

THE PRESIDENT

No. 33/2025/L-CTN

THE SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Hanoi, June 27, 2025

ORDER

On the promulgation of Law

THE PRESIDENT OF THE SOCIALIST REPUBLIC OF VIETNAM

Pursuant to Articles 88 and 91 of the Constitution of the Socialist Republic of Vietnam;

Pursuant to Article 43 of the Law on Promulgation of Legal Documents,

PROMULGATES:

The Law on Personal Data Protection,

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

President of the Socialist Republic of Vietnam

LUONG CUONG

LAW
On Personal Data Protection¹

Pursuant to the Constitution of the Socialist Republic of Vietnam, which has 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 prescribes personal data, personal data protection, and rights, obligations and responsibilities of related 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 remains unidentifiable and who are living in Vietnam and have been issued identity certificates.

Article 2. Interpretation of terms

In this Law, the terms below are 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 after being de-identified is no longer personal data.

¹ Công Báo Nos 971-972 (24/7/2025)

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

3. *Sensitive personal data* means personal data associated with the privacy of individuals which, when infringed upon, will directly affect lawful rights and interests of agencies, organizations and individuals, and is on the list issued by the Government.

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

5. *Personal data subject* means a person who is reflected by personal data.

6. *Personal data processing* mean activities that affect personal data, including one or more than one of the following activities: collecting, analyzing, synthesizing, encrypting, decrypting, rectifying, deleting, destroying, de-identifying, providing, disclosing and transferring personal data, and other activities that affect personal data.

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

8. *Personal data processor* means an agency, organization or individual that conducts personal data processing at the request of a personal data controller or a personal data controlling and processing party under a contract.

9. *Personal data controlling and processing party* means an agency, organization or individual that decides the purpose and means of personal data processing and directly processes personal data.

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

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

12. *Assessment of the impact of personal data processing* means the analysis and assessment of risks that are likely to occur during the process of personal data processing in order to apply measures to minimize 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. To only collect and process personal data within the proper scope and for specific and clear purposes, ensuring compliance with law.

3. To ensure the accuracy of personal data; to rectify, update and supplement personal data when necessary; to store personal data for a period appropriate to the purpose of personal data processing, unless otherwise prescribed by law.

4. To synchronously and effectively implement appropriate institutional, technical and human resource-related measures and solutions to protect personal data.

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

6. To protect personal data in association with safeguarding the interests of the country and the nation, serving socio-economic development, ensuring national defense, security and foreign affairs; and ensuring the harmony between personal data protection and safeguarding of lawful rights and interests of agencies, organizations and individuals.

Article 4. Rights and obligations of personal data subjects

1. Rights of a personal data subject:

a/ To be informed of personal data processing activities;

b/ To agree or disagree with, and request withdrawal of the consent to, personal data processing;

c/ To view, rectify, or request rectification of, his/her personal data;

d/ To request the provision and deletion of his/her personal data and restriction of personal data processing; to submit requests to object to personal data processing;

dd/ To file complaints and denunciations, initiate lawsuits, and request compensation for damage in accordance with law;

e/ To request competent agencies or agencies, organizations and individuals related to personal data processing to implement measures and solutions to protect his/her personal data in accordance with law.

2. Obligations of a personal data subject:

a/ To self-protect his/her personal data;

b/ To respect for and protect personal data of others;

c/ To provide complete and accurate personal data of his/her own as prescribed by law, under the contract or when agreeing to his/her personal data processing;

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

3. When exercising his/her rights and performing his/her obligations, a personal data subject shall fully adhere to the following principles:

a/ To abide by law; to comply with obligations of the personal data subject under the contract. The exercise of the rights and performance of obligations by the personal data subject must aim at protecting his/her own lawful rights and interests;

b/ Not to cause difficulties or hinder the exercise of the rights and performance of legal obligations of the personal data controller, personal data controlling and processing party or personal data processor;

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

4. Agencies, organizations and individuals shall create favorable conditions for, and may not cause difficulties or hinder, the exercise of rights and performance of obligations by personal data subjects as prescribed by law.

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

The Government shall detail this Clause.

