Allens

In alliance with Linklaters

DECREE 356/2025/ND-CP

PROVIDING DETAILED REGULATIONS ON A NUMBER OF ARTICLES AND MEASURES FOR IMPLEMENTATION OF THE LAW ON PROTECTION OF PERSONAL DATA

TABLE OF CONTENTS

CHAPTER I **1**

GENERAL PROVISIONS **1**

Article 1 *Governing scope* *1*
Article 2 *Applicable entities* *1*
Article 3 *List of basic personal data* *1*
Article 4 *List of sensitive personal data* *2*

CHAPTER II **3**

REQUIREMENTS AND CONDITIONS FOR PROTECTION OF PERSONAL DATA **3**

Article 5 *Exercise of rights of personal data subjects* *3*
Article 6 *Methods of expressing personal data subjects' consent* *4*
Article 7 *Transfer of personal data* *4*
Article 8 *Protection of personal data in financial, banking, and credit information activities* *6*
Article 9 *Protection of personal data in processing of big data* *6*
Article 10 *Protection of personal data in artificial intelligence systems and metaverse* *7*
Article 11 *Protection of personal data in blockchains* *8*
Article 12 *Protection of personal data in cloud computing* *8*
Article 13 *Conditions applicable to personal data protection personnel and personal data protection divisions in agencies and organizations* *9*
Article 14 *Duties of personal data protection divisions and personal data protection personnel in agencies and organizations* *10*
Article 15 *Individuals providing personal data protection services* *11*
Article 16 *Organizations providing personal data protection services* *11*

CHAPTER III **12**

APPLICATION FILES, SEQUENCE AND PROCEDURES IN RESPECT OF PERSONAL DATA **12**

Article 17 *Cross-border personal data transfer* *12*
Article 18 *Conditions, sequence, procedures for and components of files on cross-border personal data transfer impact assessment* *13*
Article 19 *Conditions, sequence, procedures for and components of files on personal data processing impact assessment* *14*
Article 20 *Update of files on personal data processing impact assessment and files on cross-border personal data transfer impact assessment* *16*
Article 21 *Personal data processing services* *16*
Article 22 *Conditions applicable to a personal data processing service business organization* *17*
Article 23 *Responsibilities of personal data processing service business organizations* *17*
Article 24 *Authority to issue, re-issue, replacement and revocation of certificates of satisfaction of conditions for business of personal data processing services* *18*
Article 25 *Application file, sequence and procedures for issuance of certificates of satisfaction of conditions for business of personal data processing services [certificates]* *18*

Article 26 *Application files, sequence and procedures for re-issuance and replacement of certificates of satisfaction of conditions for business of personal data processing services [certificates]* *19*
Article 27 *Revocation of certificates of satisfaction of conditions for business of personal data processing services [certificates]* *19*
Article 28 *Contents of notice of breach of regulations on protection of personal data* *20*
Article 29 *Notification of breach in respect of personal position data and biometric data* *20*

CHAPTER IV **21**

IMPLEMENTATION OF PERSONAL DATA PROTECTION WORK **21**

Article 30 *Responsibility to implement international cooperation on protection of personal data* *21*
Article 31 *Inspection of personal data protection activities* *21*
Article 32 *Research and development of solutions for personal data protection* *22*
Article 33 *Contents of State administration of protection of personal data* *23*
Article 34 *Responsibilities of the Ministry of Public Security* *23*
Article 35 *Responsibilities of the Ministry of National Defence* *24*
Article 36 *Responsibilities of the Ministry of Science and Technology* *24*
Article 37 *Responsibilities of ministries, ministerial equivalent agencies and Government agencies* *24*
Article 38 *Responsibilities of people's committees of provinces and cities under central authority* *25*
Article 39 *Specialized agency for personal data protection and national information portal on personal data protection* *25*
Article 40 *Funds for ensuring personal data protection activities* *25*

CHAPTER V **26**

ORGANIZATION OF IMPLEMENTATION **26**

Article 41 *Provisions on application of clauses 2 and 3 of article 38 of the Law on Protection of Personal Data* *26*
Article 42 *Effectiveness and responsibility for implementation* *26*

GOVERNMENT

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

No.: 356/2025/ND-CP

Ha Noi, 31 December 2025

DECREE
PROVIDING DETAILED REGULATIONS ON A NUMBER OF ARTICLES AND MEASURES FOR IMPLEMENTATION OF THE LAW ON PROTECTION OF PERSONAL DATA

Pursuant to the *Law on Organization of the Government* No. 63/2025/QH15;

Pursuant to the *Law on Protection of Personal Data* No. 91/2025/QH15;

Pursuant to the *Law on Data* No. 60/2024/QH15;

Pursuant to the *Law on Amendment of the Law on Tendering, the Law on Investment in the Public Private Partnership Form, the Law on Customs, the Law on Value Added Tax, the Law on Export and Import Duties, the Law on Investment, the Law on Public Investment, and the Law on Management of Use of Public Assets* No. 90/2025/QH15;

At the request of the Minister of Public Security;

The Government hereby promulgates the Decree providing detailed regulations on a number of articles and measures for implementation of the *Law on Protection of Personal Data*.

