THE NATIONAL ASSEMBLY

Law No. 91/2025/QH15

THE SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom - Happiness

LAW

On Personal Data Protection

Pursuant to the Constitution of the Socialist Republic of Vietnam, which had a number of articles amended and supplemented under Resolution No. 203/2025/QH15;

The National Assembly promulgates the Law on Personal Data Protection.

Chapter I

GENERAL PROVISIONS

Article 1. Scope of regulation and subjects of application

1. This Law provides for personal data and personal data protection, rights, obligations and responsibilities of related agencies, organizations and individuals.

2. This Law applies to:

a) Vietnamese agencies, organizations and individuals;

b) Vietnam-based foreign agencies, organizations and individuals;

c) Foreign agencies, organizations and individuals directly engaged or involved in personal data processing activities of Vietnamese citizens and persons of Vietnamese origin residing in Vietnam who have not yet determined their nationality and have been granted personal identification certificates.

Article 2. Interpretation of terms

In this Law, the terms below shall be construed as follows:

1. *Personal data* means digital data or information in other forms that identifies or helps identify a specific person, including basic personal data and sensitive personal data. Personal data, once de-identified, shall no longer be regarded as personal data.

2. *Basic personal data* means personal data that reflects common and identifiable personal elements, frequently used in transactions and social relations, as prescribed in the list issued by the Government.

3. *Sensitive personal data* means personal data associated with the privacy of an individual that, once infringed upon, will directly affect lawful rights and

interests of agencies, organizations or individual, as prescribed in the list issued by the Government.

4. *Personal data protection* means that agencies, organizations, and individuals employ forces, means, and measures to prevent and combat personal data infringement.

5. *Data subject* means an individual whose information is reflected by personal data.

6. *Personal data processing* means activity or activities that affect(s) personal data, such as collecting, analyzing, certifying, aggregating, encrypting, decoding, modifying, deleting, destroying, de-identifying, providing, publicizing and transferring personal data or other relevant activities that affect personal data.

7. *Personal data controller* means an agency, organization or individual that decides on the purposes and means of personal data processing.

8. *Personal data processor* means an agency, organization or individual that carries out data processing as required by a personal data controller or personal data controlling and processing party under a contract.

9. *Personal data controlling and processing party* means an agency, organization, or individual that decides on the purposes and means and directly performs personal data processing.

10. *Third party* means any organization or individual other than the data subject, personal data controller, personal data controlling and processing party, or personal data processor that is involved in personal data processing in accordance with law.

11. *De-identification of personal data* means the process of altering or removing information to create new data that cannot identify or help identify a specific person.

12. *Personal data processing impact assessment* means the analysis and evaluation of risks that may arise in the course of personal data processing in order to implement measures to mitigate risks and protect personal data.

Article 3. Principles of personal data protection

1. To comply with the Constitution, this Law, and other relevant laws.

2. Personal data may only be collected and processed within the correct scope and for specific and clear purposes, and in accordance with the law.

3. To ensure the accuracy of personal data and allowing it to be corrected, updated, or supplemented when necessary; personal data shall be stored for a period appropriate to the purpose of personal data processing, unless otherwise provided by law.

4. To synchronously and effectively implement institutional, technical, and human measures and solutions appropriate for the protection of personal data.

5. To proactive prevent, detect, deter, timely and strictly handle all acts of violation against the law on personal data protection.

6. Protection of personal data shall be associated with the protection of national and ethnic interests, serving socio-economic development, ensuring national defense, security, and foreign affairs; and shall ensure a harmonious balance between the protection of personal data and the protection of the lawful rights and interests of agencies, organizations, and individuals.

Article 4. Rights and obligations of data subjects

1. Rights of data subjects include:

a) To be informed of personal data processing activities;

b) To consent or refuse to consent or request withdraw of consent to personal data processing;

c) To access for viewing, modifying or requesting modification of the personal data;

d) To request provision, deletion, or restriction of processing of personal data; to submit objections to personal data processing;

dd) To make complaints, denunciations, initiate lawsuits, claim compensation for damage as prescribed by law;

e) To request competent agencies or agencies, organizations, and individuals involved in personal data processing to implement measures and solutions to protect their personal data in accordance with law.

2. Obligations of data subjects include:

a) To protect their own personal data by themselves;

b) To respect and protect personal data of others;

c) To provide adequate and accurate personal data in accordance with law, under contract, or when permitting the processing of their personal data;

d) To comply with the law on personal data protection and participate in the prevention and combat of personal data infringement.

3. When exercising their rights and obligations, data subjects must fully comply with the following principles:

a) To act in accordance with the provisions of law; to fulfill obligations under contracts. The exercise of rights and obligations by data subjects must be for the purpose of protecting their own lawful rights and interests;

b) Not to obstruct or hinder the exercise of legal rights and obligations by personal data controllers, personal data controlling and processing parties, or personal data processors;

c) Not to infringe upon the lawful rights and interests of the State, agencies, organizations, or other individuals.

4. Agencies, organizations, and individuals shall be responsible for facilitating, and shall not obstruct or hinder, the exercise of rights and obligations of data subjects as prescribed by law.

