Validity: Known

Status: Known

NATIONAL ASSEMBLY

Law No.: 91/2025/QH15

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom – Happiness

LAW

PERSONAL DATA PROTECTION

Pursuant to the Constitution of the Socialist Republic of Vietnam, as amended and supplemented by a number of articles 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 applicable subjects

1. This Law regulates personal data, personal data protection and the rights, obligations and responsibilities of relevant agencies, organizations and individuals.

2. This Law applies to:

a) Vietnamese agencies, organizations and individuals;

b) Foreign agencies, organizations and individuals in Vietnam;

c) Foreign agencies, organizations and individuals directly involved in or related to the processing of personal data of Vietnamese citizens and people of Vietnamese origin whose nationality has not been determined and who are living in Vietnam and have been granted identity cards.

Article 2. Interpretation of terms

In this Law, the following terms are construed as follows:

1. Personal data is 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 after de-identification is no longer personal data.

2. Basic personal data is personal data reflecting common personal and background factors, frequently used in transactions and social relations, and included in the list issued by the Government.

3. Sensitive personal data is personal data associated with an individual's privacy, which, when violated, will directly affect the rights and legitimate interests of agencies, organizations, and individuals, and is listed by the Government.

4. Personal data protection is the use of forces, means and measures by agencies, organizations and individuals to prevent and combat personal data infringement.

5. The personal data subject is the person about whom the personal data is reflected.

6. Personal data processing is an activity affecting personal data, including one or more of the following activities: collecting, analyzing, synthesizing, encoding, decoding, editing, deleting, destroying, de-identifying, providing, disclosing, transferring personal data and other activities affecting personal data.

7. The personal data controller is the agency, organization or individual that decides the purpose and means of processing personal data.

8. The personal data processor is an agency, organization or individual that processes personal data at the request of the personal data controller or the personal data controller and processor through a contract.

9. The controller and processor of personal data is the agency, organization or individual that decides the purpose, means and directly processes personal data.

10. Third party is an organization or individual other than the personal data subject, the personal data controller, the personal data controller and processor, or the personal data processor involved in the processing of personal data in accordance with the provisions of law.

11. De-identification of personal data is the process of changing or deleting information to create new data that is unidentifiable or cannot help identify a specific individual.

12. Personal data processing impact assessment is the analysis and assessment of possible risks during the processing of personal data in order to apply measures to minimize risks and protect personal data.

Article 3. Principles of personal data protection

1. Comply with the provisions of the Constitution, the provisions of this Law and other relevant legal provisions.

2. Personal data must only be collected and processed within the correct scope and for specific, clear purposes, ensuring compliance with legal regulations.

3. Ensure the accuracy of personal data and edit, update and supplement it when necessary; store it for a period of time appropriate to the purpose of processing personal data, unless otherwise provided by law.

4. Effectively and synchronously implement appropriate institutional, technical and human measures and solutions to protect personal data.

5. Proactively prevent, detect, stop, combat, and promptly and strictly handle all violations of the law on personal data protection.

6. Personal data protection is associated with the protection of national and ethnic interests, serving socio-economic development, ensuring national defense, security and foreign affairs; ensuring harmony between personal data protection and the protection of the rights and legitimate interests of agencies, organizations and individuals.

Article 4. Rights and obligations of personal data subjects

1. The rights of personal data subjects include:

a) Be informed about personal data processing activities;

b) Agree or disagree, request withdrawal of consent to the processing of personal data;

c) View, edit or request correction of personal data;

d) Request for provision, deletion, restriction of processing of personal data; submit request to object to processing of personal data;

d) Complain, denounce, sue, and request compensation for damages according to the provisions of law;

e) Request competent authorities or agencies, organizations and individuals related to the processing of personal data to implement measures and solutions to protect their personal data in accordance with the provisions of law.

2. The obligations of the personal data subject include:

a) Protect your personal data;

b) Respect and protect the personal data of others;

c) Provide complete and accurate personal data as required by law, under contract or when agreeing to allow the processing of personal data;

d) Comply with the law on personal data protection and participate in preventing and combating personal data infringement.

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

a) Comply with the provisions of law; comply with the obligations of the personal data subject under the contract. The exercise of the rights and obligations of the personal data subject must aim to protect the rights and legitimate interests of that personal data subject;

b) Do not cause difficulties or hinder the exercise of legal rights and obligations of the personal data controller, personal data controller and processor, and personal data processor;

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

4. Agencies, organizations and individuals are responsible for creating favorable conditions and must not cause difficulties or hinder the exercise of rights and obligations of personal data subjects as prescribed by law.

