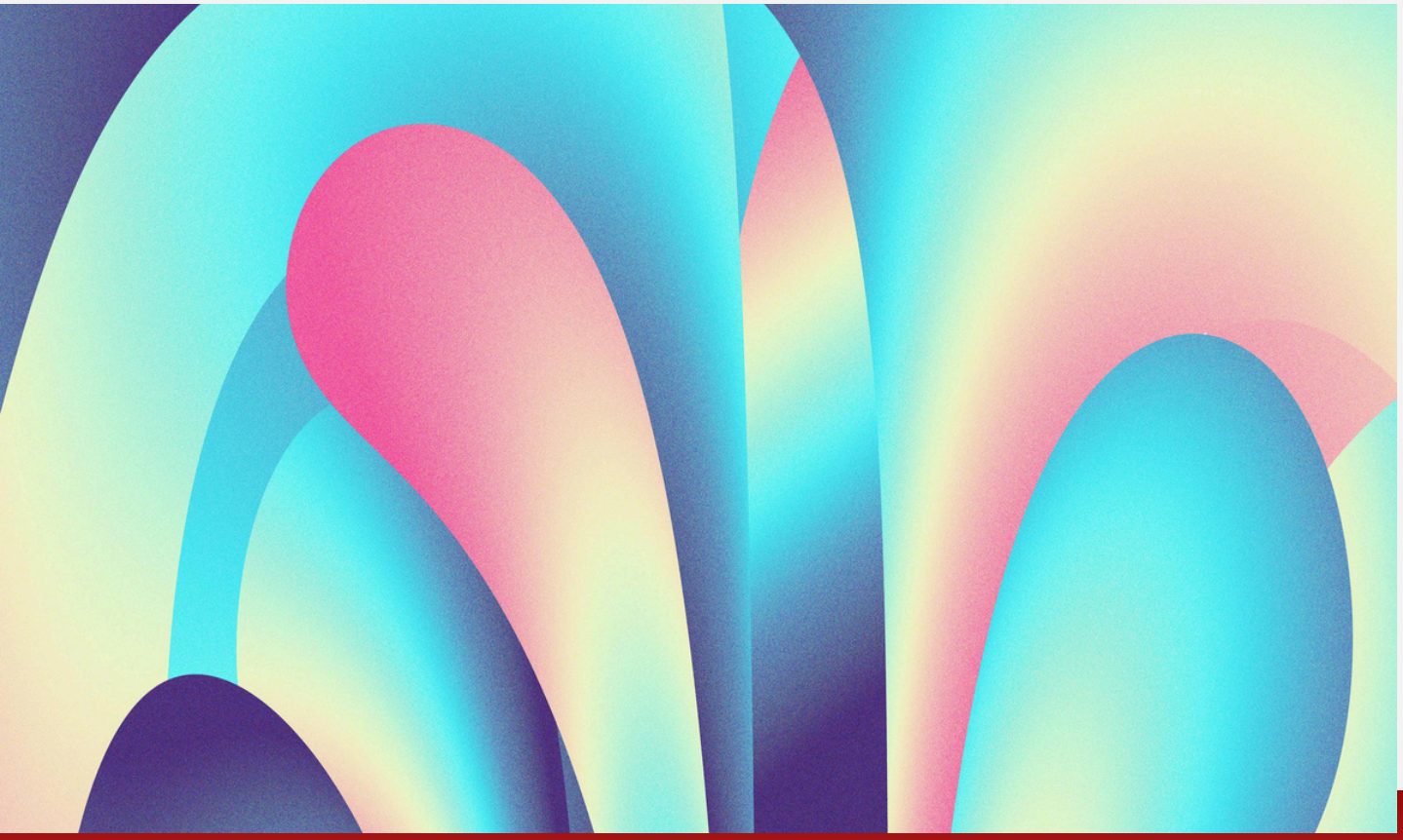
CDLAF
YOUR CONFIDANT

/2025

LEGAL NOTICE ON PERSONAL DATA EFFECTIVE JANUARY 1, 2026



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

LEGAL NOTICE ON PERSONAL DATA EFFECTIVE JANUARY 1, 2026

Effective January 1, 2026, the Law on Personal Data Protection will come into force. Concurrently, a Draft guiding decree is currently under review and is expected to be adopted in early 2026. This imposes significant responsibilities on enterprises to ensure strict compliance with the regulations established by personal data laws. These responsibilities include general compliance obligations and the specific requirement to obtain consent from personal data subjects or relevant parties prior to conducting any activities related to the collection, storage, or processing of personal data.

From CDLAF's perspective, we recommend that enterprises pay attention to the following key points:

1. Promptly supplement personal data-related clauses into contracts and agreements established between enterprises and their employees, customers, and partners, through which enterprises directly or indirectly receives, processes, stores, or controls personal data. This addition is particularly critical, as these clauses will establish the enterprises' legal rights regarding personal data matters.

2. Develop and implement appropriate management and technical measures to protect personal data, tailored to the specific needs and capabilities of enterprises.