Chapter I

GENERAL PROVISIONS

Article 1 *Governing scope*

This Decree provides detailed regulations on the following articles: 2.2 and 2.3; 4.5; 6.3; 9.5; 17.3; 20.7; 21.7; 22.4; 23.5; 27.3; 30.6; 31.4(b); 33.3; 35; and 38.4 of the *Law on Protection of Personal Data* and regulates the measures for organization of implementation of the Law regarding research and development of solutions for protection of personal data, the specialized agency for personal data protection, the national information portal on personal data protection; responsibilities of ministries, branches and localities for protection of personal data; and funds for ensuring personal data protection activities.

Article 2 *Applicable entities*

1. Vietnamese agencies, organizations and individuals.

2. Foreign agencies, organizations and individuals in Vietnam.

3. Foreign agencies, organizations and individuals directly engaged in or involved in 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 3 *List of basic personal data*

Basic personal data shall comprise:

1. Surname, middle name and given name at birth, and other names (if any).

2. Date of birth; date of death or missing.

3. Gender.

4. Place of birth, registered place of birth declaration, registered permanent residential address, registered temporary residential address, current residential address, place of origin, and contact address.

5. Nationality.

6. Individual's photo.

7. Telephone number, personal identification number, passport number, driver's licence number, and vehicle registration plate number.

8. Marital status.

9. Information about the family relationship (parents, children or spouse).

10. Information about the digital account of the individual.

11. Other information associated with a specific person or helping identify a specific person which is not stipulated in article 4 of this Decree.

Article 4 *List of sensitive personal data*

1. Sensitive personal data shall comprise:

   (a) Data revealing racial origins and ethnic origins;

   (b) Viewpoints on politics, religion and belief;

   (c) Information about private life, personal secrets and family secrets;

   (d) Health status;

   (dd) Biometric data and genetic characteristics;

   (e) Data revealing sexual life and sexual orientation of an individual;

   (g) Data on crimes and breaches of law as collected and stored by law enforcement agencies;

   (h) Positions of individuals determined via positioning services;

   (i) Information about usernames and passwords for accessing electronic identification accounts of individuals; images of identity cards, citizen's identity cards and people's identity cards;

   (k) Usernames and passwords for access to bank accounts; bank card information, and data on transaction history of bank accounts; financial, credit information and information about financial, securities and insurance transaction history and activities of clients at credit institutions, foreign bank branches, organizations providing services of intermediary payment, securities and insurance, and other licensed organizations;

   (l) Data monitoring acts and activities of using telecom services, social media, online

communication services and other services in cyberspace;

(m) Other personal data required to be kept confidential by law or requiring strict security measures.

2. During the processing of sensitive personal data, agencies and organizations must formulate regulations on limited authorization of access, procedures for processing and security measures.

Chapter II

REQUIREMENTS AND CONDITIONS FOR PROTECTION OF PERSONAL DATA

Article 5 *Exercise of rights of personal data subjects*

1. Personal data controllers, and personal data controlling and processing parties must formulate clear processes, procedures and standard forms to exercise rights of personal data subjects in conformity with the personal data processing activities and responsibilities of related divisions; and ensure that personal data subjects are notified of the procedures for exercise of the rights prescribed in article 4.1 of the *Law on Protection of Personal Data*.

2. Upon receipt of a request for withdrawal of the consent to the processing of personal data, restriction on the processing of personal data, or objection to the processing of personal data in strict accordance with the procedures from a personal data subject, the personal data controller or the personal data controlling and processing party must provide a response within 2 working days, and provide the personal data subject with complete information about the procedures for ceasing the processing of personal data and implement [such request] within 15 days, except for the cases of processing of personal data without consent of personal data subjects as stipulated in article 19 of the *Law on Protection of Personal Data*. Where it is necessary to request the personal data processor or a third party to cease the processing of personal data of the personal data subject, it shall be implemented within 20 days.

   Depending on the nature and complexity of the request, if it is necessary to extend the period of implementation, the extension shall be made no more than once for a period of no more than 15 days, and the personal data controller or the personal data controlling and processing party shall notify the personal data subject of the reasons for extension and shall be responsible to prove that the extension is necessary and reasonable.

3. Upon receipt of a request for review or revise, or a request for revision of personal data or provision of personal data in strict accordance with the procedures from a personal data subject, the personal data controller or the personal data controlling and processing party must provide a response within 2 working days, and provide the personal data subject with complete information about the procedures and implement [such request] within 10 days. Where it is necessary to request the personal data processor or a third party to revise personal data of the personal data subject, it shall be implemented within 15 days.

   Depending on the nature and complexity of the request, if it is necessary to extend the period of implementation, the extension shall be made no more than once for a period of no more than 10 days, and the personal data controller or the personal data controlling and processing party shall notify the personal data subject of the reasons for extension and shall be responsible to prove that the extension is necessary and reasonable.

4. Upon receipt of a request for deletion of personal data in strict accordance with the procedures from a personal data subject, the personal data controller or the personal data controlling and processing party must provide a response within 2 working days, and provide the personal data subject with complete information about the procedures and implement [such request] within 20 days. Where it is

necessary to request the personal data processor or a third party to provide, delete or restrict the processing of data of the personal data subject, it shall be implemented within 30 days.

Depending on the nature and complexity of the request, if it is necessary to extend the period of implementation, the extension shall be made no more than once for a period of no more than 20 days, and the personal data controller or the personal data controlling and processing party shall notify the personal data subject of the reasons for extension and shall be responsible to prove that the extension is necessary and reasonable.