5. Upon receiving a request from a personal data subject to exercise the rights of the personal data subject as prescribed in Clause 1 of this Article, the personal data controller and the personal data controller and processor must promptly perform within the time limit prescribed by law.
The Government shall detail this clause.

Article 5. Application of laws on personal data protection

1. Personal data protection activities within the territory of the Socialist Republic of Vietnam shall comply with the provisions of this Law and other relevant legal provisions.

2. In case a law or resolution of the National Assembly issued before the effective date of this Law contains specific provisions on personal data protection that do not contravene the principles of personal data protection as prescribed in this Law, the provisions of that law or resolution shall apply.

3. In case a law or resolution of the National Assembly issued after the effective date of this Law has provisions on personal data protection that are different from the provisions of this Law, it must specify the content of implementation or non-implementation according to the provisions of this Law, and the content of implementation according to the provisions of that law or resolution.

4. In case an agency, organization or individual conducts an assessment of the impact of personal data processing or an assessment of the impact of cross-border personal data

transfer in accordance with the provisions of this Law, it is not required to conduct an assessment of the risk of personal data processing or an assessment of the impact of cross-border personal data transfer in accordance with the provisions of the law on data.

Article 6. International cooperation on personal data protection

1. Comply with Vietnamese law, international treaties to which the Socialist Republic of Vietnam is a member and international agreements on personal data protection on the basis of equality, mutual benefit, respect for independence, sovereignty and territorial integrity.

2. Contents of international cooperation on personal data protection include:

a) Develop an international cooperation mechanism to facilitate effective enforcement of laws on personal data protection;

b) Participate in mutual legal assistance on personal data protection of other countries;

c) Prevent and combat acts of personal data infringement;

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

d) Exchange experiences in developing and implementing laws on personal data protection;

e) Technology transfer to serve personal data protection.

3. The Government shall prescribe the responsibility for implementing international cooperation on personal data protection.

Article 7. Prohibited acts

1. Processing personal data to oppose the Socialist Republic of Vietnam, affecting national defense, national security, social order and safety, and the legitimate rights and interests of agencies, organizations and individuals.

2. Obstructing personal data protection activities.

3. Taking advantage of personal data protection activities to commit illegal acts.

4. Processing personal data contrary to the provisions of law.

5. Using other people's personal data, allowing others to use your personal data to commit acts contrary to the provisions of law.

6. Buying and selling personal data, except where otherwise provided by law.

7. Appropriation, intentional disclosure or loss of personal data.

Article 8. Handling of violations of the law on personal data protection

1. Organizations and individuals who violate the provisions of this Law and other provisions of law related to personal data protection may, depending on the nature, extent and consequences of the violation, be subject to administrative sanctions or criminal prosecution; if causing damage, they must compensate according to the provisions of law.

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

3. The maximum fine for administrative violations of buying and selling personal data is 10 times the amount of revenue from the violation; in case there is no revenue from the violation or the fine calculated based on the amount of revenue from the violation is lower than the maximum fine prescribed in Clause 5 of this Article, the fine prescribed in Clause 5 of this Article shall apply.

4. The maximum fine for administrative violations against organizations that violate regulations on cross-border transfer of personal data is 5% of the organization's revenue of the previous year; in case there is no revenue of the previous year or the fine calculated based on revenue is lower than the maximum fine prescribed in Clause 5 of this Article, the fine prescribed in Clause 5 of this Article shall apply.

5. The maximum fine for administrative violations in other violations in the field of personal data protection is VND 3 billion.

6. The maximum fines prescribed in Clauses 3, 4 and 5 of this Article shall apply to organizations; individuals committing the same violation shall have the maximum fine equal to half of the fine for organizations.

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

Chapter II
PERSONAL DATA PROTECTION

Section 1
PROTECTION OF PERSONAL DATA DURING PERSONAL DATA PROCESSING

Article 9. Consent of the personal data subject

1. Consent of a personal data subject is the personal data subject's permission to process his or her personal data, unless otherwise provided by law.

2. The consent of the personal data subject is only valid when it is based on voluntariness and is fully informed of the following information:

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

b) The personal data controller or the personal data controller and processor;

c) Rights and obligations of personal data subjects.

3. The consent of the personal data subject is expressed in a clear, specific, printable, copyable, written form, including in electronic or verifiable format.

4. The consent of the personal data subject must ensure the following principles:

a) Express consent to each purpose;

b) Must not include conditions requiring consent for purposes other than those stated in the agreement;

c) The consent is valid until the personal data subject changes that consent or as required by law;

d) Silence or non-response shall not be deemed to constitute consent.