Article 5. Application of the law on personal data protection

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

2. In case a law or resolution of the National Assembly, which is promulgated before the effective date of this Law, has specific provisions on personal data protection that are not contrary to the principles of personal data protection prescribed in this Law, the provisions of that law or resolution shall apply.

3. In case a law or resolution of the National Assembly, which is promulgated after the effective date of this Law, has provisions on personal data protection that are different from those of this Law, it must specify the matters which will comply and the matters which will not comply with this Law, and the matters which will comply with 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 transfer of personal data in accordance with this Law, it/he/she are not required to conduct an assessment of risks of personal data processing or an assessment of the impact of cross-border transfer of personal data in accordance with the law on data.

Article 6. International cooperation on personal data protection

1. To abide by Vietnam's law, treaties to which the Socialist Republic of Vietnam is a contracting party, and international agreements on personal data protection on the basis of equality, mutual benefit, and respect for independence, sovereignty and territorial integrity.

2. Contents of international cooperation on personal data protection:

a/ Building an international cooperation mechanism to facilitate effective enforcement of the law on personal data protection;

b/ Participating in other countries' mutual legal assistance activities with regard to personal data protection;

c/ Preventing and combating infringements of personal data;

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

dd/ Exchanging experiences in the making and enforcement of the law on personal data protection;

e/ Conducting technology transfer for 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 lawful rights and interests of agencies, organizations and individuals.

2. Obstructing personal data protection activities.

3. Taking advantage of personal data protection activities to commit violations of law.

4. Processing personal data in contravention of law.

5. Using others' personal data, allowing others to use one's personal data to commit illegal acts.

6. Buying and selling personal data, unless otherwise prescribed by law.

7. Appropriating, or intentionally leaking or losing personal data.

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

1. Organizations and individuals that violate the provisions of this Law and other regulations related to personal data protection shall, depending on the nature, severity and consequences of their violations, be subject to administrative sanctions or penal liability examination; if causing damage, they shall pay compensation in accordance with law.

2. The sanctioning of administrative violations in the field of personal data protection must comply with Clauses 3, 4, 5, 6 and 7 of this Article and the law on handling of administrative violations.

3. The maximum fine in the sanctioning of administrative violations with regard to the act of buying and selling personal data is 10 times the proceeds from the violation; in case there are no proceeds from the violation or the fine calculated based on the proceeds from the violation is lower than the maximum fine specified in Clause 5 of this Article, the fine specified in Clause 5 of this Article shall apply.

4. The maximum fine in the sanctioning of administrative violations applicable to an organization violating regulations on cross-border transfer of personal data is equal to 5% of the organization's revenue of the preceding year; in case there is no revenue in the preceding year or the fine calculated based on revenue is lower than the maximum fine specified in Clause 5 of this Article, the fine specified in Clause 5 of this Article shall apply.

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

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

7. The Government shall prescribe the method for calculating the proceeds from the violation of the law on personal data protection.

Chapter II

PERSONAL DATA PROTECTION

Section 1

PERSONAL DATA PROTECTION DURING THE PROCESS OF PERSONAL DATA PROCESSING

Article 9. Consent of personal data subjects

1. Consent of a personal data subject is the personal data subject's grant of permission for the processing of his/her personal data, unless otherwise prescribed by law.

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

a/ The type of personal data to be processed, and the purpose of personal data processing;

b/ The personal data controller or the personal data controlling and processing party;

c/ The rights and obligations of the personal data subject.

3. The consent of the personal data subject shall be expressed in an explicit, specific manner, which can be printed or copied to text, including in electronic forms or verifiable formats.

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

a/ Expressing the consent to each purpose;

b/ Not being accompanied by a mandatory condition to give the consent to purposes other than those agreed;

c/ The consent is valid until the personal data subject changes his/her consent or as prescribed by law;

d/ Silence or non-response is not considered consent.

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

Article 10. Request to withdraw the consent to, and request to restrict, personal data processing

1. A personal data subject has the right to request withdrawing the consent to personal data processing, or request restricting the processing of his/her personal data when there is doubt about the scope and purpose of personal data processing or the accuracy of personal data, except the cases specified in Article 19 of this Law or unless otherwise prescribed by law.