5. Upon receipt of a request for implementation of the measures or solutions for protection of personal data in strict accordance with the procedures from a personal data subject, the competent agency or any agency, organization or individual involved in the processing of personal data must provide a response within 2 working days, and provide the personal data subject with complete information about the procedures and implement [such request] within 15 days.

   Depending on the nature and complexity of the request, if it is necessary to extend the period of implementation, the extension shall be made no more than once for a period of no more than 15 days, and the personal data controller or the personal data controlling and processing party shall notify the personal data subject of the reasons for extension and shall be responsible to prove that the extension is necessary and reasonable.

Article 6 *Methods of expressing personal data subjects' consent*

1. Methods of obtaining the consent of personal data subjects must ensure the ability to verify the identification of personal data subjects who have given consent, and the time and contents to which the consent was given, comprising:

   (a) In writing;

   (b) By recorded phone calls;

   (c) By using the "agree" syntax via phone text messages;

   (d) Via emails, electronic information pages, platforms, and applications which are technically set up to obtain consent;

   (dd) By other appropriate methods which enable the printing and copying in writing, including in the electronic form or in a verifiable format.

2. Personal data controllers and personal data controlling and processing parties must store personal data subjects' consent. If any dispute arises, the responsibility to prove the consent of the personal data subject shall belong to the personal data controller or the personal data controlling and processing party.

3. Personal data controllers and personal data controlling and processing parties are not permitted to set the default consent mode or create unclear instructions which cause confusion between consent and non-consent to data subjects. Available default settings must ensure the principles of protection of personal data, and respect of rights of personal data subjects.

4. For obtaining consent to the processing of sensitive personal data, data subjects must be notified that the data to be processed is sensitive personal data.

Article 7 *Transfer of personal data*

1. Any organization or individual transferring personal data in accordance with sub-clauses (a), (c) and (d) of article 17.1 of the Law on Protection of Personal Data must prepare a personal data transfer

agreement with the personal data recipient, specifying the following contents:

(a) Purpose of the transfer;

(b) Entities being personal data subjects and type of personal data to be transferred in conformity with the purpose of the transfer;

(c) Period of processing of personal data, and requirements on deletion and destruction of personal data after completion of the purpose of the transfer;

(d) Legal bases for the transfer of personal data;

(dd) Responsibilities for protection of personal data during the transfer and processing of personal data;

(e) Responsibilities for exercise of the rights of personal data subjects;

(g) Responsibilities of the parties for coordination and compliance in the case of discovery of any breach of the regulations on protection of personal data.

2. The transfer of sensitive personal data shall require physical security measures with respect to storage and transmission facilities, measures for encryption and anonymisation of personal data, and other security measures during the transfer.

3. In the case of transfer of personal data in accordance with sub-clauses (a) and (d) of article 17.1 of the *Law on Protection of Personal Data* with collection of fees for the purpose of providing services to personal data subjects or for the purpose of serving lawful interests of personal data subjects, the organization or individual [conducting the transfer] must comply with the following provisions:

(a) [Such organization or individual] must set up a technical system and a transparent mechanism in order for personal data subjects to give their consent in a correct and clear manner on each occasion of transfer on the basis that [personal data subjects] are correctly notified of the purpose of transfer and of organizations and individuals receiving and processing personal data;

(b) [Such organization or individual] is only permitted to process personal data correctly for the purposes of the transfer to which personal data subjects gave consent and in conformity with the registered business lines;

(c) Types of personal data to be transferred must be limited to the scope of the purposes of the transfer;

(d) [Such organization or individual] is not permitted to collect, store or form a storage of personal data from the transfer of personal data for purposes other than those consented to by personal data subjects;

(dd) [Such organization or individual must] clearly define the roles of the personal data controller, the personal data processor and third parties in the personal data transfer activities;

(e) [Such organization or individual] must have agreements on transfer and processing of personal data before transfer and commitments on responsibilities and obligations with respect to personal data subjects.

4. Where personal data are shared among divisions in the same agency or organization in order to process personal data for established purposes of processing, the agency or organization must develop a process of controlling the sharing and use of personal data in compliance with regulations;

and have measures for preventing personnel within the agency or organization from illegally sharing personal data with third parties.

5. Personal data must be de-identified prior to trading on the data floor.

6. Agencies, organizations and individuals providing personal data in accordance with article 15.2 of the *Law on Protection of Personal Data* based on each specific request of data subjects shall not be deemed to transfer data and shall not be required to comply with this article.

Article 8 *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 are responsible to apply standards and technical regulations on protection of personal data, and technical regulations on de-identification of personal data and anonymisation of personal data as promulgated and applied in Vietnam; to conduct assessment of the compliance with the regulations on protection of personal data once a year; and to record a log of all personal data processing activities.

2. When organizations and individuals operating in the sectors of finance, banking and credit information activities and being personal data controllers or personal data controlling and processing parties seek consent of personal data subjects, they must specify:

   (a) Purposes of processing personal data, including scoring, credit rating, credit information assessment, or creditworthiness assessment, if any;

   (b) Sources for collection of personal data and related parties collecting and sharing personal data;

   (c) Duration of storage of personal data;

   (d) Mechanisms and methods of withdrawing consent and policies for deletion and destruction of personal data in accordance with regulations.

3. Within no more than 72 hours after discovering the revelation or loss of sensitive personal data of a personal data subject in the sector of finance, banking or credit information activities, the organization or individual directly collecting personal data of the data subject shall be responsible to provide a notice to the specialized agency for personal data protection and the personal data subject thereof. Such notice must at least contain the contents stipulated in article 28.1 of this Decree.