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

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

1. Personal data subjects have the right to request the withdrawal of consent to the processing of personal data, request the restriction of the processing of their personal data when there is doubt about the scope, purpose of the processing of personal data or the accuracy of the personal data, except in the cases prescribed in Article 19 of this Law or in cases where the law provides otherwise.

2. Requests for withdrawal of consent or restriction of processing of personal data by personal data subjects must be made in writing, including electronic or verifiable format, and sent to the personal data controller, the personal data controller and processor. Requests for withdrawal of consent or restriction of processing of personal data by personal data subjects shall be made in accordance with the provisions of law and the agreement between the parties.

3. The personal data controller, the personal data controller and processor shall receive, implement and request the personal data processor to implement the request to withdraw consent and restrict the processing of personal data of the personal data subject within the time prescribed by law.

4. The execution of a request to withdraw consent or to restrict the processing of personal data does not apply to personal data processing activities before the time the personal data subject requests to withdraw consent or to restrict the processing of personal data.

Article 11. Collection, analysis and synthesis of personal data

1. Personal data collected must have the consent of the personal data subject before collection, unless otherwise provided by law.

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

3. Agencies, organizations and individuals not specified in Clause 2 of this Article are allowed to analyze and synthesize personal data from personal data sources that are permitted to be processed in accordance with the provisions of law.

Article 12. Encryption and decryption of personal data

1. Encryption of personal data is the conversion of personal data into a form that is unrecognizable as personal data without decryption; personal data after encryption is still personal data.

2. Personal data that is a state secret must be encrypted and decrypted in accordance with the law on state secret protection and the law on cryptography.

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

Article 13. Editing personal data

1. The personal data subject may correct his/her personal data for certain types of personal data by agreement with the personal data controller, personal data controller and processor; request the personal data controller, personal data controller and processor to correct his/her personal data.

2. The personal data controller, the personal data controller and processor shall correct the personal data after the personal data subject requests or correct the personal data in

accordance with the provisions of law; request the personal data processor, the third party to correct the personal data of the personal data subject.

3. The correction of personal data must ensure accuracy. In case it is not possible to correct personal data for legitimate reasons, the personal data controller, the personal data controller and processor must notify the requesting agency, organization or individual.

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

1. Deletion and destruction of personal data is carried out in the following cases:

a) The personal data subject requests and accepts the risks and damages that may occur to him/her. The request of the personal data subject in this case must fully comply with the principles prescribed in Clause 3, Article 4 of this Law;

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

c) The storage period has expired according to the provisions of law;

d) Implement according to the decision of the competent state agency;

d) Comply with the agreement;

e) Other cases as prescribed by law.

2. Failure to comply with the request of the personal data subject to delete or destroy personal data in the cases specified in Article 19 of this Law or the deletion or destruction of personal data violates the provisions in Clause 3, Article 4 of this Law.

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

4. Agencies, organizations and individuals are not allowed to intentionally and illegally restore personal data that has been deleted or destroyed.

5. The personal data controller, the personal data controller and processor, and the personal data processor shall be responsible for complying with the provisions of this Law. In case it is not possible to delete or destroy personal data for legitimate reasons after receiving a request from the personal data subject, the personal data controller, the personal data controller and processor must notify the personal data subject.

6. De-identification of personal data is regulated as follows:

a) Agencies, organizations and individuals de-identifying personal data are responsible for closely controlling and monitoring the process of de-identifying personal data; preventing unauthorized access, copying, appropriation, disclosure and loss of personal data during the de-identification process;

b) Personal data must not be re-identified after it has been de-identified, unless otherwise provided by law;

c) De-identification of personal data shall comply with the provisions of this Law and other relevant legal provisions.

Article 15. Provision of personal data

1. Personal data subjects provide personal data to agencies, organizations and individuals in accordance with the provisions of law or according to agreements with such agencies, organizations and individuals.

2. The personal data controller, the personal data controller and processor provide personal data in the following cases:

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

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

Article 16. Disclosure of personal data

1. Personal data shall only be disclosed for a specific purpose. The scope of disclosure and the type of personal data disclosed must be consistent with the purpose of disclosure. The disclosure of personal data shall not infringe upon the rights and legitimate interests of the personal data subject.

2. Personal data is only disclosed in the following cases:

a) With the consent of the personal data subject;

b) Comply with the provisions of law;

c) Cases specified in Point b, Clause 1, Article 19 of this Law;

d) Perform contractual obligations.

