LAW
ON
PROTECTION OF PERSONAL DATA

Contents

CHAPTER I 3

GENERAL PROVISIONS 3

Article 1 *Governing scope and applicable entities* 3

Article 2 *Interpretation of terms* 3

Article 3 *Principles for protection of personal data* 4

Article 4 *Rights and obligations of personal data subjects* 4

Article 5 *Application of the law on protection of personal data* 6

Article 6 *International cooperation on protection of personal data* 6

Article 7 *Prohibited acts* 6

Article 8 *Dealing with breaches of the law on protection of personal data* 7

CHAPTER II 7

PROTECTION OF PERSONAL DATA 7

SECTION 1 7

PROTECTION OF PERSONAL DATA DURING THE PROCESSING OF PERSONAL DATA 7

Article 9 *Personal data subjects' consent* 7

Article 10 *Request to withdraw consent, and request to restrict processing of personal data* 8

Article 11 *Collection, analysis and compilation of personal data* 8

Article 12 *Encryption and decryption of personal data* 9

Article 13 *Modification of personal data* 9

Article 14 *Deletion, destruction and de-identification of personal data* 9

Article 15 *Provision of personal data* 10

Article 16 *Public disclosure of personal data* 10

Article 17 *Transfer of personal data* 11

Article 18 *Other activities in the processing of personal data* 11

Article 19 *Processing of personal data without personal data subjects' consent* 12

Article 20 *Cross-border transfer of personal data* 12

Article 21 *Personal data processing impact assessment* 13

Article 22 *Update of files on personal data processing impact assessment and files on cross-border personal data transfer impact assessment* 14

Article 23 *Notification of breach of the regulations on personal data protection* 14

SECTION 2 15
PROTECTION OF PERSONAL DATA IN CERTAIN ACTIVITIES 15

Article 24 *Protection of personal data of children, persons having lost or having been restricted in the capacity for civil acts and persons having cognitive difficulties or difficulties with behavioural control* 15

Article 25 *Protection of personal data in recruitment, management and use of employees* 16

Article 26 *Protection of personal data in respect of health information and in insurance business activities* 16

Article 27 *Protection of personal data in financial, banking, and credit information activities* 17

Article 28 *Protection of personal data in business of advertising services* 17

Article 29 *Protection of personal data with respect to social networking platforms and online communication services* 18

Article 30 *Protection of personal data in processing of big data, artificial intelligence, blockchains, metaverse, cloud computing* 18

Article 31 *Protection of personal data with respect to personal location data and biometric data* 19

Article 32 *Protection of personal data collected from audio and video recording activities in public places and public activities* 19

CHAPTER III 20
FORCES AND CONDITIONS FOR ENSURING PROTECTION OF PERSONAL DATA 20

Article 33 *Forces protecting personal data* 20

Article 34 *Standards and technical regulations on protection of personal data* 21

Article 35 *Inspection of activities of protection of personal data* 21

CHAPTER IV 21
RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS FOR PROTECTING PERSONAL DATA 21

Article 36 *Responsibilities for State administration of personal data protection* 21

Article 37 *Responsibilities of personal data controllers, personal data processors, and personal data controlling and processing parties* 21

CHAPTER V 22
IMPLEMENTING PROVISIONS 22

Article 38 *Effectiveness* 22

Article 39 *Transitional provisions* 23

NATIONAL ASSEMBLY

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Law No.: 91/2025/QH15

LAW
ON
PROTECTION OF PERSONAL DATA

Pursuant to the Constitution of the Socialist Republic of Vietnam as amended by Resolution No. 203/2025/QH15;

The National Assembly hereby promulgates the Law on Protection of Personal Data.

Chapter I

GENERAL PROVISIONS

Article 1 *Governing scope and applicable entities*

1. This Law regulates personal data, protection of personal data, and 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 yet been determined and who are living in Vietnam and have been issued with identity certificates.

Article 2 *Interpretation of terms*

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

1. *Personal data* means digital data or information in any other form which identifies or helps identify a specific natural person, comprising basic personal data and sensitive personal data. Personal data after de-identification shall be no longer personal data.

2. *Basic personal data* means personal data which reflect common personal and background factors, are regularly used in transactions and social relations, and are included on the list promulgated by the Government.

3. *Sensitive personal data* means personal data associated with an individual's privacy, infringement of which shall directly affect the legitimate rights and interests of any agency, organization or individual, and which are included on the list promulgated by the Government.

4. *Protection of personal data* means the use of forces, means and measures by agencies, organizations and individuals to prevent and combat personal data infringement activities.

5. *Personal data subject* means a person whom personal data reflect.

6. *Processing of personal data* means the activities affecting personal data, comprising one or more of the following activities: collecting, analysing, compiling, encrypting, decrypting, modifying, deleting, destroying, de-identifying, providing, publicizing and transferring personal data and other activities affecting personal data.