Article 9 *Protection of personal data in processing of big data*

1. *Processing of big data containing personal data* means the activity of processing personal data which is conducted on a large scale with continuity, integration from different sources, and ability to analyse conducts, forecast tendencies or classify users.

2. In the case of processing of big data containing personal data, related agencies, organizations and individuals are responsible:

   (a) To comply with the regulations on protection of personal data during the processing of data immediately from the time of commencement of the processing;

   (b) To collect, process and store personal data only within the correct scope and for specific and clear purposes;

   (c) To formulate policies for storage, deletion and destruction of personal data which conform and comply with law;

(d) To organize periodical training, dissemination and increase in awareness of personal data security and measures for personal data protection for their employees, especially personnel directly processing personal data. To enhance awareness of the importance of personal data protection in the organization;

(dd) To enter into agreements with third parties, partners and service providers in order to ensure that the regulations on protection of personal data are fully complied with;

(e) To formulate appropriate mechanisms for notification and explanation to data subjects on use of their personal data in the big data analysis system.

3. Agencies, organizations and individuals shall apply measures for protection of personal data during the processing of big data, comprising:

(a) Applying measures for ensuring cybersecurity, data security, and prevention of loss of personal data during the storage, processing and transmission of personal data;

(b) Using strong authentication methods, requiring at least multi-factor authentication (password, PIN combined with a one-time password, digital signature device or biometric factor) in conformity with the sensitivity of personal data; implementing access authorization to ensure that only authorized persons are able to access personal data;

(c) Conducting encryption or anonymisation of personal data (being the process of separating data which identify a specific person for separate storage and security whereby after this process, personal data shall be used for processing without being able to identify a specific person) during the transfer or provision of personal data, unless otherwise stipulated in specialized law or except where the processing requires plaintext data for the purpose of prevention of crimes, anti-money laundering, assurance of national security, and dealing with claims and disputes of clients. In these cases, agencies and organizations must apply additional security solutions in order to ensure that personal data is not illegally accessed or used;

(d) Conducting continuous supervision, and using supervisory tools to monitor the access to personal data and discover abnormal conducts;

(dd) Conducting periodical inspection and assessment of cybersecurity and data security in order to discover, prevent and remedy security vulnerabilities.

Article 10 *Protection of personal data in artificial intelligence systems and metaverse*

1. Organizations and individuals are entitled to use personal data for research and development of self-learning algorithms, artificial intelligence systems and other automatic systems but are required to comply with the regulations on protection of personal data.

2. If data obtained from the artificial intelligence inference results may be used to identify or help identify a specific person, measures for protection of personal data must be applied in accordance with law.

3. Personal data controllers and personal data controlling and processing parties are responsible to notify data subjects of the automatic processing of personal data, explain operating principles of algorithms and effects on lawful rights and interests of data subjects; and provide options for data subjects to opt out.

4. *Metaverse* means a digital technical universe which combines aspects of social media, online games, augmented reality (AR), virtual reality (VR), Internet and cryptocurrency to enable users to use virtual reality technologies for interaction.

5. Organizations and individuals shall apply measures for protection of personal data in artificial intelligence systems and the metaverse, comprising:

   (a) Researching, building and deploying systems which satisfy the standards on cybersecurity, the standards on comprehensive protection of data for artificial intelligence systems, especially focusing on the following factors: information security, reliability of algorithms, system stability and ability to prevent cyber attacks;

   (b) Establishing mechanisms for supervision of operation of artificial intelligence systems in two aspects: supervision by competent State agencies; accountability of personal data controllers or personal data controlling and processing parties with respect to personal data subjects;

   (c) Formulating mechanisms for protection of personal data in accordance with appropriate standards, and developing systems of supervision and early warning of cybersecurity dangers;

   (d) Establishing mechanisms to control and prevent the abuse of artificial intelligence and the metaverse in activities of infringement of national security, and social order and safety;

   (dd) Conducting assessment of the compliance with the regulations on protection of personal data once every year.

6. Personal data subjects must have the right to revise, anonymise and delete identification files, even when platforms store behavioural history.

Article 11 *Protection of personal data in blockchains*

1. When processing personal data in blockchains, related agencies, organizations and individuals are responsible to comply with the regulations on protection of personal data immediately in the process of research and development of products, services, applications and systems using blockchains, and in the processing of personal data.

2. Agencies, organizations and individuals shall apply measures for protection of personal data when processing personal data in blockchains, comprising:

   (a) Only applying encryption algorithms, hashing algorithms, and digital signature algorithms ensuring safety;

   (b) Not directly storing personal data on blockchains, and only storing personal data which has been de-identified or storing hash values of personal data;

   (c) Conducting assessment of the compliance with the regulations on protection of personal data once every year.

Article 12 *Protection of personal data in cloud computing*

1. Related agencies, organizations and individuals must apply technical and organizational measures to prevent unauthorized access to personal data when performing cloud computing services.