3. Establish a system of processes, procedures, and templates to serve personal data processing activities.

Step 1: Review

- Conduct a comprehensive review of business operations to identify the types of personal data being collected, processing purposes, data subjects, departments involved in processing, and the technologies/systems currently in use.
- Review internal policies and procedures to identify regulations related to personal data processing and determine the need for amendments or supplementation.
- Review data collection activities to verify whether the notification to and obtaining consent from data subjects have been properly executed.
- Review domestic and cross-border data transfer activities and evaluate compliance with requirements regarding binding responsibilities between parties as prescribed by law.

- Review contracts and agreements with suppliers, partners, customers, etc., to determine the existence of clauses regarding personal data processing and protection, as well as necessary binding obligations.

Step 2: Based on the review results in Step 1, enterprise need to develop (where processes/procedures/templates do not yet exist) or amend and update (where processes/procedures/templates already exist) to ensure compliance with the requirements of the Law on Personal Data Protection.

Regarding agreements or contracts, enterprises should consider negotiating with relevant parties to sign an Addendum on Personal Data Processing (for executed Contracts that do not yet include these provisions) or to add clauses on Personal Data Processing that meet legal requirements (for Contracts that have not yet been signed).

4. Establishment of Personal Data Protection Personnel/Department within Enterprises

- The designation of personnel or a department for Personal Data Protection must be formalized via an official written document of enterprises. This document must clearly outline the assignment, functions, duties, authority, and other requirements regarding personal data protection activities within enterprises.
- The personal data protection personnel designated by the agency or organization must satisfy the following competency requirements:

a) Hold a college or university degree or higher;
b) Possess at least 02 years of work experience (calculated from the time of university graduation) related to one of the following fields: legal affairs, information technology, cybersecurity, data security, risk management, compliance control, human resources management, or personnel organization;
c) Hold a certificate of completion for a training course on basic or advanced knowledge and skills in personal data protection, issued by an organization qualified to provide personal data training in Viet Nam;
d) Be knowledgeable about personal data protection laws and the personal data processing activities of the agency or organization.

- In the event that enterprises establishe a Personal Data Protection department, all personnel within the department must satisfy the aforementioned competency requirements.
- In cases where enterprises do not have personnel meeting the legally required conditions, enterprises may engage an individual or organization providing personal data protection services to advise on compliance with personal data protection regulations and to perform personal data protection duties as agreed.

5. Preparation of Personal Data Processing Impact Assessment Dossier

Accordingly, Enterprises are required to:

- Establish a Personal Data Processing Impact Assessment Dossier;
- Maintain and ensure the constant availability of the Personal Data Processing Impact Assessment Dossier at the head office/office to serve inspection activities by competent authorities (if any);
- Submit 01 original copy to the specialized agency for personal data protection within 60 days from the first date of personal data processing;
- Update the impact assessment dossier periodically every 06 months when there are changes, or update immediately in cases prescribed in Clause 2, Article 22 of the Law on Personal Data Protection.

6. Preparation of Cross-Border Personal Data Transfer Impact Assessment Dossier

In the event that Enterprises engage in cross-border transfer of personal data as prescribed in clause 1, Article 20 of the Law on Personal Data Protection, Enterprises are required to:

- Establish a Cross-Border Personal Data Transfer Impact Assessment Dossier;
- Maintain and ensure the constant availability of the dossier at the head office/office to serve inspection activities by competent authorities (if any);
- Submit 01 original copy to the specialized agency for personal data protection within 60 days from the first date of the cross-border transfer of personal data;
- Update the impact assessment dossier periodically every 06 months when there are changes, or update immediately in cases prescribed in clause 2, Article 22 of the Law on Personal Data Protection.

7. Note on the Handling of Violations of Personal Data Protection Laws

- Organizations and individuals violating the provisions of the Law and other relevant regulations on personal data protection may, depending on the nature, severity, and consequences of the violation, be subject to administrative sanctions or criminal prosecution; if damages are caused, compensation must be made in accordance with the law.
- The maximum fine in administrative sanctions for the act of buying or selling personal data is 10 times the proceeds gained from the violation; in cases where there are no proceeds from the violation, or the fine calculated based on proceeds is lower than the maximum fine prescribed in clause 5, the fine level prescribed in clause 5 shall apply.

- The maximum fine in administrative sanctions for organizations violating regulations on cross-border personal data transfer is 5% of the total revenue of the preceding financial year of that organization; in cases where there is no revenue from the preceding year, or the fine calculated based on revenue is lower than the maximum fine prescribed in Clause 5, the fine level prescribed in Clause 5 shall apply.
- The maximum fine in administrative sanctions for other violations in the field of personal data protection is VND 03 billion.
- The maximum fines prescribed in clauses 3, 4, and 5 apply to organizations; for individuals committing the same violation, the maximum fine shall be one-half of the fine applicable to organizations.

The above is a summary of key points and notes from CDLAF regarding the Law on Personal Data Protection and the Draft guiding decree. In the coming time, compliance with personal data regulations will be strictly monitored by competent authorities; enterprises should take note to ensure proper implementation.

CDLAF
YOUR CONFIDANT

/2025

OUR ECOSYSTEM:

invest
OFFICE LEASING

CFT
CORPORATE COMPLIANCE

/cdlaflawfirm