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

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

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

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

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

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

Article 3 *Principles for protection of personal data*

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

2. Only collect and process personal data within the correct scope, for specific and clear purposes, and in compliance with law.

3. Ensure the accuracy of personal data and modify, update and supplement personal data when necessary; store personal data for a period suitable for the purpose of processing personal data, unless otherwise provided for by law.

4. Synchronously and effectively implement appropriate institutional, technical and human measures and solutions to protect personal data.

5. Proactively prevent, detect, stop, fight against and promptly and strictly deal with all breaches of the law on protection of personal data.

6. Protect personal data in association with protecting national and ethnic interests, serving the socio-economic development, ensuring national defence, security and foreign relations; ensure the harmony between the protection of personal data and the protection of legitimate rights and interests of agencies, organizations and individuals.

Article 4 *Rights and obligations of personal data subjects*

1. Rights of a personal data subject shall comprise the following:

    (a) To be informed about the processing of personal data;

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

(c) To view, modify or request modification of personal data;

(d) To request provision, deletion or restriction of processing of personal data; to submit a request to object to the processing of personal data;

(dd) To lodge a complaint or denunciation, to initiate a legal action, or to request compensation for damage in accordance with law;

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

2. Obligations of a personal data subject shall comprise the following:

(a) To protect his/her own personal data;

(b) To respect and protect personal data of others;

(c) To provide his/her personal data completely and accurately in accordance with law, in accordance with a contract or when he/she agrees to the processing of his/her personal data;

(d) To observe the law on protection of personal data and participate in the prevention and combat of personal data infringement activities.

3. When a personal data subject exercises his/her rights and obligations, he/she must fully comply with the following principles:

(a) Implement the provisions of law; comply with the obligations of the personal data subject under a contract. The exercise of the rights and performance of obligations of the personal data subject must be aimed at protecting the legitimate rights and interests of such personal data subject;

(b) Not cause difficulties in or obstruct the exercise of legal rights and obligations of the personal data controller, the personal data controlling and processing party or the personal data processor;

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

4. Agencies, organizations and individuals shall be responsible to create favourable conditions for and must not cause difficulties in or obstruct the exercise of the rights and the performance of obligations of personal data subjects in accordance with law.

5. Upon receipt of a request from a personal data subject for exercise of the rights of the personal data subject stipulated in clause 1 of this article, the personal data controller or the personal data controlling and processing party must promptly implement same within the period prescribed by law.

The Government shall provide detailed regulations on this clause.

Article 5 *Application of the law on protection of personal data*

1. Personal data protection activities in the territory of the Socialist Republic of Vietnam shall be implemented in accordance with this Law and other relevant laws.

2. Where a law or resolution of the National Assembly promulgated before the effective date of this Law contains the specific provisions on protection of personal data which are not contrary to the principles for protection of personal data as stipulated in this Law, the provisions of such law or resolution shall apply.

3. Where a law or resolution of the National Assembly promulgated after the effective date of this Law contains the provisions on protection of personal data which are different from the provisions of this Law, the contents to be implemented or not to be implemented in accordance with this Law and the contents to be implemented in accordance with such law or resolution must be specified.

4. Where an agency, organization or individual conducts personal data processing impact assessment or cross-border personal data transfer impact assessment in accordance with this Law, such agency, organization or individual shall not be required to conduct personal data processing risk assessment or cross-border personal data transfer impact assessment in accordance with the law on data.

Article 6 *International cooperation on protection of personal data*

1. [The international cooperation on protection of personal data must] comply with the laws of Vietnam, international treaties of which the Socialist Republic of Vietnam is a member and international agreements on protection of personal data on the basis of equality, mutual benefits, and respect for independence, sovereignty and territorial integrity.

2. The contents of international cooperation on protection of personal data shall comprise:

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

   (b) Participating in mutual legal assistance in the protection of personal data with other countries;

   (c) Preventing and combating personal data infringements;

   (d) Training human resources, conducting scientific researches, and applying science and technologies in the protection of personal data;

   (dd) Exchanging experience in formulating and implementing the law on protection of personal data;

   (e) Transferring technologies for the purpose of protecting personal data.

3. The Government shall stipulate responsibilities for international cooperation on protection of personal data.

Article 7 *Prohibited acts*

1 Processing personal data with a view to opposing the State of the Socialist Republic of Vietnam, affecting national defence and 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 violate law.

4. Processing personal data in contravention of law.

5. Using personal data of other persons, allowing other persons to use their own personal data to commit acts contrary to law.

6. Purchasing and selling personal data, unless otherwise provided for by law.

7. Appropriating, deliberately revealing or losing personal data.

Article 8 *Dealing with breaches of the law on protection of personal data*

1. Any organization or individual in breach of this Law and other laws related to the protection of personal data may, depending on the nature, seriousness and consequences of the breach, be subject to an administrative penalty or be prosecuted for criminal liability; if any damage is caused, such organization or individual must pay compensation in accordance with law.