2. Requests for withdrawal of the consent to, requests for restriction of, personal data processing by the personal data subject shall be made in writing, including electronic forms or verifiable formats, and sent to the personal data controller or the personal data controlling and processing party. Requests for withdrawal of the consent to, or requests for restriction of, personal data processing

by the personal data subject shall be made in accordance with law and the agreement between the parties.

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

4. The implementation of requests for withdrawal of the consent to, or requests for restriction of, personal data processing shall not cover personal data processing activities before the time the personal data subject requests withdrawing the consent to, or requests restricting, personal data processing.

Article 11. Collection, analysis and synthesis of personal data

1. Personal data may be collected with the prior consent of a personal data subject, unless otherwise prescribed by law.

2. Competent Party and State agencies may analyze and synthesize personal data from data sources that are collected by themselves or that are shared with, or provided and transferred to them for exploitation and use to serve the work of leadership, direction, state management and socio-economic development in accordance with law.

3. Agencies, organizations and individuals other than those specified in Clause 2 of this Article may analyze and synthesize personal data from personal data sources permitted for processing in accordance with law.

Article 12. Encryption and decryption of personal data

1. Encryption of personal data is the conversion of personal data into a form that makes personal data become unidentifiable if not decrypted; personal data after being encrypted is still personal data.

2. Personal data being state secrets shall 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 personal data processing activities.

Article 13. Rectification of personal data

1. For certain types of personal data, a personal data subject may rectify his/her personal data as agreed with the personal data controller or the personal data controlling and processing party; and request the personal data controller or the personal data controlling and processing party to rectify his/her personal data.

2. The personal data controller or the personal data controlling and processing party shall rectify personal data after the personal data subject so requests or rectify personal data in accordance with law; and request the personal data processor or a third party to rectify personal data of the personal data subject.

3. The rectification of personal data must ensure accuracy. In case it is impossible to rectify personal data for a plausible reason, the personal data controller or the personal data controlling and processing party shall notify thereof to the requesting agency, organization or individual.

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

1. The deletion and destruction of personal data shall be carried out in the following cases:

a/ The personal data subject so requests and accepts the risks and damage that are likely to occur to him/her. The request of the personal data subject in this case must fully adhere to the principles specified in Clause 3, Article 4 of this Law;

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

c/ The data storage period as prescribed by law has expired;

d/ The deletion and destruction are carried out under the decision of a competent state agency;

dd/ The deletion and destruction are carried out as agreed;

e/ Other cases as prescribed by law.

2. The personal data subject's request for deletion or destruction of personal data in the cases specified in Article 19 of this Law or the deletion or destruction of personal data that violates the provisions of Clause 3, Article 4 of this Law shall not be implemented.

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 request the personal data processor or a third party to delete or destroy personal data of the personal data subject. The deletion or destruction of personal data shall be carried out using security measures, preventing unauthorized access and restoration of deleted or destroyed personal data.

4. Agencies, organizations and individuals may not unauthorizedly restore deleted or destroyed personal data.

5. The personal data controller, the personal data controlling and processing party and the personal data processor shall comply with this Law. In case of impossibility to delete or destroy personal data for plausible reasons after receiving a request from the personal data subject, the personal data controller or the

personal data controlling and processing party shall notify thereof to the personal data subject.

6. De-identification of personal data:

a/ Agencies, organizations and individuals de-identifying personal data shall control and closely monitor the process of de-identification of personal data; prevent unauthorized access, copying, appropriation, leakage and loss of personal data during the de-identification process;

b/ Personal data may not be re-identified after being de-identified, unless otherwise prescribed by law;

c/ De-identification of personal data must comply with this Law and other relevant laws.

Article 15. Provision of personal data

1. Personal data subjects shall provide personal data to agencies, organizations and individuals as prescribed by law or as agreed with such agencies, organizations and individuals.