2. Any organization or individual entering into a contract in relation to the processing of personal data with any cloud computing service provider shall have the following responsibilities:

   (a) To specify the compliance with the law of Vietnam on protection of personal data in the contract; to provide information about the personal data protection division or personnel; to comply with administrative procedures in relation to the protection of personal data in accordance with law;

(b) To clearly determine personal data processing streams, and roles of the parties in the activities of providing cloud computing services and corresponding responsibilities;

(c) To require that security, technical and organizational measures are specified in the contract;

(d) To immediately notify the related parties of any change which may affect personal data;

(dd) To comply with the duration of processing personal data, and the requirements on deletion and destruction of personal data;

(e) To ensure the exercise of rights of personal data subjects;

(g) To implement all technical measures to ensure that the access to personal data is reasonably authorized.

3. Cloud computing service providers shall:

(a) Comply with the regulations of Vietnam on protection of personal data, provide information about personal data protection divisions and personnel, and comply with administrative procedures in relation to the protection of personal data in accordance with law;

(b) Request sub-contractors to comply with personal data protection regulations and obligations in accordance with law;

(c) Apply technical and organizational measures to the extent that conforms with their scale and level of processing personal data;

(d) Conduct assessment of the compliance with the regulations on protection of personal data once every year.

4. Personal data on cloud computing must be encrypted in the resting and transmitting state, together with strict access authorization.

Article 13 *Conditions applicable to personal data protection personnel and personal data protection divisions in agencies and organizations*

1. The appointment of personal protection data or a personal data protection division [in an agency or organization] must be made in the form of an official document of such agency or organization; and must reflect the assignment of work, functions, duties, powers and other requirements with respect to the personal data protection work in such agency or organization.

2. Personal data protection personnel appointed by an agency or organization must satisfy all of the following capability conditions:

(a) Have a college degree or higher;

(b) Have at least 2 years of working experience (from the date of graduation) relating to one of the following sectors: legal affairs, information technology, cybersecurity, data security, risk management, compliance control, personnel management, and personnel organization;

(c) Have completed training and retraining on legal knowledge and professional skills of personal data protection.

3. Where an agency or organization establishes a personal data protection division, personnel in such division must satisfy all of the capability conditions stipulated in clause 2 of this article.

4. Agencies and organizations are responsible to assess and select personal data protection personnel.

5. Agencies and organizations shall enter into confidentiality agreements with personal data protection personnel, and may agree on cases of exemption of liabilities when there is a breach or damage to protected personal data.

6. Agencies and organizations appointing personal data protection personnel or personal data protection divisions are responsible to arrange training and retraining on knowledge and skills of personal data protection for personal data protection personnel.

Article 14 *Duties of personal data protection divisions and personal data protection personnel in agencies and organizations*

1. A personal data protection division shall have the following functions and duties:

   (a) To organize formulation of policies, procedures, regulations and standard forms to comply with the law on protection of personal data;

   (b) To organize exercise of rights of personal data subjects;

   (c) To periodically organize assessment of the actual status of compliance with the law on protection of personal data by the organization by reports on assessment of the level of performance of obligations stipulated by law in order to propose measures for increasing the efficiency of compliance with law, and preventing and controlling risks in personal data processing activities;

   (d) To prepare files on cross-border personal data transfer impact assessment and files on personal data processing impact assessment, and to receive and report breaches in terms of personal data protection and implement other requirements of competent agencies in accordance with regulations;

   (dd) To formulate plans and implement periodical training and retraining on protection of personal data in the agency or organization;

   (e) To organize implementation of technical measures for maintaining confidentiality of personal data, standards and regulations on protection of personal data, and plans on emergency response to incidents regarding the protection of personal data;

   (g) To conduct research and propose decisions relating to the personal data protection.

2. Personal data protection personnel shall have the following duties:

   (a) To provide advice on formulating policies, procedures, regulations and standard forms to comply with the law on protection of personal data;

   (b) To participate in the exercise of rights of personal data subjects;

   (c) To participate in periodical assessment of the actual status of compliance with the law on protection of personal data and propose measures for increasing the efficiency of compliance with law, and preventing and controlling risks;

   (d) To prepare files on cross-border personal data transfer impact assessment and files on personal data processing impact assessment, and to receive and report breaches in terms of personal data protection and implement other requirements of competent agencies in accordance with regulations;

(dd) To attend retraining courses and programs on protection of personal data;

(e) To participate in implementing technical measures for maintaining confidentiality of personal data, standards and regulations on protection of personal data, and plans on emergency response to incidents regarding the protection of personal data.

Article 15 *Individuals providing personal data protection services*

1. Individuals providing personal data protection services shall be the persons who satisfy all the capability conditions stipulated in clause 2 of this article, and shall be employed by agencies and organizations to act as personal data protection personnel.

2. An individual providing personal data protection services must satisfy all the following capability:

(a) Have a college degree or higher;

(b) Have at least 3 years of working experience (from the date of graduation) relating to one of the following sectors: legal affairs, personal data processing, cybersecurity, data security, risk management, and compliance control;

(c) Have completed intensive training and retraining on legal knowledge and professional skills of personal data protection.

3. Agencies and organizations with the need to employ individuals providing personal data protection services shall consider the capability conditions stipulated in clause 2 of this article, and enter into a contract for employment of personal data protection personnel; and publicly disclose information about personal data protection personnel to personal data subjects and related parties.

4. Individuals providing personal data protection services shall be responsible:

(a) To perform services in strict accordance with the scope and duties stated in the contract or agreement;

(b) Not to take advantage of the provision of services to commit a breach of law;

(c) To delete and destroy personal data processed during the provision of services upon completion of the contract and in accordance with law.