2. The imposition of penalties for administrative breaches in the sector of protection of personal data shall comply with clauses 3, 4, 5, 6 and 7 of this article and the law on dealing with administrative breaches.

3. In the case of imposition of an administrative penalty for an act of purchasing or selling personal data, the maximum fine shall be 10 times the proceeds from the breach; where no proceeds are obtained from the breach or the fine calculated on the basis of the proceeds from the breach is lower than the maximum fine stipulated in clause 5 of this article, the fine stipulated in clause 5 of this article shall apply.

4. In the case of imposition of an administrative penalty on an organization committing a breach of the provisions on cross-border personal data transfer, the maximum fine shall be 5% of the turnover of such organization in the preceding year; where no turnover is generated in the preceding year or the fine calculated on the basis of the turnover is lower than the maximum fine stipulated in clause 5 of this article, the fine stipulated in clause 5 of this article shall apply.

5. The maximum fine in the case of imposition of an administrative penalty for other breaches in the sector of protection of personal data shall be 3 billion dong.

6. The maximum fines stipulated in clauses 3, 4 and 5 of this article shall apply to organizations; individuals committing the same breach shall be subject to the maximum fine equal to half of the fine applicable to organizations.

7. The Government shall stipulate methods of calculating proceeds from committing breaches of the law on protection of personal data.

Chapter II

PROTECTION OF PERSONAL DATA

Section 1

PROTECTION OF PERSONAL DATA DURING THE PROCESSING OF PERSONAL DATA

Article 9 *Personal data subjects' consent*

1. Personal data subject's consent means a personal data subject permits the processing of his/her personal data, unless otherwise provided for by law.

2. A personal data subject's consent shall only be effective when it is given [by the data subject] on a voluntary basis and [the personal data subject is] fully aware of the following information:

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

   (b) Personal data controller or personal data controlling and processing party;

   (c) Rights and obligations of the personal data subject.

3. Personal data subjects' consent shall be expressed clearly and specifically, and may be printed or copied in writing, including in electronic form or verifiable format.

4. A personal data subject's consent must ensure the following principles:

   (a) Expressing the consent for each purpose;

   (b) It must not be accompanied by the condition that the personal data subject is bound to agree to purposes other than those agreed;

   (c) The consent is effective until the personal data subject changes such consent or as prescribed by law;

   (d) Silence or no response shall not be considered as consent.

5. The Government shall provide detailed regulations on clause 3 of this article.

Article 10 *Request to withdraw consent, and request to restrict processing of personal data*

1. A personal data subject has the right to request withdrawal of his/her consent to the processing of his/her personal data or request restriction of the processing of his/her personal data when there is a doubt about the scope or purpose of the processing of personal data or the accuracy of personal data, except for the cases stipulated in article 19 of this Law or unless otherwise provided for by law.

2. The request for withdrawal of consent or request for restriction of the processing of personal data from a personal data subject must be made in writing, including in electronic form or verifiable format, and sent to the personal data controller or the personal data controlling and processing party. Such request shall be implemented in accordance with law and as agreed by the parties.

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

4. The implementation of the request for withdrawal of consent or request for restriction of the processing of personal data shall not apply to the personal data processing activities [conducted] before the personal data subject makes such request.

Article 11 *Collection, analysis and compilation of personal data*

1. Personal data to be collected must be consented by personal data subjects before collection, unless otherwise provided for by law.

2. Competent Party and State agencies may analyse and compile personal data from data sources collected by such agencies themselves or shared, provided, transferred, exploited and used to serve

the leadership, direction, State management and socio-economic development in accordance with law.

3. Agencies, organizations and individuals other than those prescribed in clause 2 of this article may analyse and compile 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 means the conversion of personal data into a form whereby personal data are unidentifiable if such personal data are not decrypted; personal data after encryption shall remain personal data.

2. Personal data being State secrets must be encrypted and decrypted in accordance with the law on protection of State secrets and the law on cipher.

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

Article 13 *Modification of personal data*

1. A personal data subject may modify his/her own personal data with respect to a number of types of personal data as agreed with the personal data controller or the personal data controlling and processing party; or request the personal data controller or the personal data controlling and processing party to modify his/her personal data.

2. The personal data controller or the personal data controlling and processing party shall modify personal data after the personal data subject makes the request or shall modify personal data in accordance with law; [or] request the personal data processor or a third party to modify personal data of the personal data subject.

3. The modification of personal data must ensure the accuracy. Where it is unable to modify personal data for a legitimate reason, the personal data controller or the personal data controlling and processing party must notify the requesting agency, organization or individual thereof.

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

1. Personal data shall be deleted or destroyed in the following cases:

   (a) The personal data subject makes a request and accepts possible risks and damage to him/her. The request of the personal data subject in this case must fully comply with the principles stipulated in article 4.3 of this Law;

   (b) The purpose of processing personal data has been completed;

   (c) The period for storage has expired as prescribed by law;

   (d) Pursuant to a decision of a competent State agency;

   (dd) As agreed;

   (e) Other cases as prescribed by law.