5. Upon receipt of a request from a data subject to exercise the rights specified in Clause 1 of this Article, the personal data controller or personal data controlling and processing party shall promptly comply within the time limit prescribed by law.

The Government shall detail this Clause.

Article 5. Application of the law on personal data protection

1. The protection of personal data in the territory of the Socialist Republic of Vietnam must comply with the provisions of this Law and other relevant laws.

2. In case laws or resolutions of the National Assembly promulgated before the effective date of this Law contain specific provisions on personal data protection that are not contrary to the principles of personal data protection as provided in this Law, such laws or resolutions shall apply.

3. In case laws or resolutions of the National Assembly promulgated after the effective date of this Law provide for personal data protection in a manner different from this Law, such laws or resolutions must specify the contents to be implemented or not to be implemented in accordance with this Law, and the contents to be implemented under such laws or resolutions.

4. Where agencies, organizations, or individuals conduct personal data processing impact assessments or cross-border personal data transfer impact assessments in accordance with this Law, they shall not be required to conduct personal data processing risk assessments or cross-border personal data transfer impact assessments as required under other laws on data.

Article 6. International cooperation on personal data protection

1. Complying with the laws of Vietnam, treaties to which the Socialist Republic of Vietnam is a contracting party, and international agreements on personal data protection, based on the principles of equality, mutual benefit, and respect for independence, sovereignty, and territorial integrity.

2. International cooperation on personal data protection includes:

a) Formulating international cooperation mechanisms to facilitate the effective implementation of the law on personal data protection;

b) Participating in mutual legal assistance on personal data protection with other countries;

c) Preventing and combating acts of infringement upon personal data;

d) Training human resources, conducting scientific research, and applying science and technology in personal data protection;

dd) Exchanging experience in the formulation and implementation of laws on personal data protection;

e) Carrying out technology transfer to serve personal data protection.

3. The Government shall specify the responsibilities for implementing international cooperation on personal data protection.

Article 7. Prohibited acts

1. Processing personal data with the purpose of opposing the State of the Socialist Republic of Vietnam; affecting national defense, national security, social order and safety; or infringing upon the lawful rights and interests of agencies, organizations, and individuals.

2. Obstructing personal data protection activities.

3. Abusing personal data protection activities to commit acts in violation of the law.

4. Processing personal data in contravention of the law.

5. Using others' personal data or allowing others to use one's own personal data to commit acts in violation of the law.

6. Buying or selling personal data, unless otherwise provided by law.

7. Appropriating, intentionally disclosing, or causing the loss of personal data.

Article 8. Handling of violations of regulations on personal data protection

1. Organizations and individuals committing violations of this Law or other relevant laws on personal data protection shall, depending on the nature, severity, and consequences of the violations, be administratively sanctioned or examined for penal liability; and, if causing damage, shall pay compensation in accordance with law.

2. Administrative sanctions for violations in the field of personal data protection shall be imposed in accordance with Clauses 3, 4, 5, 6, and 7 of this Article and the law on handling of administrative violations.

3. The maximum fine for administrative violations involving the purchase or sale of personal data shall be ten times the illicit gain from the violation; in case there is no illicit gain or the fine calculated based on the illicit gain is lower

than the maximum fine stipulated in Clause 5 of this Article, the fine shall be imposed as prescribed in Clause 5 of this Article.

4. The maximum fine for administrative violations by organizations involved in the cross-border transfer of personal data in violation of regulations shall be 5% of the organization's revenue in the preceding year; in case there is no revenue from the preceding year or the fine calculated based on the revenue is lower than the maximum fine stipulated in Clause 5 of this Article, the fine shall be imposed as prescribed in Clause 5 of this Article.

5. The maximum fine for other administrative violations in the field of personal data protection shall be VND 3,000,000,000.

6. The maximum fines stipulated in Clauses 3, 4, and 5 of this Article apply to organizations; individuals committing the same violations shall be subject to a maximum fine equal to half of the fine imposed on organizations.

7. The Government shall prescribe the method of calculating the illicit gain obtained from committing violations of the law on personal data protection.

Chapter II

PERSONAL DATA PROTECTION

Section 1

PROTECTION OF PERSONAL DATA DURING THE PERSONAL DATA PROCESSING

Article 9. Consent of data subjects

1. The consent of the data subject means the data subject permits the processing of his/her personal data, unless otherwise provided by law.

2. The consent of a data subject takes effect only when it is given voluntarily and based on full awareness of the following information:

a) Type of personal data to be processed, purpose of personal data processing;

b) The personal data controller or personal data controlling and processing party;

c) Rights and obligations of data subjects.

3. The consent of a data subject must be expressed in a clear and specific manner, in a format that can be printed or copied in written form, including also in electronic form or verifiable format.

4. The consent of the data subject must comply with the following principles:

a) Consent must be given for each specific purpose;

b) Consent must not be subject to a condition requiring agreement to other purposes beyond the agreed content;

c) Consent remains valid until the data subject changes it or as otherwise prescribed by law;

d) Silence or non-response is not regarded as a consent.