3. Public personal data must ensure that it accurately reflects personal data from the original data source and facilitates agencies, organizations and individuals in accessing, exploiting and using it.

4. Forms of public disclosure of personal data, including: posting data on electronic information pages, electronic information portals, mass media and other forms as prescribed by law.

5. Agencies, organizations and individuals that publicly disclose personal data must strictly control and supervise the disclosure of personal data to ensure compliance with the purposes, scope and provisions of the law; prevent access, use, disclosure, copying, modification, deletion, destruction or other unauthorized processing of publicly disclosed personal data within their capabilities and conditions.

Article 17. Transfer of personal data

1. The transfer of personal data is carried out in the following cases:

a) Transfer of personal data with the consent of the personal data subject;

b) Sharing personal data between departments within the same agency or organization to process personal data in accordance with the established processing purposes;

c) Transfer of personal data for continued processing of personal data in the event of division, separation, merger of agencies, organizations, administrative units and reorganization, conversion of ownership form of state-owned enterprises; division, separation, merger, consolidation, termination of operations of units, organizations; units, organizations established on the basis of termination of operations of other units, organizations;

d) The personal data controller, the personal data controller and processor transfer personal data to the personal data processor, a third party to process personal data as prescribed;

d) Transfer personal data at the request of competent state agencies;

e) Transfer of personal data in the cases specified in Clause 1, Article 19 of this Law.

2. The transfer of personal data in the cases specified in Clause 1 of this Article, whether for a fee or not, shall not be considered as the purchase or sale of personal data.

3. The Government shall detail this Article.

Article 18. Other activities in personal data processing

1. The personal data controller, the personal data controller and processor, the personal data processor, and the third party shall store personal data in a form appropriate to their operations and take measures to protect personal data during storage in accordance with the provisions of law.

2. The storage, access, retrieval, connection, coordination, confirmation, authentication of personal data, and other activities affecting personal data shall be carried out in accordance with the provisions of this Law, the law on data, other relevant legal provisions, and the agreement between the parties.

3. Prioritize the exploitation and use of personal data in state management activities and the operations of public service units to serve the piloting of a number of special mechanisms and policies to create breakthroughs in the development of science, technology, innovation and national digital transformation.

Article 19. Processing of personal data without the consent of the personal data subject

1. Cases of personal data processing without the consent of the personal data subject include:

a) To protect the life, health, honor, dignity, rights and legitimate interests of the personal data subject or other people in urgent cases; to protect the legitimate rights or interests of oneself, of others or the interests of the State, of agencies and organizations in a necessary manner against acts of infringement of the above interests. The personal data controller, the personal data processor, the personal data controller and processor, and the third party are responsible for proving this case;

b) To resolve a state of emergency; a threat to national security but not to the extent of declaring a state of emergency; to prevent and combat riots, terrorism, and to prevent and combat crimes and violations of the law;

c) Serving the activities of state agencies and state management activities according to the provisions of law;

d) Implement the agreement of the personal data subject with relevant agencies, organizations and individuals according to the provisions of law;

d) Other cases as prescribed by law.

2. Relevant agencies, organizations and individuals must establish a monitoring mechanism when processing personal data in cases where the consent of the personal data subject is not required, including:

a) Establish procedures and regulations for processing personal data and determine the responsibilities of agencies, organizations and individuals in the process of processing personal data;

b) Implement appropriate personal data protection measures; regularly assess potential risks in the processing of personal data;

c) Conduct periodic inspections and assessments of compliance with legal provisions, procedures and regulations on personal data processing;

d) Have a mechanism to receive and handle feedback and recommendations from relevant agencies, organizations and individuals.

Article 20. Cross-border transfer of personal data

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

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

b) Agencies, organizations and individuals in Vietnam transfer personal data to organizations and individuals abroad;

c) Agencies, organizations and individuals in Vietnam or abroad using platforms outside the territory of the Socialist Republic of Vietnam to process personal data collected in Vietnam.

2. Agencies, organizations and individuals transferring personal data across borders to perform the activities specified in Clause 1 of this Article must prepare a dossier assessing the impact of transferring personal data across borders and send 01 original copy to the agency in charge of protecting personal data within 60 days from the first day of transferring personal data across borders, except for the case specified in Clause 6 of this Article.

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

4. The authority in charge of personal data protection shall decide to periodically inspect cross-border personal data transfers no more than once a year or conduct surprise inspections when detecting violations of the provisions of the law on personal data protection or when incidents of personal data disclosure or loss occur.

5. The authority in charge of personal data protection decides to request the suspension of cross-border transfer of personal data by agencies, organizations and individuals when it

discovers that the personal data transferred for use in activities may harm national defense and security.