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

a/ Providing personal data to the personal data subject at the latter's request in accordance with law and as agreed with the data subject, unless such provision is likely to cause harm to national defense and security and social order and safety or infringe upon the life, health and property of others;

b/ Providing personal data to other agencies, organizations and individuals with the consent of the personal data subject, unless otherwise prescribed 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 to be disclosed must be consistent with the purpose of disclosure. Disclosure of personal data may not infringe upon the lawful rights and interests of the personal data subject.

2. Personal data shall only be disclosed:

a/ With the consent of the personal data subject;

b/ In accordance with law;

c/ In the case specified at Point b, Clause 1, Article 19 of this Law;

d/ In order to fulfill contractual obligations.

3. The disclosure of personal data must ensure that it accurately reflects personal data from the original data source and facilitates the assess, exploitation and use of personal data by agencies, organizations and individuals.

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

5. Agencies, organizations and individuals that disclose personal data shall strictly control and supervise the disclosure of personal data to ensure conformity with the purposes and scope of data disclosure and compliance with law; prevent access, use, leakage, copying, rectification, deletion, destruction or other illegal processing of disclosed personal data within their capacity and conditions.

Article 17. Transfer of personal data

1. Transfer of personal data shall be carried out in the following cases:

a/ Transferring personal data with the consent of the personal data subject;

b/ Sharing personal data between units of the same agency or organization to process personal data in conformity with the established processing purposes;

c/ Transferring personal data for further processing in the event of division, separation or merger of agencies, organizations or administrative units and reorganization or conversion of ownership of state enterprises; division, separation, merger, consolidation, or termination of operation of units or organizations; and establishment of units or organizations on the basis of termination of operation of other units or organizations;

d/ The personal data controller or the personal data controlling and processing party transfers personal data to the personal data processor or a third party for processing according to regulations;

dd/ Transferring personal data at the request of a competent state agency;

e/ Transferring 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, with or without a charge, shall not be considered the purchase or sale 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 a form

appropriate to their activities and take measures to protect personal data during the process of data storage in accordance with law.

2. The storage, access, retrieval, connection, coordination, confirmation and authentication of personal data, and other activities affecting personal data must comply with this Law, the law on data, other relevant laws, and the agreement between the parties.

3. To prioritize the exploitation and use of personal data in state management activities and activities of public non-business units to serve the pilot implementation of a number of special mechanisms and policies to create breakthroughs in science and technology development, innovation and national digital transformation.

Article 19. Personal data processing without the consent of personal data subjects

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

a/ To protect the life, health, honor, dignity, and lawful rights and interests of the personal data subject or other persons in urgent cases; to protect legitimate rights or interests of oneself or others or the interests of the State, agencies and organizations when necessary against acts of infringement of the above-mentioned interests. In this case, the burden of proof rests with the personal data controller, the personal data processor, the personal data controlling and processing party, and a third party;

b/ To resolve a state of emergency or a threat to national security which does not reach the extent for declaration of a state of emergency; to prevent and combat riots, terrorism, crimes and violations of law;

c/ To serve operation of state agencies and state management activities in accordance with law;

d/ To implement the agreement between personal data subjects and related agencies, organizations and individuals in accordance with law;

dd/ Other cases as prescribed by law.

2. Related agencies, organizations and individuals shall establish a monitoring mechanism when processing personal data in case the consent of personal data subjects is not required, specifically as follows:

a/ Establishing procedures and formulating regulations on personal data processing and determination of the responsibilities of agencies, organizations and individuals during the process of personal data processing;

b/ Implementing appropriate measures to protect personal data; regularly assessing risks that are likely to occur during the process of personal data processing;

c/ Conducting periodical inspections and assessments of compliance with law, procedures and regulations on personal data processing;

d/ Having a mechanism to receive and handle feedback and recommendations from related agencies, organizations and individuals.

Article 20. Cross-border transfer of personal data

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

a/ Transferring 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 transferring 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. An agency, organization or individual that carries out cross-border transfer of personal data and performs the activities specified in Clause 1 of this Article shall prepare a dossier of assessment of the impact of cross-border transfer of personal data and send 1 original to the agency in charge of personal data protection within 60 days from the first day of conducting cross-border transfer of personal data, except the case specified in Clause 6 of this Article.