2. Requests of personal data subjects for deletion or destruction of personal data shall not be implemented in the cases stipulated in article 19 of this Law or in the case where the deletion or destruction of personal data is in breach of article 4.3 of this Law.

3. The personal data controller or the personal data controlling and processing party shall delete or destroy personal data in the cases stipulated 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 must be carried out by applying safety measures; [and must] prevent illegal intrusion and restoration of the deleted or destroyed personal data.

4. Agencies, organizations and individuals are not permitted to intentionally carry out illegal restoration of personal data which have been deleted or destroyed.

5. The personal data controller, the personal data controlling and processing party, and the personal data processor shall be responsible to comply with this Law. Where it is unable to delete or destroy personal data for a legitimate reason after receiving the request of the personal data subject, the personal data controller or the personal data controlling and processing party must notify the personal data subject thereof.

6. The de-identification of personal data shall be stipulated as follows:

   (a) Agencies, organizations and individuals de-identifying personal data shall be responsible to closely control and supervise the process of de-identification of personal data; and prevent unauthorized access, copying, appropriation, revelation and loss of personal data in the process of de-identification;

   (b) Personal data shall not be re-identified after such personal data have been de-identified, unless otherwise provided for by law;

   (c) The de-identification of personal data shall 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 in accordance with law or as agreed with such agencies, organizations and individuals.

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

   (a) Providing to the personal data subject at the request of the personal data subject in accordance with law [and/or] as agreed with the data subject, except where such provision may cause harm to national defence and security, social order and safety or infringe upon the life, health and property of others;

   (b) Providing to any other agency, organization or individual with the consent of the personal data subject, unless otherwise provided for by law.

Article 16 *Public disclosure of personal data*

1. Personal data shall only be publicly disclosed for specific purposes. The scope of public disclosure and types of personal data to be publicly disclosed must be suitable for the purposes of public disclosure. The public disclosure of personal data must not infringe upon the legitimate rights and interests of personal data subjects.

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

(a) With the consent of the personal data subject;

(b) In compliance with law;

(c) In the case prescribed in article 19.1(b) of this Law;

(d) Performance of contractual obligations.

3. Publicly disclosed personal data must correctly reflect personal data from original data sources and create favourable conditions for agencies, organizations and individuals to access, exploit and use.

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

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

Article 17 *Transfer of personal data*

1. The 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 among departments in the same agency or organization to process personal data in accordance with the established processing purposes;

(c) Transferring personal data for further processing of personal data in the case of division, separation or merger of an agency, organization or administrative unit and re-organization or conversion of the form of ownership of a State owned enterprise; division, separation, merger, consolidation or termination of operation of a unit or organization; [or where] a unit or organization is established on the basis of termination of operation of another unit or organization;

(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 to process personal data in accordance with regulations;

(dd) Transferring personal data at the request of a competent State agency;

(e) Transferring personal data in the cases stipulated in article 19.1 of this Law.

2. The transfer of personal data in the cases stipulated in clause 1 of this article with or without collection of fees shall not be determined as the purchase or sale of personal data.

3. The Government shall provide detailed regulations on this article.

Article 18 *Other activities in the processing of personal data*

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

2. The storage, access, retrieval, connection, coordination, certification and authentication of personal data and other activities affecting personal data shall be implemented in accordance with this Law, the law on data and other relevant provisions of law and as agreed by the parties.

3. Priority is given to exploiting and using personal data in activities serving State management and activities of public professional units for the purpose of serving the pilot [implementation] 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 personal data subjects' consent*

1. Cases of processing of personal data without personal data subjects' consent shall comprise:

   (a) In order to protect the life, health, honor, dignity, and lawful rights and interests of personal data subjects or others in emergency cases; and protect legitimate rights or interests [of personal data subjects] or of others or the interests of the State, agencies and organizations as required against acts of infringing upon the above-mentioned interests. The personal data controller, the personal data processor, the personal data controlling and processing party, [and/or] a third party shall be responsible for proving this case;

   (b) In order to resolve a state of emergency, [or] a threat to national security but not to the extent of declaring a state of emergency; to prevent and combat riots, terrorism, crimes and breaches of law;

   (c) Serving activities of State agencies and State management activities in accordance with law;

   (d) Implementing agreements between personal data subjects and relevant agencies, organizations and individuals in accordance with law;

   (dd) Other cases as prescribed by law.

2. Relevant agencies, organizations and individuals must establish a supervisory mechanism when processing personal data without personal data subjects' consent including:

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

   (b) Implementing appropriate personal data protection measures; regularly assessing possible risks in the process of processing personal data;

   (c) Conducting periodic inspection and assessment of the compliance with law and the processes and regulations on processing of personal data;

   (d) Having a mechanism for receiving and dealing with reports and recommendations from agencies, organizations and individuals concerned.