6. Cases that are not required to comply with regulations on cross-border personal data transfer impact assessment include:

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

b) Agencies and organizations store personal data of employees of those agencies and organizations on cloud computing services;

c) The personal data subject transfers his/her personal data across borders;

d) Other cases as prescribed by the Government.

7. The Government shall detail Clauses 1, 5 and 6 of this Article; prescribe the components of the dossier, conditions, order and procedures for assessing the impact of cross-border personal data transfer.

Article 21. Assessment of the impact of personal data processing

1. The personal data controller, the personal data controller and processor shall establish and store a record of the assessment of the impact of personal data processing and send 01 original copy to the authority in charge of personal data protection within 60 days from the first day of processing personal data, except for the case specified in Clause 6 of this Article.

2. The assessment of the impact of personal data processing is conducted once for the entire period of operation of the personal data controller, the personal data controller and processor and is updated according to the provisions of Article 22 of this Law.

3. The personal data processor shall establish and maintain a record of the impact assessment of personal data processing in accordance with the agreement with the personal data controller and the personal data controller and processor, except as provided for in Clause 6 of this Article.

4. The authority in charge of personal data protection shall assess and request the personal data controller, the personal data controller and processor, and the personal data processor to complete the personal data processing impact assessment dossier in case the dossier is incomplete and not in accordance with regulations.

5. The personal data controller, the personal data controller and processor, and the personal data processor shall update and supplement the personal data processing

impact assessment dossier when there is a change in the content of the dossier sent to the personal data protection authority.

6. Competent state agencies are not required to comply with the provisions on assessment of the impact of personal data processing specified in this Article.

7. The Government shall prescribe the components of the dossier, conditions, order and procedures for assessing the impact of personal data processing.

Article 22. Updating the personal data processing impact assessment dossier and the cross-border personal data transfer impact assessment dossier

1. The personal data processing impact assessment dossier and the cross-border personal data transfer impact assessment dossier shall be updated periodically every 6 months when there is a change or immediately updated in the cases specified in Clause 2 of this Article.

2. Changes that need to be updated immediately include:

a) When an agency, organization or unit is reorganized, ceases operations, dissolves or goes bankrupt in accordance with the provisions of law;

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

c) When there is a change in the business line, profession or service related to personal data processing registered in the personal data processing impact assessment dossier or the cross-border personal data transfer impact assessment dossier.

3. Updating the personal data processing impact assessment dossier and the cross-border personal data transfer impact assessment dossier is carried out on the National Personal Data Protection Information Portal or at the personal data protection authority.

4. The Government shall detail this Article.

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

1. The personal data controller, the personal data controller and processor, or a third party that discovers a violation of the provisions on personal data protection that may harm national defense, national security, social order and safety, or infringe upon the life, health, honor, dignity, or property of the personal data subject must notify the competent authority for personal data protection no later than 72 hours from the time of discovery of the violation. In case the personal data processor discovers a violation, it must promptly notify the personal data controller or the personal data controller and processor.

2. The personal data controller, the personal data controller and processor must make a record confirming the occurrence of a violation of the regulations on personal data protection, and coordinate with the agency in charge of personal data protection to handle the violation.

3. Agencies, organizations and individuals shall notify the competent authority for personal data protection in the following cases:

a) Detecting violations of regulations on personal data protection;

b) Personal data is processed for the wrong purpose, not in accordance with the agreement between the personal data subject and the personal data controller, the personal data controller and processor;

c) Failure to guarantee or improperly exercise the rights of personal data subjects;

d) Other cases as prescribed by law.

4. The agency in charge of personal data protection is responsible for receiving notifications and handling violations of regulations on personal data protection. The personal data controller, the personal data controller and processor, third parties and relevant agencies, organizations and individuals are 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 prescribe the content of notification of violations of regulations on personal data protection.

Section 2
PROTECTION OF PERSONAL DATA IN CERTAIN ACTIVITIES

Article 24. Protection of personal data of children, persons with lost or limited civil capacity, and persons with difficulties in cognition or behavior control

1. Protection of personal data of children, persons with lost or limited civil capacity, persons with difficulty in cognition or behavior control shall comply with the provisions of this Law.

2. For children, people who have lost or have limited civil capacity or people with difficulty in cognition or behavior control, the legal representative shall exercise the rights of the personal data subject 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 the private life and personal secrets of children aged 7 years or older must have the consent of the child and the legal representative.