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

4. The agency in charge of personal data protection shall decide to periodically inspect cross-border transfer of personal data no more than once a year or conduct an unscheduled inspection when detecting violations of the law on personal data protection or upon leakage or loss of personal data.

5. The agency in charge of personal data protection shall decide to request the termination of cross-border transfer of personal data by agencies, organizations and individuals when it detects that personal data is transferred for use in activities that are likely to harm national defense and security.

6. Cases not requiring compliance with regulations on assessment of the impact of cross-border transfer of personal data:

- a/ Cross-border transfer of personal data by competent state agencies;
- b/ Agencies and organizations storing personal data of their employees with the use of cloud computing services;
- c/ The personal data subject transferring his/her personal data across the border;
- d/ Other cases as prescribed by the Government.

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

Article 21. Assessment of the impact of personal data processing

1. The personal data controller or the personal data controlling and processing party shall prepare a dossier of assessment of the impact of personal data processing and store the dossier and send 1 original to the agency in charge of personal data protection within 60 days from the first day of conducting personal data processing, except the case specified in Clause 6 of this Article.

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

3. The personal data processor shall prepare and store dossiers of assessment of the impact of personal data processing as agreed with the personal data controller or the personal data controlling and processing party, except the case specified in Clause 6 of this Article.

4. The agency in charge of personal data protection shall assess, and request the personal data controller or the personal data controlling and processing party and the personal data processor to complete the dossier of assessment of the impact of personal data processing in case the dossier is incomplete or invalid.

5. The personal data controller or the personal data controlling and processing party and the personal data processor shall update and supplement the dossier of assessment of the impact of personal data processing when there is a change in the content of the dossier sent to the agency in charge of personal data protection.

6. Competent state agencies are not required to implement this Article's provisions on assessment of the impact of personal data processing.

7. The Government shall prescribe the composition of dossiers, conditions, order and procedures for assessment of the impact of personal data processing.

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

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

2. Cases of change that require immediate updating:

a/ When an agency, organization or unit is reorganized, terminates operation, dissolves or goes bankrupt in accordance with law;

b/ There is a change in information about the organization or individual providing personal data protection services;

c/ There is a change in the business lines or services related to personal data processing registered in the dossier of assessment of the impact of personal data processing or the dossier of assessment of the impact of cross-border transfer of personal data.

3. The updating of dossiers of assessment of the impact of personal data processing and dossiers of assessment of the impact of cross-border transfer of personal data shall be carried out on the National Personal Data Protection Portal 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, the personal data controlling and processing party or a third party shall, within 72 hours after detecting a violation of regulations on personal data protection that is likely to cause harm to national defense and security and social order and safety, or infringe upon the life, health, honor, dignity or property of the personal data subject, notify thereof to the agency in charge of personal data protection. In case the personal data processor detects a violation, it/he/she shall promptly notify thereof to the personal data controller or the personal data controlling and processing party.

2. The personal data controller or the personal data controlling and processing party shall make a record confirming the occurrence of a violation of 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 agency in charge of personal data protection in the following cases:

- a/ They detect a violation of regulations on personal data protection;
- b/ Personal data processing serves improper purposes, is carried out not according to the agreement between the personal data subject and the personal data controller or the personal data controlling and processing party;
- c/ The rights of the personal data subject are not guaranteed or are improperly exercised;
- d/ Other cases as prescribed by law.

4. The agency in charge of personal data protection shall receive notifications and handle violations of regulations on personal data protection. The personal data controller, the personal data controlling and processing party, a third party and related agencies, organizations and individuals shall prevent violations, remedy consequences and coordinate 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

PERSONAL DATA PROTECTION IN CERTAIN ACTIVITIES

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

1. The protection of personal data of children, persons with lost or limited civil act capacity and persons with difficulty in cognition or behavior control must comply with this Law.