Article 20 *Cross-border transfer of personal data*

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

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

(b) An agency, organization or individual in Vietnam transfers personal data to an overseas organization or individual;

(c) An agency, organization or individual in Vietnam or abroad uses a platform outside the territory of the Socialist Republic of Vietnam to process personal data collected in Vietnam.

2. Any agency, organization or individual making a cross-border transfer of personal data which carries out the activities stipulated in clause 1 of this article must prepare a file on cross-border personal data transfer impact assessment and send one original copy to the specialized agency for personal data protection within 60 days from the first day of cross-border personal data transfer, except for the case stipulated in clause 6 of this article.

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

4. The specialized agency for personal data protection shall decide on the periodic inspection of the cross-border personal data transfer no more than once a year or on a one-off basis when detecting any breach of the law on protection of personal data or upon occurrence of any revelation or loss of personal data.

5. The specialized agency for personal data protection shall make a decision requesting suspension of the cross-border personal data transfer by an agency, organization or individual when detecting that personal data are transferred for use in any activity which may cause harm to national defence and security.

6. Cases where it is not required to implement the provisions on cross-border personal data transfer impact assessment shall comprise:

(a) The cross-border personal data transfer is made by a competent State agency;

(b) An agency or organization stores personal data of its employees by using cloud computing services;

(c) A personal data subject transfers his/her personal data across borders by himself/herself;

(d) Other cases as prescribed by the Government.

7. The Government shall provide detailed regulations on clauses 1, 5 and 6 of this article; and stipulate components of files, conditions, sequence and procedures for cross-border personal data transfer impact assessment.

Article 21 *Personal data processing impact assessment*

1. A personal data controller or a personal data controlling and processing party shall prepare and store a file on personal data processing impact assessment and send one original copy to the specialized agency for personal data protection within 60 days from the first day of personal data processing, except for the case stipulated in clause 6 of this article.

2. The personal data processing impact assessment shall be conducted once for the entire duration of operation of a personal data controller or a 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 a file on personal data processing impact assessment as agreed with the personal data controller or the personal data controlling and processing party, except for the case stipulated in clause 6 of this article.

4. The specialized agency for personal data protection shall assess and request the personal data controller, the personal data controlling and processing party or the personal data processor to complete the file on personal data processing impact assessment if the file is incomplete and not in accordance with regulations.

5. The personal data controller, the personal data controlling and processing party or the personal data processor shall update and supplement the file when there is any change to the contents of the file sent to the specialized agency for personal data protection.

6. Competent State agencies are not required to comply with the provisions on personal data processing impact assessment in this article.

7. The Government shall stipulate the composition of files, conditions, sequence and procedures for personal data processing impact assessment.

Article 22 *Update of files on personal data processing impact assessment and files on cross-border personal data transfer impact assessment*

1. Files on personal data processing impact assessment and files on cross-border personal data transfer impact assessment shall be updated every 6 months when there is any change thereto or shall be updated immediately in the cases stipulated in clause 2 of this article.

2. Cases where changes are required to be updated immediately shall comprise:

   (a) When an agency, organization or entity is re-organized, terminated, dissolved or bankrupt in accordance with law;

   (b) When there is any change to information about an organization or individual providing personal data protection services;

   (c) When a business line or service arises or is changed in relation to the processing of personal data which was registered in the file on personal data processing impact assessment or the file on cross-border personal data transfer impact assessment is suspended.

3. Files on personal data processing impact assessment and files on cross-border personal data transfer impact assessment shall be updated on the National Portal on Personal Data Protection or at the specialized agency for personal data protection.

4. The Government shall provide detailed regulations on this article.

Article 23 *Notification of breach of the regulations on personal data protection*

1. A personal data controller, personal data controlling and processing party or third party detecting any breach of the regulations on personal data protection which may cause harm to national defence and security, social order and safety or infringe upon the life, health, honor, dignity or assets of personal data subjects must notify the specialized agency for personal data protection no later than 72 hours from the detection of the breach. Where the personal data processor detects a breach, it must promptly notify the personal data controller or the personal data controlling and processing party thereof.

2. The personal data controller or the personal data controlling and processing party must prepare the minutes to certify the occurrence of the breach of the regulations on personal data protection, and coordinate with the specialized agency for personal data protection to deal with the breach.

3. Agencies, organizations and individuals shall provide a notice to the specialized agency for personal data protection in the following cases:

   (a) Detecting any breach of the regulations on personal data protection;

   (b) Personal data are not processed for correct purposes or as agreed 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 correctly exercised;

   (d) Other cases as prescribed by law.

4. The specialized agency for personal data protection shall be responsible to receive notices and deal with breaches of the regulations on protection of personal data. Personal data controllers, personal data controlling and processing parties, third parties and relevant agencies, organizations and individuals shall be responsible for preventing breaches, remedying any consequences and coordinating with the specialized agency for personal data protection in dealing with breaches of the regulations on protection of personal data.