3. Stop processing personal data of children, people with lost or limited civil capacity, people with difficulty in cognition or behavior control in the following cases:

a) The person who has agreed as prescribed in Clause 2 of this Article withdraws the consent to allow the processing of personal data of children, people who have lost or have limited civil act capacity, people with difficulty in cognition or behavior control, except in cases where the law provides otherwise;

b) At the request of a competent authority when there is sufficient evidence to prove that the processing of personal data may infringe upon the rights and legitimate interests of children, people with lost or limited civil capacity, or people with difficulty in cognition or behavior control, except where otherwise provided by law.

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

1. The responsibility of agencies, organizations and individuals in labor recruitment to protect personal data is stipulated as follows:

a) Only be required to provide information serving the recruitment purposes of the recruiting agency, organization or individual in accordance with the provisions of law; the information provided is only used for recruitment purposes and other purposes as agreed in accordance with the provisions of law;

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

c) Must delete or destroy the information provided by the applicant in case of non-recruitment, unless otherwise agreed with the applicant;

2. The responsibility of agencies, organizations and individuals in managing and employing employees to protect personal data is stipulated as follows:

a) Comply with the provisions of this Law, laws on labor, employment, laws on data and other relevant legal provisions;

b) Personal data of employees must be stored for the period prescribed by law or by agreement;

c) Must delete or destroy employee's personal data upon termination of contract, except in cases where otherwise agreed or provided by law.

3. The processing of employees' personal data collected by technological and technical measures in employee management is regulated as follows:

a) Only technological and technical measures may be applied in accordance with the provisions of law and ensuring the rights and interests of personal data subjects, on the basis that the employee clearly knows about such measures;

b) Do not process or use personal data collected from technological and technical measures contrary to the provisions of law.

Article 26. Protection of personal data regarding health information and in insurance business activities

1. Personal data protection for health information and in insurance business activities is regulated as follows:

a) Consent of the personal data subject is required during the collection and processing of personal data, except in the case specified in Clause 1, Article 19 of this Law;

b) Fully apply regulations on personal data protection and other relevant legal regulations.

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

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

4. In case the enterprise conducts reinsurance business, ceding reinsurance and transferring personal data to partners, it must be clearly stated 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 have the following responsibilities:

a) Fully comply with regulations on protection of sensitive personal data, safety and security standards in financial and banking activities as prescribed by law;

b) Do not use the credit information of the personal data subject to score, rank credit, evaluate credit information, or evaluate the creditworthiness of the personal data subject without the consent of the personal data subject;

c) Only collect personal data necessary for credit information activities from sources in accordance with the provisions of this Law and other relevant legal provisions;

d) Notify the personal data subject in case of disclosure or loss of information about bank accounts, finances, credit, and credit information.

2. Organizations and individuals conducting credit information activities are responsible for complying with the provisions of this Law; applying measures to prevent unauthorized access, use, disclosure, and modification of customers' personal data; having solutions to restore customers' personal data in case of loss; ensuring confidentiality in the process of collecting, providing, and processing customers' personal data to serve credit information assessment.

3. The Government shall detail this Article.

Article 28. Protection of personal data in advertising service business

1. Organizations and individuals providing advertising services may only use personal data of customers transferred by the personal data controller, the personal data controller and processor according to the agreement or collected through their business activities to provide advertising services. The collection, use and transfer of personal data must ensure the rights of the personal data subject as prescribed in Article 4 of this Law.

2. The personal data controller, the personal data controller and processor may only transfer personal data to organizations and individuals providing advertising services in accordance with the provisions of law.

3. Processing of customers' personal data for advertising services must have the consent of the customer, on the basis that the customer clearly knows the content, method, form, and frequency of product introduction; providing a method for customers to refuse to receive advertising information.

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

5. Personal data subjects have the right to request to stop receiving information from advertising services. Organizations and individuals providing advertising services must provide a mechanism and stop advertising upon request of personal data subjects.

6. Organizations and individuals providing advertising services are not allowed to sub-lease or agree to let other organizations or individuals perform all advertising services using personal data on their behalf.

7. Organizations and individuals providing advertising services are responsible for proving the use of customers' personal data for advertising purposes; complying with the provisions in Clauses 1, 2, 3, 4 of this Article and the provisions of law on advertising.

8. Organizations and individuals using personal data for behavioral or targeted advertising or personalized advertising must comply with the provisions of this Article and the following provisions:

a) Personal data may only be collected through monitoring websites, electronic portals, and applications with the consent of the personal data subject;

b) Must establish a method to allow personal data subjects to refuse to share data; determine the storage period; delete and destroy data when no longer needed.