2. For children, persons with lost or limited civil act capacity, or persons with difficulty in cognition or behavior control, their legal representative shall exercise the rights of the personal data subjects on their behalf, except the cases specified in Clause 1, Article 19 of this Law. For children aged 7 years or older, it is required to obtain the consent of the children and their legal representatives concerning the processing of personal data for the purpose of publishing or disclosing information about their private life and personal secrets.

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

a/ The person who has given the consent as specified in Clause 2 of this Article withdraws his/her consent to the processing of personal data of children, persons with lost or limited civil capacity or persons with difficulty in cognition or behavior control, unless otherwise prescribed by law;

b/ A competent agency so requests when there is sufficient evidence to prove that the processing of personal data is likely to infringe upon the lawful rights and interests of children, persons with lost or limited civil capacity or persons with difficulty in cognition and behavior control, unless otherwise prescribed by law.

Article 25. Protection of personal data in labor recruitment, management and employment

1. Responsibilities of agencies, organizations and individuals for personal data protection in labor recruitment:

a/ To require only information that serves the recruitment purpose of the recruiting agency, organization or individual in accordance with law; to use the provided information only for the recruitment purpose and other purposes as agreed between the involved parties in accordance with law;

b/ To process the information provided by applicants in accordance with law and with the consent of the applicants;

c/ To delete or destroy the information provided by the applicants who are not recruited, unless otherwise agreed with the applicants;

2. Responsibilities of agencies, organizations and individuals for personal data protection in labor management and employment:

a/ To comply with this Law, the laws on labor, employment, and data and other relevant laws;

b/ To store personal data of employees for the period prescribed by law or as agreed;

c/ To delete or destroy personal data of employees upon termination of their contracts, unless otherwise agreed or prescribed by law.

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

a/ To apply only technological and technical measures that are compliant with law and guarantee the rights and interests of the personal data subjects, on the basis that the employees clearly know about such measures;

b/ Not to process and use personal data collected by technological and technical measures in contravention of law.

Article 26. Personal data protection with regard to health information and in insurance business activities

1. Personal data protection with regard to health information and in insurance business activities is prescribed as follows:

a/ It is required to obtain the consent of the personal data subjects during the process of personal data collection and processing, except the cases specified in Clause 1, Article 19 of this Law;

b/ To fully comply with regulations on personal data protection and other relevant 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 cases in which there is a written request from the personal data subject or in the cases specified in Clause 1, Article 19 of this Law.

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

4. In case reinsurance or reinsurance ceding enterprises transfer personal data to partners, such shall be clearly stated in contracts signed with customers.

Article 27. Personal data protection in finance, banking and credit information activities

1. Organizations and individuals operating in the fields of finance, banking and credit information have the following responsibilities:

a/ To fully comply with regulations on protection of sensitive personal data, and safety and security standards in finance and banking activities as prescribed by law;

b/ Not to use credit information of personal data subjects to conduct credit scoring or ranking, evaluate credit information, and assess the creditworthiness of personal data subjects without the consent of personal data subjects;

c/ To collect only personal data necessary for credit information activities from suitable sources in accordance with this Law and other relevant laws;

d/ To notify personal data subjects of leakage or loss of information on bank accounts, finance and credit, or credit information.

2. Organizations and individuals conducting credit information activities shall comply with this Law; apply measures to prevent and combat unauthorized access, use, disclosure and rectification of customers' personal data; adopt solutions to

restore customers' personal data in case of loss; and ensure 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. Personal data protection in provision of advertising services

1. Organizations and individuals providing advertising services may only use customers' personal data that are transferred by the personal data controller or the personal data controlling and processing party as agreed or that are collected through their business activities to serve the provision of advertising services. The collection, use and transfer of personal data must guarantee the rights of personal data subjects as specified in Article 4 of this Law.

2. The personal data controller or the personal data controlling and processing party may only transfer personal data to organizations and individuals providing advertising services in accordance with law.

3. It is required to obtain customers' consent to the processing of their personal data serving the provision of advertising services, on the basis that the customers clearly know about the content, method, form and frequency of product introduction; and to provide a method to enable customers to refuse to receive advertising information.

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

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

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

7. Organizations and individuals providing advertising services shall prove the use of customers' personal data for advertising; and comply with Clauses 1, 2, 3 and 4 of this Article and the law on advertising.