Article 16 *Organizations providing personal data protection services*

1. An organization providing personal data protection services [must satisfy the following conditions]:

(a) Being an organization or enterprise with functions or duties, or business lines in technology, legal affairs, or consultancy on technology or legal affairs which is hired by other agencies or organizations to provide consultancy on compliance with the regulations on protection of personal data and perform the duties of personal data protection as agreed;

(b) Having at least 3 employees who satisfy all the capability conditions stipulated in article 15.2 of this Decree;

(c) Having provided products and services related to security, cybersecurity, information technology, assessment of standards, and consultancy on personal data protection.

2. Any organization providing personal data protection services must formulate a capability file to prove its ability to protect personal data and provide same to agencies and organizations which have the

need to use such services. The file must reflect the business lines and sectors; scale and scope of and experience in provision of services; policy on provision of services; standards, qualifications and capability of personnel; and relevant supporting documents and materials.

3. Any agency or organization wishing to hire personal data protection services shall review the capability file [of a personal data protection organization], and enter into a service use contract and an agreement on personal data processing with the personal data protection organization; and publicly disclose information about such personal data protection organization to personal data subjects and related parties.

4. An agency or organization may, depending on its needs, concurrently appoint personal data protection personnel or a personal data protection division and hire an individual or organization providing personal data protection services.

5. Based on the agreement with the agency or organization hiring personal data protection services, the organization providing personal data protection services shall perform the duties of a personal data protection division for such agency or organization.

6. An organization providing personal data protection services shall be responsible:

   (a) To perform services in strict accordance with the scope and duties stated in the contract or agreement;

   (b) Not to take advantage of the provision of services to commit a breach of law;

   (c) To delete and destroy personal data processed during the provision of services upon completion of the contract and in accordance with law.

Chapter III

APPLICATION FILES, SEQUENCE AND PROCEDURES IN RESPECT OF PERSONAL DATA

Article 17 *Cross-border personal data transfer*

1. Personal data controllers, personal data controlling and processing parties, personal data processors and third parties shall conduct cross-border personal data transfer in the following cases:

   (a) Personal data storage activities involve the transfer of personal data collected or stored in Vietnam to a server system located outside the territory of the Socialist Republic of Vietnam or on cloud computing services of an overseas service provider;

   (b) Personal data is transferred from an agency, organization or individual in Vietnam to a recipient being an organization or individual overseas;

   (c) Personal data collected in Vietnam is processed and then transferred to a platform outside the territory of the Socialist Republic of Vietnam for further processing.

2. The specialized agency for personal data protection shall make a decision requesting a cross-border data transferor to cease the cross-border personal data transfer in the following cases:

   (a) It is discovered that personal data transferred is used for activities of infringement of national defence and national security;

   (b) There is a breach of the regulations on protection of personal data, which may harm national defence and national security.

3. In the cases other than those prescribed in sub-clauses (a), (b) and (c) of article 20.6 of the Law on Protection of Personal Data, it is not required to implement the provisions on assessment of impact of cross-border personal data transfer, comprising:

   (a) Press and communication activities in accordance with law;

   (b) Cross-border transfer of personal data which has been publicly disclosed in accordance with law;

   (c) In emergency situations where it is actually necessary to provide personal data across borders in order to protect the life, health and safety of assets of individuals; and in order to perform duties and obligations in accordance with law;

   (d) Cross-border personal data transfer for cross-border management of personnel in accordance with the rules and regulations on labour and collective labour agreements in accordance with law;

   (dd) Cross-border personal data provision for entering into contracts or implementing the procedures relating to cross-border transportation, logistics, money transfer, payment, hotels, application for visas, and application for scholarships.

Article 18 *Conditions, sequence, procedures for and components of files on cross-border personal data transfer impact assessment*

1. Agencies, organizations and individuals engaged in cross-border personal data transfer activities in accordance with article 20.1 of the Law on Protection of Personal Data must prepare a file on cross-border personal data transfer impact assessment in accordance with this article.

2. A file on cross-border personal data transfer impact assessment shall comprise:

   (a) Report on cross-border personal data transfer impact assessment in accordance with Form No. 09 in the Appendix of this Decree;

   (b) Copy of the contract or document on personal data transfer which is binding upon and reflects responsibilities between the organizations and individuals transferring and receiving personal data across borders;

   (c) Policies, procedures, regulations, standard forms and other documents in relation to protection of personal data of the agency, organization or individual engaged in cross-border personal data transfer activities.

3. A report on cross-border personal data transfer impact assessment shall contain the following contents:

   (a) Information about and contact details of the personal data transferor, the personal data recipient, the personal data processor and other parties involved in the cross-border personal data transfer activities;

   (b) Contact details of the personal data protection division or personnel; and of the organizations or individuals providing personal data protection services (if any) to the personal data transferor and the personal data recipient;

   (c) Description and interpretation of the purpose of cross-border personal data transfer, type of personal data to be transferred across borders, details of the cross-border personal data transfer and processing activities and diagram showing personal data processing streams;

(d) Description and interpretation of how to seek consent of personal data subjects, and policy for storage, deletion and destruction of personal data;

(dd) Plan for ensuring safety of personal data after cross-border transfer, measures for protection of personal data, and standards for protection of personal data which are applied;

(e) Diagram and description of features of the system of storage and processing of personal data after receiving personal data across borders;

(g) Process of transfer or provision of personal data by the cross-border personal data recipient to a third party;

(h) Results of self-assessment of the compliance with the regulations on protection of personal data provided by the agency, organization or individual engaged in cross-border personal data transfer activities;

(i) Assessment of the level of protection of personal data of the personal data recipient; the level of effect and risk of the cross-border personal data transfer and processing; possible unexpected consequences and damage, and measures for mitigation or elimination of such danger or risk.