5. The Government shall detail Clause 3 of this Article.

Article 10. Request for withdrawal of consent and request for restriction of personal data processing

1. A data subject is entitled to request the withdrawal of consent for personal data processing or request the restriction of processing of his/her personal data upon suspicion concerning the scope or purpose of personal data processing, or the accuracy of personal data, except as provided in Article 19 of this Law or unless otherwise provided by law.

2. The request for withdrawal of consent or restriction of personal data processing by the data subject must be made in writing, including in electronic form or verifiable format, and shall be submitted to the personal data controller or the personal data controlling and processing party. Such requests shall be carried out in accordance with the law and the agreement between the parties.

3. The personal data controller or personal data controlling and processing party shall receive, implement, and request the personal data processor to implement the data subject's request for withdrawal of consent or restriction of personal data processing within the time limit prescribed by law.

4. The execution of the request for withdrawal of consent or restriction of personal data processing shall not apply to personal data processing activities carried out prior to the time the data subject submits such request.

Article 11. Collection, analysis, and aggregation of personal data

1. Personal data shall be collected only with the prior consent of the data subject, unless otherwise provided by law.

2. Competent Party and State agencies may analyze and aggregate personal data from data sources that are self-collected or shared, provided, transferred, exploited, or used to serve leadership, direction, state management, and socio-economic development in accordance with the law.

3. Agencies, organizations, and individuals not referred to in Clause 2 of this Article may analyze and aggregate personal data from sources of personal data that are lawfully permitted for processing in accordance with the law.

Article 12. Encryption and decryption of personal data

1. Encryption of personal data means the transformation of personal data into a form that cannot be identified as personal data unless it is decrypted; personal data, once encrypted, shall still be considered personal data.

2. Personal data classified as state secrets must be encrypted and decrypted in accordance with the law on protection of state secrets and the law on cryptography.

3. Agencies, organizations, and individuals shall decide on the encryption and decryption of personal data in conformity with the personal data processing activities.

Article 13. Modification of personal data

1. Data subjects may themselves modify their personal data with respect to certain types of personal data in accordance with the agreement with the personal data controller or the personal data controlling and processing party; or may request the personal data controller or the personal data controlling and processing party to modify their personal data.

2. The personal data controller or the personal data controlling and processing party shall modify personal data upon the request of the data subject or as required by law; and shall request the personal data processor or third party to modify the data subject's personal data.

3. The modification of personal data must ensure accuracy. In case personal data cannot be modified for legitimate reasons, the personal data controller or the personal data controlling and processing party must notify the requesting agency, organization, or individual accordingly.

Article 14. Deletion, destruction, and de-identification of personal data

1. Deletion, destruction, and de-identification of personal data shall be carried out in the following cases:

a) The data subject so requests and accepts any potential risks or damages. The data subject's request in this case must fully comply with the principles provided in Clause 3, Article 4 of this Law;

b) The purpose of personal data processing has been fulfilled;

c) The storage period has expired in accordance with the law;

d) As required by a competent state agency's decision;

dd) As agreed upon;

e) Other cases as prescribed by law.

2. The data subject's request for deletion or destruction of personal data shall not be executed in the cases provided in Article 19 of this Law or where the

deletion or destruction of personal data violates the provisions of Clause 3, Article 4 of this Law.

3. The personal data controller or the personal data controlling and processing party shall delete or destroy personal data in the cases specified in Clause 1 of this Article, or shall request the personal data processor or a third party to delete or destroy the data subject's personal data. The deletion or destruction of personal data must be carried out using secure measures to prevent unauthorized access and restoration of the deleted or destroyed personal data.

4. Agencies, organizations, and individuals shall not intentionally restore deleted or destroyed personal data without authorization.

5. The personal data controller, the personal data controlling and processing party, and the personal data processor shall comply with this Law. If, for justifiable reasons, it is not possible to delete or destroy personal data after receiving the data subject's request, the personal data controller or the personal data controlling and processing party must notify the data subject accordingly.

6. De-identification of personal data shall be conducted as follows:

a) Agencies, organizations, and individuals that de-identify personal data shall be responsible for strictly controlling and supervising the de-identification process; and shall prevent unauthorized access, copying, appropriation, disclosure, or loss of personal data during the de-identification process;

b) Re-identification of personal data after it has been de-identified is prohibited, unless otherwise provided by law;

c) The de-identification of personal data must comply with this Law and other relevant laws.

Article 15. Provision of personal data

1. Data subjects may provide their personal data to agencies, organizations, or individuals in accordance with the law or based on agreements with such agencies, organizations, or individuals.

2. The personal data controller or the personal data controlling and processing party shall provide personal data in the following cases:

a) Provide personal data to the data subject upon his/her request in accordance with the law and the agreement with the data subject, except where such provision may cause harm to national defense, national security, social order and safety, or infringe upon the life, health, or property of others;

b) Provide personal data to other agencies, organizations, or individuals with the consent of the data subject, unless otherwise provided by law.

Article 16. Disclosure of personal data

1. Personal data may only be disclosed for a specific purpose. The scope of disclosure and types of personal data to be disclosed must be consistent with the intended purpose. The disclosure of personal data must not infringe upon the lawful rights and interests of the data subject.