Article 29. Protection of personal data for social networking platforms and online communication services

Organizations and individuals providing social networking services and online communication services have the following responsibilities:

1. Clearly notify the content of personal data collected when the personal data subject installs and uses social networks and online communication services; do not illegally collect personal data and do not collect personal data beyond the scope of the agreement with the customer;

2. Do not request to provide images, videos containing full or partial identity documents as a factor in account authentication;

3. Provide users with an option to opt out of the collection and sharing of data files (called cookies);

4. Provide a “do not track” option or only track social media and online media usage with the user’s consent;

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

6. Publish a privacy policy that clearly explains how personal data is collected, used and shared; provide users with a mechanism to access, edit, delete data and set privacy for personal data, report security and privacy violations; protect personal data of Vietnamese citizens when transferring data across borders; develop a process to handle violations of personal data protection quickly and effectively.

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

1. Personal data in the environment of big data, artificial intelligence, blockchain, virtual universe and cloud computing must be processed for the right purpose and limited to the necessary scope, ensuring the rights and legitimate interests of personal data subjects.

2. The processing of personal data in the environment of big data, artificial intelligence, blockchain, virtual universe and cloud computing must comply with the provisions of this Law and other relevant legal provisions; in accordance with ethical standards and Vietnamese customs and traditions.

3. Systems and services using big data, artificial intelligence, blockchain, virtual universe and cloud computing must integrate appropriate personal data security measures; must use appropriate authentication, identification and access authorization methods to process personal data.

4. The processing of personal data by artificial intelligence must be classified according to the level of risk in order to have appropriate measures to protect personal data.

5. Do not use or develop big data processing systems, artificial intelligence, blockchain, virtual universe, cloud computing that use personal data to harm national defense, security, social order and safety or infringe upon the life, health, honor, dignity, or property of others.

6. The Government shall detail this Article.

Article 31. Protection of personal data regarding personal location data, biometric data

1. Personal location data is data determined through positioning technology to know the location and help identify specific people.

2. Biometric data is data about the physical attributes, unique and stable biological characteristics of a person to identify that person.

3. Personal data protection for personal location data is regulated as follows:

a) Location tracking via radio frequency identification cards and other technologies shall not be applied, except with the consent of the personal data subject or at the request of a competent authority as prescribed by law or as otherwise provided by law;

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

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

a) Agencies, organizations and individuals collecting and processing biometric data must have physical security measures for their biometric data storage and transmission devices; limit access to biometric data; have a monitoring system to prevent and detect biometric data infringement; comply with relevant legal provisions and international standards;

b) In case the processing of biometric data causes damage to the personal data subject, the organization or individual collecting and processing biometric data must notify the personal data subject in accordance with Government regulations.

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

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

a) To perform national defense tasks, protect national security, ensure social order and safety, and protect the legitimate rights and interests of agencies, organizations and individuals;

b) Sounds, images, and other identifying information obtained from public activities including conferences, seminars, sports competitions, art performances, and other public activities that do not harm the honor, dignity, or reputation of the personal data subject;

c) Other cases as prescribed by law.

2. In case of audio or video recording as prescribed in Clause 1 of this Article, the agency, organization or individual shall be responsible for notifying or providing other forms of information so that the personal data subject knows that he or she is being recorded, except in cases where the law provides otherwise.

3. Personal data collected shall only be processed and used in accordance with the processing purposes, and shall not be used for illegal purposes or for purposes that infringe upon the rights and legitimate interests of the personal data subject.

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

5. Agencies, organizations and individuals that record audio, video and process personal data obtained from recording audio and video in the cases specified in Clause 1 of this

Article are responsible for protecting personal data in accordance with the provisions of this Law and other relevant legal provisions.

Chapter III
FORCES AND CONDITIONS TO ENSURE PERSONAL DATA PROTECTION

Article 33. Personal data protection force

1. Personal data protection forces include:

a) The agency responsible for personal data protection under the Ministry of Public Security;

b) Department and personnel responsible for protecting personal data in agencies and organizations;

c) Organizations and individuals providing personal data protection services;

d) Organizations and individuals are mobilized to participate in protecting personal data.

2. Agencies and organizations are responsible for designating departments and personnel with the capacity to protect personal data or hiring organizations and individuals to provide personal data protection services.

3. The Government shall prescribe the conditions and tasks of the department and personnel responsible for personal data protection in agencies and organizations; organizations and individuals providing personal data protection services; and personal data processing services.

Article 34. Technical standards and 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 developed, issued, and applied in Vietnam.