5. The Government shall stipulate the contents of notices of breach of the regulations on personal data protection.

Section 2

PROTECTION OF PERSONAL DATA IN CERTAIN ACTIVITIES

Article 24 *Protection of personal data of children, persons having lost or having been restricted in the capacity for civil acts and persons having cognitive difficulties or difficulties with behavioural control*

1. The protection of personal data of children, persons having lost or having been restricted in the capacity for civil acts, and persons having cognitive difficulties or difficulties with behavioural control shall comply with this Law.

2. In the case of a child, person having lost or having been restricted in the capacity for civil acts, or person having cognitive difficulties or difficulties with behavioural control, a legal representative shall, on his/her behalf, exercise the rights of the personal data subject, except for the cases stipulated in article 19.1 of this Law. The processing of children's personal data for the purpose of publicly disclosing or revealing information about private life and personal secrets of children who are seven or more years of age must be consented to by the children and their legal representatives.

3. The processing of personal data of a child, person having lost or having been restricted in the capacity for civil acts or person having cognitive difficulties or difficulties with behavioural control shall be suspended in the following cases:

   (a) The person who provided the consent as stipulated in clause 2 of this article withdraws his/her consent to the processing of personal data of such child or person, unless otherwise provided for by law;

(b) At the request of a competent agency when there are sufficient grounds to prove that the processing of personal data may infringe upon legitimate rights and interests of such child or person, unless otherwise provided for by law.

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

1. Responsibilities of agencies, organizations and individuals to protect personal data in recruitment of employees shall be prescribed as follows:

   (a) To only request provision of information for recruitment purposes of recruiting agencies, organizations and individuals in conformity with law; information provided shall only be used for recruitment purposes and other purposes as agreed in accordance with law;

   (b) Information provided must be processed in accordance with law and must be consented to by candidates;

   (c) Information provided by candidates must be deleted or destroyed in the case where they are not recruited, unless otherwise agreed with candidates;

2. Responsibilities of agencies, organizations and individuals to protect personal data in management and use of employees shall be prescribed as follows:

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

   (b) To store personal data of employees within the period prescribed by law or as agreed;

   (c) To delete or destroy employees' personal data upon termination of their contracts, unless otherwise agreed or stipulated by law.

3. The processing of employees' personal data which are collected by technological and technical measures in the management of employees shall be prescribed as follows:

   (a) Only applying technological and technical measures in conformity with law and ensuring rights and interests of personal data subjects, on the basis that employees are fully aware of such measures;

   (b) Not processing or using personal data collected from technological and technical measures in contravention of law.

Article 26 *Protection of personal data in respect of health information and in insurance business activities*

1. The protection of personal data in respect of health information and in insurance business activities shall be prescribed as follows:

   (a) Obtaining consent of personal data subjects in the process of collecting and processing personal data, except for the cases specified in article 19.1 of this Law;

   (b) Applying all the regulations on protection of personal data and other relevant laws.

2. Agencies, organizations and individuals operating in the health sector shall not provide personal data to any third parties which are organizations providing health care services or health insurance or life insurance services, except where personal data subjects so request in writing or [except for] the cases specified in article 19.1 of this Law.

3. Organizations and individuals developing health applications or insurance business applications must fully comply with the regulations on protection of personal data.

4. Where an enterprise conducts reinsurance business or cedes reinsurance and transfers personal data to any partner, it is required to be specified in the contracts with its customers.

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

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

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

   (b) Not to use credit information of personal data subjects for scoring, credit rating, credit information assessment, or creditworthiness assessment in respect of personal data subjects without their consent;

   (c) To only collect personal data which are necessary for credit information activities from sources in conformity with this Law and other relevant laws;

   (d) To notify personal data subjects of any revelation or loss of bank account information, financial information, credit and credit information.

2. Organizations and individuals conducting credit information activities shall be responsible to comply with this Law; apply measures to prevent and combat unauthorized access, use, disclosure and modification of personal data of customers; have solutions to restore customers' personal data in case of loss thereof; and keep confidentiality in the process of collecting, providing and processing personal data of customers servicing assessment of credit information.

3. The Government shall provide detailed regulations on this article.

Article 28 *Protection of personal data in business of advertising services*

1. Organizations and individuals conducting business of advertising services are only permitted to use customers' personal data transferred by personal data controllers or personal data controlling and processing parties as agreed or collected through their business activities to conduct business of advertising services. The collection, use and transfer of personal data must ensure the rights of personal data subjects as stipulated in article 4 of this Law.

2. Personal data controllers and personal data controlling and processing parties are only permitted to transfer personal data to organizations and individuals conducting business of advertising services in accordance with law.

3. The processing of personal data of customers for conducting business of advertising services must be consented to by customers on the basis that the customers explicitly know the contents, methods, forms and frequency of product introduction; and [on the basis of] provision of methods to customers which enable them to refuse to receive advertising information.

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

5. Personal data subjects have the right to request to stop receiving information from advertising services. Organizations and individuals conducting business of advertising services must provide the mechanism and stop [sending] advertising [information] at the request of personal data subjects.