2. Personal data may only be disclosed in the following cases:

a) With the consent of the data subject;

b) In accordance with the law;

c) As prescribed at Point b, Clause 1, Article 19 of this Law;

d) For the performance of contractual obligations.

3. Disclosed personal data must accurately reflect the original data source and facilitate access, exploitation, and use by agencies, organizations, and individuals.

4. Forms of disclosure of personal data include: publishing data on websites, e-portals, mass media, and other forms as prescribed by law.

5. Agencies, organizations, and individuals disclosing personal data must closely monitor and control the disclosure of personal data to ensure compliance with the purpose, scope, and legal regulations; and must prevent unauthorized access, use, disclosure, copying, modification, deletion, destruction, or other unlawful processing of disclosed personal data, within their capabilities and conditions.

Article 17. Transfer of personal data

1. Personal data may be transferred in the following cases:

a) The data subject consents to the transfer of personal data;

b) Personal data are shared among departments within the same agency or organization for processing consistent with the established purpose;

c) Personal data are transferred for continued processing in the event of division, separation, merger of agencies, organizations, administrative units, or in the event of reorganization or transformation of ownership of state-owned enterprises; division, separation, merger, consolidation, or cessation of operations of units or organizations; or the establishment of a new unit or organization following the termination of another;

d) The personal data controller or personal data controlling and processing party transfers personal data to the personal data processor or a third party for processing in accordance with regulations;

dd) Personal data are transferred at the request of a competent state agency;

e) In the cases prescribed in Clause 1, Article 19 of this Law.

2. The transfer of personal data under Clause 1 of this Article, whether subject to fees or not, shall not be considered as the buying or selling of personal data.

3. The Government shall detail this Article.

Article 18. Other activities in personal data processing

1. Personal data controllers, personal data controlling and processing parties, personal data processors and third parties shall store personal data in forms suitable to their operation and take measures to protect personal data in accordance with law.

2. The storage, access, retrieval, connection, coordination, confirmation, authentication of personal data, and other operations that affect personal data shall comply with this Law, data laws, other relevant laws, and the agreement between the parties.

3. Priority shall be given to the exploitation and use of personal data in activities serving state management and activities of public non-business units for the pilot implementation of certain special mechanisms and policies to create breakthroughs in scientific and technological development, innovation, and national digital transformation.

Article 19. Processing of personal data without requiring consent of data subjects

1. The processing of personal data without requiring consent of data subjects is permitted in the following cases:

a) To protect the life, health, honor, dignity, rights, or lawful interests of the data subject or another person in emergency circumstances; or to protect one's own legitimate rights or interests, the legitimate rights or interests of others, or those of the State or an agency or organization in a necessary manner in response to acts infringing upon such interests. Personal data controllers, personal data processors, personal data controlling and processing parties and third parties shall prove this case.

b) To respond to emergencies or threats to national security which are not serious to the extent of requiring the declaration of a state of emergency; for preventing and combating riots, terrorism, crimes and violations in accordance with law.;

c) To serve the operation of state agencies and the exercise of state management functions in accordance with specialized laws;

d) To perform an agreement entered into between the data subject and the relevant agency, organization, or individual in accordance with law;

dd) Other cases as prescribed by law.

2. Agencies, organizations, and individuals concerned must establish supervision mechanisms when processing personal data without requiring consent of data subjects, including:

a) Establishing procedures and regulations on personal data processing and defining the responsibilities of agencies, organizations, and individuals in personal data processing;

b) Implementing appropriate personal data protection measures; regularly assessing risks that may arise during personal data processing;

c) Conducting periodic inspections and evaluations of compliance with laws, procedures, and regulations on personal data processing;

d) Establishing mechanisms for receiving and handling feedback and recommendations from relevant agencies, organizations, and individuals.

Article 20. Cross-border transfer of personal data

1. Cases of cross-border transfer of personal data include:

a) Transfer of personal data stored in Vietnam to a data storage system located outside the territory of the Socialist Republic of Vietnam;

b) Agencies, organizations, or individuals in Vietnam transferring personal data to organizations or individuals abroad;

c) Vietnam-based or overseas agencies, organizations, or individuals using a platform located outside the territory of the Socialist Republic of Vietnam to process personal data collected in Vietnam.

2. Agencies, organizations, or individuals conducting cross-border personal data transfer activities as specified in Clause 1 of this Article must prepare a dossier on the impact assessment of the cross-border transfer of personal data and submit one original copy to the agency in charge of personal data protection within 60 days from the first day of cross-border personal data transfer, except for the cases specified in Clause 6 of this Article.

3. The impact assessment of the cross-border transfer of personal data shall be conducted once for the entire duration of operation of such agency, organization, or individual, and shall be updated in accordance with Article 22 of this Law.

4. The agency in charge of personal data protection shall decide to carry out periodic inspections of cross-border personal data transfers not more than once per year, or extraordinary inspections upon detection of violations of the law on personal data protection or when incidents of personal data leakage or loss occur.

5. The agency in charge of personal data protection shall decide to request the suspension of cross-border personal data transfer by any agency, organization,

or individual upon discovering that the transferred personal data is being used for activities that may harm national defense or national security.