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

Article 35. Inspection of personal data protection activities

Inspection of personal data protection activities shall be carried out in accordance with the provisions of this Law and regulations of the Government.

Chapter IV
RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS FOR PROTECTING PERSONAL DATA

Article 36. State management responsibility for personal data protection

1. The Government shall uniformly implement state management of personal data protection.

2. The Ministry of Public Security is the focal agency responsible to the Government for implementing state management of personal data protection, except for content under the management scope of the Ministry of National Defense.

3. The Ministry of National Defense is responsible to the Government for implementing state management of personal data protection within its scope of management.

4. Ministries, ministerial-level agencies, and government agencies shall perform state management of personal data protection in sectors and fields under their management in accordance with the provisions of law and assigned functions and tasks.

5. Provincial People's Committees shall perform state management of personal data protection in accordance with the provisions of law and assigned functions and tasks.

Article 37. Responsibilities of personal data controllers, personal data processors, personal data controllers and processors

1. The responsibilities of the personal data controller are as follows:

a) Clearly state the responsibilities, rights and obligations of the parties to the agreement and contract related to the processing of personal data in accordance with the provisions of this Law and other relevant legal provisions;

b) Decide on the purpose and means of processing personal data in documents and agreements with personal data subjects, ensuring compliance with the principles and contents prescribed by this Law;

c) Implement appropriate technical and management measures to protect personal data in accordance with the law, review and update these measures as necessary;

d) Notification of violations of regulations on personal data protection as prescribed in Article 23 of this Law;

d) Select the appropriate personal data processor to process personal data;

e) Ensure the rights of personal data subjects as prescribed in Article 4 of this Law;

g) Be responsible to the personal data subject for damages caused by the processing of personal data;

h) Prevent unauthorized collection of personal data from its systems, equipment and services;

i) Coordinate with the Ministry of Public Security and competent state agencies in protecting personal data, providing information to serve the investigation and handling of violations of the law on personal data protection;

k) Perform other responsibilities as prescribed by this Law and other relevant legal provisions.

2. The responsibilities of the personal data processor are as follows:

a) Personal data may only be received after an agreement or contract on personal data processing has been reached with the personal data controller, the personal data controller and processor;

b) Process personal data in accordance with agreements and contracts signed with the personal data controller and the personal data controller and processor;

c) Fully implement measures to protect personal data as prescribed by this Law and other relevant legal provisions;

d) Be responsible to the personal data controller, the personal data controller and processor for damages caused by the processing of personal data;

d) Prevent unauthorized collection of personal data from its systems, equipment and services;

e) Coordinate with the Ministry of Public Security and competent state agencies in protecting personal data, providing information to serve the investigation and handling of violations of the law on personal data protection;

g) Perform other responsibilities as prescribed by this Law and other relevant legal provisions.

3. The party controlling and processing personal data is responsible for fully implementing the provisions in Clause 1 and Clause 2 of this Article.

Chapter V
IMPLEMENTATION PROVISIONS

Article 38. Entry into force

1. This Law comes into force from January 1, 2026.

2. Small enterprises and start-ups have the right to choose whether or not to implement the provisions in Article 21, Article 22 and Clause 2, Article 33 of this Law within 05 years from the effective date of this Law, except for small enterprises and start-ups that provide personal data processing services, directly process sensitive personal data or process personal data of a large number of personal data subjects.

3. Business households and micro-enterprises are not required to comply with the provisions of Articles 21, 22 and Clause 2, Article 33 of this Law, except for business households and micro-enterprises that provide personal data processing services, directly process sensitive personal data or process personal data of a large number of personal data subjects.

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

Article 39. Transitional provisions

1. Personal data processing activities that are being carried out with the consent or agreement of the personal data subject as prescribed in Decree No. 13/2023/ND-CP dated April 17, 2023 of the Government before the effective date of this Law shall continue to be carried out without having to seek re-consent or re-agreement.

2. The dossiers assessing the impact of personal data processing and dossiers assessing the impact of transferring personal data abroad as prescribed in Decree No. 13/2023/ND-CP dated April 17, 2023 of the Government that have been received by the agency in charge of personal data protection before the effective date of this Law shall continue to be used and it is not necessary to establish a dossier assessing the impact of personal data processing and dossiers assessing the impact of transferring personal data across borders as prescribed in this Law; the updating of the above-established dossiers after the effective date of this Law shall be implemented in accordance with the provisions of this Law.

This Law was passed by the 15th National Assembly of the Socialist Republic of Vietnam at its 9th session on June 26, 2025.

CHAIRMAN OF THE NATIONAL ASSEMBLY

Tran Thanh Man