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

a/ To collect personal data through monitoring websites, portals and applications only with the consent of personal data subjects;

b/ To establish a method to allow personal data subjects to refuse to share data; to determine the data storage period; to delete or destroy data when no longer needed.

Article 29. Personal data protection with regard to social media platforms and online communication services

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

1. To clearly notify the content of personal data to be collected when the personal data subjects install and use social media and online communication services; not to collect personal data illegally and beyond the scope agreed with the customers;

2. Not to request the provision of images or videos containing the whole or part of identification papers for use as an account authentication factor;

3. To provide options to allow users to refuse the collection and sharing of cookies;

4. To provide the option “do not track” or only track the use of social media platforms or online communication services with the consent of the users;

5. Not to eavesdrop, wiretap or record calls and read text messages without the consent of the personal data subjects, unless otherwise prescribed by law;

6. To make public the privacy policy, clearly explain the methods of collecting, using and sharing personal data; to provide users with mechanisms to access, rectify and delete data and set privacy for personal data, and report on security and privacy violations; to protect personal data of Vietnamese citizens upon cross-border transfer of data; to formulate a process for quickly and effectively handling violations of the regulations on personal data protection.

Article 30. Personal data protection in big data processing, artificial intelligence, blockchain, metaverse and cloud computing

1. Personal data in the environment of big data, artificial intelligence, blockchain, metaverse and cloud computing shall be processed for the proper purpose and within the necessary scope, ensuring lawful rights and interests of the personal data subjects.

2. The processing of personal data in the environment of big data, artificial intelligence, blockchain, metaverse and cloud computing must comply with this

Law and other relevant laws; and conform with ethical standards and Vietnamese customs and traditions.

3. Systems and services using big data, artificial intelligence, blockchain, metaverse and cloud computing shall be integrated with appropriate personal data security measures; and must use appropriate authentication and identification methods and delegate access for personal data processing.

4. Personal data processing using artificial intelligence must apply risk level-based classification so as to have appropriate personal data protection measures.

5. Not to use or develop systems processing big data, artificial intelligence, blockchain, metaverse and cloud computing that use personal data to cause harm to national defense and security and social order and safety or infringe on the life, health, honor, dignity and property of others.

6. The Government shall detail this Article

Article 31. Personal data protection with regard to personal location data and biometric data

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

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

3. Personal data protection with regard to personal location data is prescribed as follows:

a/ Not to apply location tracking via radio frequency identification cards and other technologies, unless the personal data subject so agrees or a competent agency so requests as prescribed by law or unless otherwise prescribed by law;

b/ Organizations and individuals providing mobile application platforms shall notify users of 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 concerning personal location tracking.

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

a/ Agencies, organizations and individuals collecting and processing biometric data shall apply physical security measures for their biometric data storage and transmission devices; limit access to biometric data; have a monitoring system to prevent and detect acts of infringement upon biometric data; and comply with relevant laws and international standards;

b/ In case the processing of biometric data causes damage to a personal data subject, the organization or individual collecting and processing biometric data

shall notify thereof to the personal data subject in accordance with the Government's regulations.

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

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

a/ To perform national defense tasks, protect national security, ensure social order and safety, or protect lawful rights and interests of agencies, organizations and individuals;

b/ Sound, images and other identification information collected from public activities, including conferences, seminars, sports competitions and art performances and other public activities, that do not harm the honor, dignity and prestige of the personal data subjects;

c/ Other cases as prescribed by law.

2. In case of making audio or video recording as specified in Clause 1 of this Article, the agencies, organizations or individuals shall notify or otherwise inform the personal data subjects for the latter to know that they are being audio- or video-recorded, unless otherwise prescribed by law.

3. Collected personal data shall only be processed and used in conformity with the purpose of processing, and may not be used for illegal purposes or for purposes that infringe upon lawful rights and interests of the personal data subjects.

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

5. Agencies, organizations and individuals that make audio or video recording, and process personal data collected from audio and video recording in the cases specified in Clause 1 of this Article shall protect personal data in accordance with this Law and other relevant laws.