6. The following cases are exempt from the requirement to conduct an impact assessment of the cross-border transfer of personal data:

a) Cross-border personal data transfers by competent state agencies;

b) Agencies or organizations storing the personal data of their employees on cloud computing services;

c) Data subjects personally transferring their own personal data across borders;

d) Other cases as prescribed by the Government.

7. The Government shall provide detailed regulations on Clauses 1, 5, and 6 of this Article, and shall prescribe the components of the dossier, conditions, order and procedures for the impact assessment of the cross-border transfer of personal data.

Article 21. Personal data processing impact assessment

1. The personal data controller and the personal data controlling and processing party shall prepare and retain a dossier on the personal data processing impact assessment and submit one original copy to the agency in charge of personal data protection within 60 days from the first date of personal data processing, except in the cases specified in Clause 6 of this Article.

2. The personal data processing impact assessment shall be conducted once for the entire duration of the operation of the personal data controller or the personal data controlling and processing party and shall be updated in accordance with Article 22 of this Law.

3. The personal data processor shall prepare and retain a dossier on the personal data processing impact assessment as agreed with the personal data controller or the personal data controlling and processing party, except in the cases specified in Clause 6 of this Article.

4. The agency in charge of personal data protection shall evaluate and may request the personal data controller, personal data controlling and processing party, or personal data processor to complete the personal data processing impact assessment dossier in case it is incomplete or non-compliant with regulations.

5. Personal data controllers, personal data controlling and processing parties or personal data processors shall update changes and send a notice of changes in dossiers of impact assessment of personal data processing when there is a change in contents of dossiers sent to the agency in charge of personal data protection.

6. Competent state agencies are not required to conduct the personal data processing impact assessment as prescribed in this Article.

7. The Government shall provide detailed regulations on the components, conditions, order and procedures for personal data processing impact assessments.

Article 22. Updating of personal data processing impact assessment dossiers and cross-border personal data transfer impact assessment dossiers

1. The personal data processing impact assessment dossier and the cross-border personal data transfer impact assessment dossier shall be updated periodically every six (06) months upon any change, or updated immediately in the cases specified in Clause 2 of this Article.

2. Cases requiring immediate updates include:

a) When an agency, organization, or unit is reorganized, terminates its operations, is dissolved, or declares bankruptcy in accordance with law;

b) When there is a change in information regarding the organization or individual providing personal data protection services;

c) When there arises or there is a change in business lines, sectors, or services related to personal data processing as registered in the personal data processing impact assessment dossier or the cross-border personal data transfer impact assessment dossier.

3. The updating of the personal data processing impact assessment dossier and the cross-border personal data transfer impact assessment dossier shall be carried out via the National Portal on Personal Data Protection or at the agency in charge of personal data protection.

4. The Government shall detail this Article.

Article 23. Notification of violations of regulations on personal data protection

1. The personal data controller, personal data controlling and processing party, or third party that detects a violation of regulations on personal data protection which may cause harm to national defense, national security, public order and safety, or infringe upon the life, health, honor, dignity, or property of the data subject must notify the agency in charge of personal data protection no later than 72 hours from the time the violation is detected. In case the personal data processor detects the violation, it must promptly notify the personal data controller or the personal data controlling and processing party.

2. The personal data controller or personal data controlling and processing party shall make a written confirmation of the occurrence of a violation of regulations on personal data protection, and coordinate with the agency in charge of personal data protection in handling the violation.

3. Agencies, organizations, or individuals must notify the agency in charge of personal data protection in the following cases:

a) Detecting violations of regulations on personal data protection;

b) Detecting that personal data are processed for improper purposes and in contravention of the agreement reached between the data subject and the personal data controller or personal data controlling and processing party;

c) Detecting that rights of the data subject are not guaranteed or are improperly exercised;

d) Other cases specified by law.

4. The agency in charge ò personal data protection shall be responsible for receiving notifications and handling violations of regulations on personal data protection. The personal data controller, personal data controlling and processing party, third party, and other relevant agencies, organizations, and individuals shall be responsible for preventing violations, remedying the consequences, and coordinating with the agency in charge of personal data protection in handling violations of regulations on personal data protection.

5. The Government shall provide detailed regulations on the contents of the notification of violations of regulations on personal data protection.

Section 2

PERSONAL DATA PROTECTION IN CERTAIN ACTIVITIES

Article 24. Protection of personal data of children, persons who have lost civil act capacity or have limited civil act capacity, and persons with difficulty in perceiving and controlling their acts

1. The protection of personal data of children, persons who have lost or have limited civil act capacity, and persons with difficulty in perceiving and controlling their acts shall be carried out in accordance with this Law.

2. In the case of children, persons who have lost or have limited civil act capacity, or persons with difficulty in perceiving and controlling their acts, the legal representative shall exercise the rights of the data subjects on their behalf, except for the cases specified in Clause 1, Article 19 of this Law. The processing of children's personal data for the purpose of publishing or disclosing information about their private life or personal secrets, in the case of children aged seven (07) years or older, must obtain the consent of both the child and the legal representative.

