Clearly describe the types of personal data that will be transferred.
5. Describe in detail the compliance with the provisions of Decree 13 and the personal data protection measures applied.
6. Assess the level of impact, consequences, potential unwanted damage and measures to mitigate those risks.
7. Evidence of the data subject's consent to the data transfer.
8. The document shows the obligations and responsibilities between the Data Transfer Party and the Data Receiving Party.

4. Periodic assessment

The relevant timelines and frequencies are specified in Article 25 of Decree 13/2023/ND-CP:

- **First submission**: Submit the application to the Ministry of Public Security within **60 days** from the date of data processing.
- **Notice after transfer**: Written notification must be sent to the Ministry of Public Security after the data transfer is successful.
- **Update**: Must update, supplement and resubmit documents when there is a change in the submitted content.
- **Periodic check**: Note that the Ministry of Public Security has the right to conduct an inspection of data transfer activities abroad **once a year**.

5. Disclaimer

Based on the provisions of Article 25 of Decree 13/2023/ND-CP, the law does not stipulate any exemption from the obligation to prepare and submit the Dossier on assessment of impact of outbound transfer of personal data.

/2025

OUR ECOSYSTEM:

invest

OFFICE LEASING

CFT

CORPORATE COMPLIANCE

/cdlaflawfirm