Chapter III

FORCES AND CONDITIONS TO ENSURE PERSONAL DATA PROTECTION

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/ Personal protection data divisions and personnel in agencies and organizations;

c/ Organizations and individuals providing personal data protection services;

d/ Organizations and individuals mobilized to participate in personal data protection.

2. Agencies and organizations shall designate qualified and capable divisions and personnel for personal data protection or hire organizations and individuals providing personal data protection services.

3. The Government shall prescribe the conditions and tasks of personal data protection divisions and personnel in 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, and personal data management, operation, processing and protection that are declared and recognized for application in Vietnam.

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

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

Article 35. Inspection of personal data protection activities

Inspection of personal data protection activities must comply with this Law and the Government's regulations.

Chapter IV

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS FOR PERSONAL DATA PROTECTION

Article 36. Responsibility for state management of personal data protection

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

2. The Ministry of Public Security shall act as the focal-point agency responsible before the Government for performing the state management of personal data protection, except matters falling under the Ministry of National Defense's management.

3. The Ministry of National Defense shall be held responsible before the Government for performing the state management of personal data protection within its management scope.

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

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

Article 37. Responsibilities of personal data controllers, personal data processors and 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 and contracts related to personal data processing in accordance with this Law and other relevant laws;

b/ To decide on the purposes and means of personal data processing in documents and agreements with the personal data subjects, ensuring compliance with the principles and contents prescribed by this Law;

c/ To implement appropriate managerial and technical measures to protect personal data in accordance with law, and review and update these measures when necessary;

d/ To notify violations of regulations on personal data protection in accordance with Article 23 of this Law;

dd/ To select a suitable personal data processor to process personal data;

e/ To guarantee the rights of personal data subjects as prescribed in Article 4 of this Law;

g/ To be held responsible before personal data subjects for damage caused during the process of personal data processing;

h/ To prevent unauthorized collection of personal data from their systems, equipment and services;

i/ To coordinate with the Ministry of Public Security and competent state agencies in protecting personal data and provide information to serve the investigation and handling of violations of the law on personal data protection;

k/ To perform other responsibilities as prescribed in this Law and other relevant laws.

2. Responsibilities of personal data processors:

a/ To receive personal data only after entering into agreements or contracts on personal data processing with personal data controllers or personal data controlling and processing parties;

b/ To process personal data in accordance with the agreements or contracts signed with the personal data controllers or personal data controlling and processing parties;

c/ To fully implement measures to protect personal data in accordance with this Law and other relevant laws;

d/ To be held responsible before the personal data controllers or personal data controlling and processing parties for damage caused during the process of personal data processing;

dd/ To prevent unauthorized collection of personal data from their systems, equipment and services;

e/ To coordinate with the Ministry of Public Security and competent state agencies in protecting personal data and provide information to serve the investigation and handling of violations of the law on personal data protection;

g/ To perform other responsibilities as prescribed by this Law and other relevant laws.

3. Personal data controlling and processing parties shall comply with Clauses 1 and 2 of this Article.

Chapter V

IMPLEMENTATION PROVISIONS

Article 38. Effect

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

2. Small-sized enterprises and startups may choose whether or not to implement Articles 21 and 22, and Clause 2, Article 33, of this Law within 5 years

from the effective date of this Law, except small-sized enterprises and startups 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 Articles 21 and 22, and Clause 2, Article 33, of this Law, except 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 of personal data subjects or as agreed upon in accordance with the Government's Decree No. 13/2023/ND-CP of April 17, 2023, before the effective date of this Law may continue to be carried out without having to obtain new consent or agreement.

2. Dossiers of assessment of the impact of personal data processing and dossiers of assessment of the impact of cross-border transfer of personal data specified in the Government's Decree No. 13/2023/ND-CP of April 17, 2023, that have been received by the agency in charge of personal data protection before the effective date of this Law may continue to be used without having to making new dossiers as prescribed in this Law; the updating of the above-said dossiers after the effective date of this Law must comply with this Law.-

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

Chairman of the National Assembly
TRAN THANH MAN