3. The processing of personal data of children, persons who have lost or have limited civil act capacity, or persons with difficulty in perceiving and controlling their acts must cease in the following cases:

a) The individual who gave consent under Clause 2 of this Article withdraws such consent for the processing of personal data of the child, person who has lost or has limited civil act capacity, or person with difficulty in perceiving and controlling his/her acts, unless otherwise provided by law;

b) At the request of a competent agency when there is sufficient basis to determine that the personal data processing may infringe upon the lawful rights and interests of the child, person who has lost or has limited civil act capacity, or person with difficulty in perceiving and controlling his/her acts, unless otherwise provided by law.

Article 25. Protection of personal data in the recruitment, management, and use of employees

1. Responsibilities of agencies, organizations, and individuals in protecting personal data during employee recruitment are as follows:

a) Only request the provision of information necessary for the purpose of recruitment in accordance with the law; the provided information shall be used solely for recruitment and for other purposes agreed upon in compliance with the law;

b) The provided information must be processed in accordance with the law and with the consent of the applicant;

c) Information provided by unsuccessful applicants must be deleted or destroyed, unless otherwise agreed with the applicant.

2. Responsibilities of agencies, organizations, and individuals in protecting personal data during employee management and use are as follows:

a) Comply with this Law, labor and employment laws, data-related laws, and other relevant laws;

b) Employee personal data must be stored for a duration in accordance with the law or as agreed upon;

c) Employee personal data must be deleted or destroyed upon termination of the employment contract, unless otherwise agreed or prescribed by law.

3. The processing of employee personal data collected through technological or technical measures for the purpose of employee management is subject to the following provisions:

a) Only technological and technical measures compliant with the law and protective of the rights and interests of the data subject may be applied, and such measures must be clearly known to the employee;

b) It is prohibited to process or use personal data collected through technological or technical measures that violate the law.

Article 26. Protection of personal data related to health information and insurance business activities

1. The protection of personal data related to health information and in insurance business activities shall be governed as follows:

a) The consent of the data subject must be obtained during the collection and processing of personal data, except in the cases specified in Clause 1, Article 19 of this Law;

b) Full compliance with the provisions on personal data protection and other relevant laws is required.

2. Agencies, organizations, and individuals operating in the health sector shall not provide personal data to third parties that are healthcare service providers or providers of health insurance or life insurance services, unless there is a written request from the data subject or in the cases specified in Clause 1, Article 19 of this Law.

3. Organizations and individuals developing medical applications or insurance business applications must fully comply with the provisions on personal data protection.

4. In cases where reinsurance or retrocession enterprises transfer personal data to partners, such transfer must be clearly stipulated in the contract with the customer.

Article 27. Protection of personal data in financial, banking, and credit information activities

1. Organizations and individuals operating in the fields of finance, banking, and credit information activities shall:

a) Fully comply with the regulations on protection of sensitive personal data and with safety and security standards in financial and banking activities in accordance with the law;

b) Not use the credit information of the data subject to perform credit scoring, credit ranking, credit information assessment, or creditworthiness evaluation without the data subject's consent;

c) Only collect personal data necessary for credit information activities from sources that comply with this Law and other relevant laws;

d) Notify the data subject in the event of a leak or loss of information related to bank accounts, financial, credit, or credit information.

2. Organizations and individuals conducting credit information activities shall comply with this Law; take measures to prevent unauthorized access, use,

disclosure, or modification of customers' personal data; provide solutions for data recovery in the event of data loss; ensure confidentiality in the collection, provision, and processing of customers' personal data for the purposes of credit information assessment.

3. The Government shall detail this Article.

Article 28. Protection of personal data in advertising service business

1. Organizations and individuals engaged in advertising service business may only use the personal data of customers transferred by the personal data controller or the personal data controlling and processing party under agreement, or collected through their own business activities, for the purpose of advertising services. The collection, use, and transfer of personal data must ensure the rights of the data subject as provided in Article 4 of this Law.

2. The personal data controller and the personal data controlling and processing party may only transfer personal data to organizations and individuals engaged in advertising service business in accordance with the law.

3. The processing of customers' personal data for the purpose of advertising services must be based on the customer's consent, with the customer being fully informed of the content, method, format, and frequency of product promotion; and a method must be provided for the customer to opt out of receiving advertising information.

4. The use of personal data for advertising must comply with the law on fighting spam messages, spam emails and spam calls, and the advertising law.

5. The data subject may request cessation of receiving information from advertising services. Organizations and individuals engaged in advertising service business must provide a mechanism for and cease advertising activities at the request of the data subject.

6. Organizations and individuals engaged in advertising service business must not subcontract or enter into agreements allowing other organizations or individuals to conduct the entire advertising service on their behalf using personal data.

7. Organizations and individuals engaged in advertising service business shall be responsible for proving their use of customers' personal data for advertising purposes; and must comply with Clauses 1, 2, 3, and 4 of this Article and the advertising law.

8. Organizations and individuals using personal data for behavior-based, targeted, or personalized advertising must comply with this Article and the following requirements:

a) Personal data may only be collected through tracking websites, e-portals, or applications with the data subject's consent;

b) A method must be established to enable the data subject to refuse data sharing; specify data retention periods; and delete or destroy data when no longer necessary.