6. Organizations and individuals conducting business of advertising services must not sublease or agree for other organizations and individuals to perform, on their behalf, all advertising services using personal data.

7. Organizations and individuals conducting business of advertising services shall be responsible for proving the use of personal data of customers for advertising; and complying with clauses 1, 2, 3 and 4 of this article and the law on advertising.

8. When using personal data for advertising based on behaviour or with specific objectives or for personalized advertising, organizations and individuals must comply with this article and the following provisions:

   (a) Only collecting personal data by way of monitoring electronic information pages, electronic information portals and applications with the consent of personal data subjects;

   (b) Establishing a method which allows personal data subjects to refuse to share data; determine the storage period; and delete or destroy data when they are no longer required.

Article 29 *Protection of personal data with respect to social networking platforms and online communication services*

Organizations and individuals providing social network services or online communication services shall have the following responsibilities:

1. To explicitly notify the contents of personal data collected when personal data subjects install and use social networks or online communication services; not to collect personal data illegally and outside the scope agreed with customers;

2. Not to request provision of images or videos containing all or part of contents of identification documents as account authentication factors;

3. To provide an option which allows users to refuse the collection and sharing of data files (called cookies);

4. To provide the option "not tracking" or to track the use of social networks and online communication services with the consent of users only;

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

6. To publicize security policies and explicitly explain how personal data are collected, used and shared; to provide users with mechanisms to access, modify and delete data, and set up the privacy for personal data, and report breaches in respect of security and privacy; to protect personal data of Vietnamese citizens when transferring data across borders; and to formulate the process of dealing with breaches in respect of the protection of personal data promptly and effectively.

Article 30 *Protection of personal data in processing of big data, artificial intelligence, blockchains, metaverse, cloud computing*

1. Personal data in the environments of big data, artificial intelligence, blockchains, virtual universe and cloud computing must be processed for correct purposes and limited to the extent as required, ensuring legitimate rights and interests of personal data subjects.

2. The processing of personal data in the environments of big data, artificial intelligence, blockchains, metaverse and cloud computing must be in compliance with this Law and other relevant laws; and in conformity with ethical standards, fine customs and traditions of Vietnam.

3. Systems and services using big data, artificial intelligence, blockchains, metaverse and cloud computing must be integrated with appropriate personal data security measures; must use appropriate methods for authentication and identification and delegate the authority to access in order to process personal data.

4. In the case of processing of personal data by artificial intelligence, it is required to classify [personal data] according to levels of risks in order to take appropriate measures to protect personal data.

5. Not to use or develop systems for processing big data, artificial intelligence, blockchains, metaverse, or cloud computing using personal data for the purpose of causing harm to national defence, national security, social order and safety or infringing upon the life, health, honor, dignity and assets of other people.

6. The Government shall provide detailed regulations on this article.

Article 31 *Protection of personal data with respect to personal location data and biometric data*

1. Personal location data means data which are determined through the positioning technology in order to know locations and help identify a specific natural person.

2. Biometric data means data on physical attributes, and unique and stable biological characteristics of a person to identify such person.

3. The protection of personal data with respect to personal location data shall be prescribed as follows:

   (a) Not applying location tracking via radio frequency identification cards and other technologies, unless there is consent of personal data subjects or a request of competent agencies as prescribed by law or [unless] otherwise provided for by law;

   (b) Organizations and individuals providing mobile application platforms must 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 personal location tracking options.

4. The protection of biometric data shall be prescribed as follows:

   (a) Agencies, organizations and individuals collecting and processing biometric data must take physical security measures for their biometric data storage and transmission devices; restrict access to biometric data; have a monitoring system to prevent and detect infringements of biometric data; and comply with law and relevant international standards;

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

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

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

(a) To perform the duties of national defence, protect national security, ensure social order and safety, and protect their legitimate rights and interests;

(b) Sound, images or other identifiable information collected from public activities including conferences, seminars, sports competitions, art performances and other public activities do not cause harm to the honor, dignity or reputation of personal data subjects;

(c) Other cases as prescribed by law.

2. In the case of audio or video recording as prescribed in clause 1 of this article, agencies, organizations and individuals are responsible to notify or communicate in any other form to personal data subjects that they are being audio or video recorded, unless otherwise provided for by law.

3. Personal data collected shall only be processed and used in conformity with the processing purposes, and must not be used for illegal purposes or infringement of legitimate rights and interests of personal data subjects.

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

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

Chapter III

FORCES AND CONDITIONS FOR ENSURING PROTECTION OF PERSONAL DATA

Article 33 *Forces protecting personal data*

1. Forces protecting personal data comprise:

(a) Specialized agency for personal data protection under the Ministry of Public Security;

(b) Departments and personnel protecting personal data in agencies and organizations;

(c) Organizations and individuals providing personal data protection services;

(d) Organizations and individuals mobilized to participate in protection of personal data.