4. The file on cross-border personal data transfer impact assessment must be available at all times for the purpose of serving the inspection and assessment conducted by the specialized agency for personal data protection.

The cross-border personal data transferor shall submit one original copy of the complete file online or directly or via postal services to the specialized agency for personal data protection together with Form No. 01a/01b in the Appendix of this Decree within 60 days from the date of cross-border personal data transfer.

5. The specialized agency for personal data protection shall assess and return results stating whether the file on cross-border personal data transfer impact assessment satisfies requirements within 15 days.

6. The specialized agency for personal data protection shall conduct assessment and request the cross-border personal data transferor to complete the file within 30 days if the file is incomplete and does not comply with regulations. Where the personal data transferor fails to complete the file in accordance with regulations, the specialized agency for personal data protection shall consider and apply the regulations on administrative penalties in the personal data protection sector.

7. The cross-border personal data transferor shall update and supplement the file cross-border personal data transfer impact assessment in accordance with article 20 of this Decree.

Article 19 *Conditions, sequence, procedures for and components of files on personal data processing impact assessment*

1. Personal data controllers, personal data controlling and processing parties, and personal data processors shall prepare and store their files on personal data processing impact assessment from the date of commencement of personal data processing.

2. The file on personal data processing impact assessment prepared by a personal data controller, personal data controlling and processing party or personal data processor shall comprise:

(a) Report on personal data processing impact assessment in accordance with Form No. 10 in the Appendix of this Decree;

(b) Copy of the contract or agreement on personal data processing which is binding upon and reflects responsibilities between organizations and individuals in the personal data processing activities;

(c) Policies, procedures, regulations, standard forms and other documents in relation to protection of personal data of the personal data controller, the personal data controlling and processing party or the personal data processor.

3. A report on personal data processing impact assessment shall contain the following contents:

(a) Information about and contact details of the personal data controller, the personal data controlling and processing party, the personal data processor or a third party;

(b) Contact details of the personal data protection division or personnel; and of the organization or individual providing personal data protection services (if any) to the personal data controller, the personal data controlling and processing party, the personal data processor or a third party;

(c) Description and interpretation of the purpose of personal data processing, type of personal data to be processed, details of personal data processing activities and diagram showing personal data streams;

(d) Description and interpretation of how to seek consent of personal data subjects, and policy for storage, deletion and destruction of personal data;

(dd) Plan for ensuring safety of personal data, measures for protection of personal data, system design diagram, and standards for protection of personal data which are applied;

(e) Results of assessment of the compliance with the regulations on protection of personal data;

(g) Assessment of the level of effect and risk of the personal data processing activities; possible unexpected consequences and damage, and measures for mitigation or elimination of such danger or risk.

4. The file on personal data processing impact assessment must be available at all times for the purpose of serving the inspection and assessment conducted by the specialized agency for personal data protection, and one original copy of the file together with Form No. 02a/02b in the Appendix of this Decree shall be submitted online or directly or via postal services to the specialized agency for personal data protection within 60 days from the date of processing of personal data.

5. The specialized agency for personal data protection shall assess and return results stating whether the file on personal data processing impact assessment satisfies requirements within 15 days.

6. The specialized agency for personal data protection shall conduct assessment and request the personal data controller, the personal data controlling and processing party or the personal data processor to complete the file within 30 days if the file is incomplete and does not comply with regulations. Where the personal data controller, the personal data controlling and processing party or the personal data processor fails to complete the file in accordance with regulations, the specialized agency for personal data protection shall consider and apply the regulations on administrative penalties in the personal data protection sector.

7. The personal data controller, the personal data controlling and processing party or the personal data processor shall update and supplement the file on personal data processing impact assessment in accordance with article 20 of this Decree.

Article 20 *Update of files on personal data processing impact assessment and files on cross-border personal data transfer impact assessment*

1. Files on cross-border personal data transfer impact assessment and files on personal data processing impact assessment shall be updated every 6 months from the initial submission of the file in the following cases:

   (a) When there is a new purpose of personal data transfer or personal data processing;

   (b) When there is [an issue] arising [in relation to] or a change of the personal data controller, the personal data controlling and processing party, the personal data processor or a third party.

2. The changes required to be immediately updated within 10 days shall comprise the following:

   (a) An agency, organization or unit is subject to re-organization, termination of operation, dissolution or bankruptcy in accordance with law;

   (b) There is a change to information about the organization or individual providing personal data protection services;

   (c) The business lines or services relating to personal data processing which have been registered in the file on personal data processing impact assessment or the file on cross-border personal data transfer impact assessment arise or are changed.

3. A file on personal data processing impact assessment or a file on cross-border personal data transfer impact assessment shall be updated in accordance with Form No. 03a/03b in the Appendix of this Decree and shall be submitted online or directly or via postal services to the specialized agency for personal data protection.

Article 21 *Personal data processing services*

1. Services of providing and operating automatic systems and software to conduct personal data processing on behalf of a personal data controller or a personal data controlling and processing party.