Article 29. Protection of personal data on social media platforms and online communication services

Organizations and individuals providing social media services and online communication services shall:

1. Clearly notify the content of personal data to be collected when the data subject installs and uses social media platforms or online communication services; not collect personal data unlawfully or beyond the agreed scope with the customer;

2. Not request the provision of images or videos containing full or partial identity documents as elements for account authentication;

3. Provide an option for users to refuse the collection and sharing of data files (referred to as cookies);

4. Provide a "do not track" option or only track social media or online communication service activity upon user consent;

5. Not eavesdrop, wiretap, record calls, or read text messages without the consent of the data subject, unless otherwise provided by law;

6. Publicly disclose the privacy policy, clearly explain the methods of collecting, using, and sharing personal data; provide users with mechanisms to access, modify, and delete data, configure privacy settings for personal data, and report violations of security and privacy; protect personal data of Vietnamese citizens during cross-border data transfers; and establish procedures for prompt and effective handling of violations of personal data protection.

Article 30. Protection of personal data in big data, artificial intelligence, blockchain, virtual universe, and cloud computing

1. Personal data in big data, artificial intelligence, blockchain, virtual universe, and cloud computing environment must be processed for the correct purpose and within the necessary scope, ensuring the lawful rights and interests of the data subject.

2. The processing of personal data in the environments of big data, artificial intelligence, blockchain, virtual universe, and cloud computing must comply with this Law and other relevant laws, and must be consistent with Vietnamese ethical standards and cultural traditions.

3. Systems and services utilizing big data, artificial intelligence, blockchain, virtual universe, and cloud computing must integrate appropriate personal data

protection measures; use suitable authentication and identification methods; and implement access authorization mechanisms for personal data processing.

4. The processing of personal data using artificial intelligence must be categorized by risk level in order to implement appropriate personal data protection measures.

5. It is prohibited to use or develop big data, artificial intelligence, blockchain, virtual universe, or cloud computing systems involving personal data to cause harm to national defense, national security, public order, social safety, or to infringe upon the life, health, honor, dignity, or property of others.

6. The Government shall detail this Article.

Article 31. Protection of personal data related to personal location data and biometric data

1. Personal location data refers to data determined through geolocation technology to identify the location and help determine a specific individual.

2. Biometric data refers to data concerning the physical attributes, unique and stable biological characteristics of an individual, used to identify that individual.

3. The protection of personal data related to personal location data is prescribed as follows:

a) Location tracking through radio frequency identification (RFID) tags and other technologies shall not be applied, unless with the consent of the data subject or upon request of a competent agency in accordance with the law, or where otherwise provided by law;

b) Organizations and individuals providing mobile application platforms must inform users of the use of personal location data; implement measures to prevent the collection of personal location data by unrelated organizations and individuals; and provide users with options for tracking their personal location.

4. The protection of biometric data is prescribed as follows:

a) Agencies, organizations, and individuals collecting and processing biometric data must implement physical security measures for their biometric data storage and transmission devices; restrict access to biometric data; establish monitoring systems to prevent and detect acts of infringement of biometric data; and comply with the law and relevant international standards;

b) In cases where the processing of biometric data causes damage to the data subject, the organization or individual collecting and processing the biometric data must notify the concerned data subject in accordance with the Government's regulations.

Article 32. Protection of personal data collected from audio and video recording activities in public places and public activities

1. Agencies, organizations, and individuals may record audio and video and process personal data collected from audio and video recording activities in public places and public activities without the consent of the data subject in the following cases:

a) For the purpose of performing national defense tasks, safeguarding national security, ensuring public order and safety, and protecting the lawful rights and interests of agencies, organizations, and individuals;

b) Where audio, images, or other identifiable information are obtained from public activities, including conferences, seminars, sports competition activities, art performances and other public activities that do not harm the honor, dignity or reputation of the data subject;

c) Other cases as prescribed by law.

2. In cases of audio and video recording as prescribed in Clause 1 of this Article, agencies, organizations, and individuals shall be responsible for notifying, or using other forms of communication to inform, the data subjects that they are being recorded, unless otherwise provided by law.

3. Personal data collected may only be processed and used in accordance with the intended purpose and shall not be used for unlawful purposes or to infringe upon the lawful rights and interests of the data subject.

4. Personal data collected from audio and video recording activities in public places and public activities may only be stored for the period necessary to serve the collection purpose, unless otherwise provided by law. Upon expiration of the storage period, personal data must be deleted or destroyed in accordance with this Law.

5. Agencies, organizations, and individuals conducting audio and video recording and processing personal data collected from such recordings in the cases specified in Clause 1 of this Article shall be responsible for protecting personal data in accordance with this Law and other relevant laws.

Chapter III

FORCES, CONDITIONS FOR PROTECTION OF PERSONAL DATA

Article 33. Personal data protection forces

1. Personal data protection forces include:

a) The agency in charge of personal data protection under the Ministry of Public Security;

b) Departments and personnel responsible for personal data protection within agencies and organizations;

c) Organizations and individuals providing personal data protection services;

c) Organizations and individuals mobilized to participate in personal data protection.

2. Agencies and organizations shall be responsible for appointing departments or personnel who meet the qualifications and capacities for personal data protection, or for hiring organizations and individuals providing personal data protection services.