2. Agencies and organizations shall be responsible to appoint departments and personnel who are qualified to protect personal data or hire organizations or individuals providing personal data protection services.

3. The Government shall stipulate conditions and duties of departments and personnel protecting personal data in agencies and organizations; organizations and individuals providing personal data protection services; and personal data processing services.

Article 34 *Standards and technical regulations on protection of personal data*

1. Standards on protection of personal data shall comprise the standards applicable to information systems, hardware, software, management, operation, processing and protection of personal data which are announced and recognized for application in Vietnam.

2. Technical regulations on protection of personal data shall comprise the technical regulations applicable to information systems, hardware, software, management, operation, processing and protection of personal data which are formulated, promulgated and applied in Vietnam.

3. Standards and technical regulations on protection of personal data shall be promulgated in accordance with the law on standards and technical regulations.

Article 35 *Inspection of activities of protection of personal data*

Activities of protection of personal data shall be inspected in accordance with this Law and Government regulations.

Chapter IV

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS FOR PROTECTING PERSONAL DATA

Article 36 *Responsibilities for State administration of personal data protection*

1. The Government shall exercise uniform State administration of personal data protection.

2. The Ministry of Public Security is the co-ordinating body and responsible to the Government for exercising State administration of personal data protection, except for the contents under the management of the Ministry of National Defence.

3. The Ministry of National Defence shall be responsible to the Government for exercising State administration of personal data protection under its management.

4. Ministries, ministerial equivalent agencies and Government agencies shall exercise State administration of personal data protection with respect to the industries and sectors under their management in accordance with law and their assigned functions and duties.

5. Provincial people's committees shall exercise State administration of personal data protection in accordance with law and their assigned functions and duties.

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

1. Responsibilities of personal data controllers shall be as follows:

   (a) To explicitly indicate responsibilities, rights and obligations to be complied with by the parties in an agreement or contract in relation to the processing of personal data in accordance with this Law and other relevant laws;

   (b) To decide on the purposes and means of processing personal data in the documents or agreements with personal data subjects, ensuring compliance with the principles and contents stipulated in this Law;

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

(d) To notify breaches of the regulations on protection of personal data as prescribed in article 23 of this Law;

(dd) To select a suitable personal data processor to process personal data;

(e) To ensure the rights of personal data subjects as prescribed in article 4 of this Law;

(g) To take responsibility to personal data subjects for damage caused by the processing of personal data;

(h) To prevent illegal collection of personal data from their systems, equipment and services;

(i) To coordinate with the Ministry of Public Security and competent State agencies in protection of personal data, and to provide information for investigating and dealing with breaches of the law on protection of personal data;

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

2. Responsibilities of personal data processors shall be as follows:

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

(b) To process personal data in strict accordance with contracts or agreements entered into with personal data controllers or personal data controlling and processing parties;

(c) To implement all the measures for protection of personal data in accordance with this Law and other relevant laws;

(d) To take responsibility to personal data controllers or personal data controlling and processing parties for damage caused by the processing of personal data;

(dd) To prevent illegal collection of personal data from their systems, equipment and services;

(e) To coordinate with the Ministry of Public Security and competent State agencies in protection of personal data, and to provide information for investigating and dealing with breaches of the law on protection of personal data;

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

3. Personal data controlling and processing parties shall be responsible to fully comply with clauses 1 and 2 of this article.

Chapter V

IMPLEMENTING PROVISIONS

Article 38 *Effectiveness*

1. This Law shall take effect from 1 January 2026.

2. Small enterprises and start-ups may or may not implement articles 21, 22 and 33.2 of this Law for a period of 5 years from the effective date of this Law, except for small enterprises and start-ups conducting business of personal data processing services, directly processing sensitive personal data or processing personal data of a large number of personal data subjects.

3. Business households and micro-enterprises are not required to implement articles 21, 22 and 33.2 of this Law, except for business households and micro-enterprises conducting business of personal data processing services, directly processing sensitive personal data or processing personal data of a large number of personal data subjects.

4. The Government shall provide detailed regulations on clauses 2 and 3 of this article.

Article 39 *Transitional provisions*

1. The processing of personal data currently carried out to which personal data subjects consented or as agreed in accordance with Decree No. 13/2023/ND-CP dated 17 April 2023 of the Government before the effective date of this Law shall continue to be carried out without obtaining the consent or reaching agreement again.

2. With respect to files on personal data processing impact assessment or files on overseas personal data transfer impact assessment in accordance with Decree No. 13/2023/ND-CP dated 17 April 2023 of the Government which were received by the specialized agency for personal data protection before the effective date of this Law, such files shall continue to be used, and it shall not be required to prepare files on personal data processing impact assessment or files on cross-border personal data transfer impact assessment in accordance with this Law; if any update is made to the files already prepared as stated above after the effective date of this Law, it shall be implemented in accordance with this Law.

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

CHAIRMAN OF THE NATIONAL ASSEMBLY
Tran Thanh Man