3. The Government shall provide regulations on the conditions and responsibilities of departments and personnel responsible for personal data protection within agencies and organizations; organizations and individuals providing personal data protection services; and personal data processing services.

Article 34. Standards and technical regulations on personal data protection

1. Standards on personal data protection include standards for information systems, hardware, software, management, operation, processing, and protection of personal data that are published and recognized for application in Vietnam.

2. Technical regulations on personal data protection include technical regulations for information systems, hardware, software, management, operation, processing, and protection of personal data that are developed, promulgated, and applied in Vietnam.

3. The promulgation of standards and technical regulations on personal data protection shall comply with the law on standards and technical regulations.

Article 35. Inspection of personal data protection activities

The inspection of personal data protection activities shall be conducted in accordance with this Law and the Government's regulations.

Chapter IV

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS RELATING TO PERSONAL DATA PROTECTION

Article 36. State management responsibility for personal data protection

1. The Government shall perform unified state management of personal data protection.

2. The Ministry of Public Security shall act as the focal agency responsible to the Government for performing state management over personal data protection, except for matters falling under the management scope of the Ministry of National Defence.

3. The Ministry of National Defence shall take responsibility before the Government for performing state management over personal data protection within its scope of management.

4. Ministries, ministerial-level agencies, and Government-attached agencies shall perform state management over personal data protection in sectors and fields under their management in accordance with law and their assigned functions and duties.

5. Provincial-level People's Committees shall perform state management over personal data protection in accordance with law and their assigned functions and duties.

Article 37. Responsibilities of personal data controllers, personal data processors or personal data controlling and processing parties

1. Responsibilities of personal data controllers:

a) To clearly state the responsibilities, rights, and obligations of the parties in agreements or contracts related to personal data processing in accordance with this Law and other relevant laws;

b) To determine the purpose and means of personal data processing in documents and agreements with the data subject, ensuring compliance with the principles and content as prescribed by this Law;

c) To take appropriate managerial and technical measures to protect personal data in accordance with the law, and review and update such measures when necessary;

d) To notify acts of violating regulations on personal data protection under Article 23 of this Law;

dd) To select appropriate personal data processors to carry out the processing of personal data;

e) To guarantee the rights of data subjects as specified in Article 4 of this Law;

g) To take responsibility before data subjects for damage caused in the course of personal data processing;

h) To prevent unauthorized collection of personal data through its systems, equipment, or services;

i) To coordinate with the Ministry of Public Security and competent state agencies in personal data protection and provision of information serving the investigation and handling of violations of the law on personal data protection;

k) To discharge other responsibilities in accordance with this Law and other relevant laws.

2. Responsibilities of personal data processors:

a) To receive personal data only after entering into an agreement or contract on personal data processing with the personal data controller or the personal data controlling and processing party;

b) To process personal data in accordance with the agreement or contract entered into with the personal data controller or the personal data controlling and processing party;

c) To fully perform personal data protection measures in accordance with this Law and other relevant laws;

d) To take responsibility before the personal data controller and the personal data controlling and processing party for any damage caused by the processing of personal data;

dd) To prevent unauthorized collection of personal data through their systems, equipment, or services;

e) To coordinate with the Ministry of Public Security and competent state agencies in personal data protection and provision of information serving the investigation and handling of violations of the law on personal data protection;

g) To discharge other responsibilities in accordance with this Law and other relevant laws.

3. The personal data controlling and processing party shall be responsible for fully complying with the provisions of Clauses 1 and 2 of this Article.

Chapter V
IMPLEMENTATION PROVISIONS

Article 38. Effect

1. This Law takes effect from January 1, 2026.

2. Small enterprises and start-up enterprises may choose whether or not to comply with the provisions of Article 21, Article 22, and Clause 2, Article 33 of this Law for a period of 05 years from the effective date of this Law, except for small enterprises and start-up enterprises that provide personal data processing

services, directly process sensitive personal data, or process personal data of a large number of data subjects.

3. Household businesses and microenterprises are not required to comply with the provisions of Article 21, Article 22, and Clause 2, Article 33 of this Law, except for household businesses and microenterprises that provide personal data processing services, directly process sensitive personal data, or process personal data of a large number of data subjects.

4. The Government shall detail Clause 2 and Clause 3 of this Article.

Article 39. Transitional provisions

1. Ongoing personal data processing activities that were consented to by the data subject or carried out based on agreements under the Government's Decree No. 13/2023/ND-CP dated April 17, 2023, prior to the effective date of this Law, may continue to be implemented without the need for renewed consent or renegotiation.

2. Personal data processing impact assessment dossiers and cross-border personal data transfer impact assessment dossiers as prescribed in Government's Decree No. 13/2023/ND-CP dated April 17, 2023, that were received by the agency in charge of personal data protection prior to the effective date of this Law, shall remain valid and shall not be re-prepared in accordance with this Law. The updating of such dossiers after the effective date of this Law shall comply with the provisions of this Law.

This Law was passed on June 26, 2025, by the XVth National Assembly of the Socialist Republic of Vietnam at its 9th session.

CHAIRMAN OF THE NATIONAL ASSEMBLY

Tran Thanh Man