2. Services of scoring, ranking and assessment of creditworthiness of personal data subjects.

3. Services of online collection and processing of personal data from websites, applications, software and social media.

4. Services of collection and processing of personal data via websites, applications and software in respect of health care, health monitoring and medical services.

5. Services of collection and processing of personal data via educational applications and software involving supervision elements such as roll call, video recording, behaviour scoring, and emotion identification.

6. Services of analysis and exploitation of personal data, comprising: use of analysis tools for searching information, trends and patterns from personal data; application of methods of exploitation of data for extracting values from personal data, predicting users' behaviour or optimizing services.

7. Services of encryption of personal data during the transmission and storage.

8. Services of automatic personal data processing based on the big data technology, artificial intelligence, blockchains and metaverse.

9. Application platform services of providing personal position data.

Article 22 *Conditions applicable to a personal data processing service business organization*

1. The organization must be an organization or enterprise established and operating in accordance with the laws of Vietnam, and satisfying the conditions stipulated in this article.

2. [The organization must satisfy the following] conditions on personnel:

   (a) The head in charge of professional matters in respect of personal data processing of the organization must be a Vietnamese citizen and must permanently reside in Vietnam;

   (b) There is a management and executive team which satisfies the professional requirements on personal data processing;

   (c) There are at least 3 staff members who satisfy the capability conditions stipulated in article 13.2 of this Decree.

3. The organization must have infrastructure, equipment systems, physical facilities and technology in conformity with the personal data processing services.

4. The organization must obtain satisfactory results with respect to the file on personal data processing impact assessment or the file on cross-border personal data transfer impact assessment if the organization is engaged in cross-border personal data transfer.

Article 23 *Responsibilities of personal data processing service business organizations*

1. To fully comply with the law on protection of personal data; and responsibilities and obligations of personal data controlling and processing parties or personal data processors.

2. To formulate a risk management framework on protection of personal data in conformity with the services provided.

3. To conduct assessment of the current status of compliance and the creditworthiness in respect of protection of personal data once every year.

4. To apply standards and regulations relating to data security, protection of personal data, and cybersecurity.

5. To formulate regulations on responsibilities and powers of the organization during the personal data processing.

6. To ensure that the personal data processing is conducted for correct purposes, and to restrict the collection, transfer and storage in compliance with and in accordance with law; to prevent unauthorized access, collection, use, disclosure or similar risks in the personal data processing activities.

7. If the organization is a personal data processor, it shall request the personal data controller to seek consent of data subjects in accordance with regulations before providing services, and shall ensure that personal data subjects are notified of the type of personal data to be processed, the purpose of the processing and the organization providing personal data processing services.

8. To carry out the organization identity authentication in accordance with the law on electronic identification and authentication.

Article 24 *Authority to issue, re-issue, replacement and revocation of certificates of satisfaction of conditions for business of personal data processing services*

1. The Ministry of Public Security shall issue, re-issue, replace and revoke certificates of satisfaction of conditions for provision of personal data processing services.

2. The Minister of Public Security shall assign the specialized agency for personal data protection to issue, re-issue, replace and revoke certificates of satisfaction of conditions for provision of personal data processing services in accordance with regulations.

Article 25 *Application file, sequence and procedures for issuance of certificates of satisfaction of conditions for business of personal data processing services [certificates]*

1. The application file for issuance of a certificate shall comprise:

   (a) Application for issuance of a certificate in accordance with Form No. 04 in the Appendix of this Decree;

   (b) Copy of the enterprise registration certificate;

   (c) Letter appointing a personal data protection division or contract on use of personal data protection services in accordance with regulations;

   (d) Proposal for issuance of a certificate;

   (dd) Credentials and other supporting documents of personnel as stipulated in article 22.2(c) of this Decree;

   (e) The applicant is not required to submit the document prescribed in sub-clause (b) of this clause if the State agency can retrieve it on the database.

2. The proposal for issuance of a certificate shall contain the following contents:

   (a) Necessity and objectives;

   (b) Contents and sectors requested for approval;

   (c) Business lines and sectors, and business plan;

   (d) Proposed scale of personal data processing activities;

   (dd) Risk management framework on protection of personal data;

   (e) Plan for periodical assessment of the current status of compliance and the creditworthiness in respect of protection of personal data;

   (g) Application of standards and regulations in relation to data security and protection of personal data;

   (h) Plan for use of electronic identification and authentication services;

   (i) Responsibilities and powers of the applicant for personal data processing;

   (k) Qualified personnel in accordance with regulations.

3. The applicant shall submit one (1) set of an application file for issuance of a certificate online or

directly or via postal services to the specialized agency for personal data protection.

The specialized agency for personal data protection shall assess whether the file satisfies requirements or not within 10 days. If the file is incomplete and does not comply with regulations, the specialized agency for personal data protection shall provide a written notice to the applicant requesting the applicant to supplement and complete the file within 15 days and specify the reasons therefor.

4. Within 30 days from the date of receipt of a complete and valid file, the specialized agency for personal data protection shall evaluate, consider and decide to issue a certificate in accordance with Form No. 05 in the Appendix of this Decree. Such a certificate may be in the paper or electronic form; the certificate in the paper form shall be issued if the file is submitted directly or via postal services or as requested when the file is submitted online via the public service portal. In the case of refusal to issue a certificate, the specialized agency for personal data protection shall notify the applicant thereof, and specify the reasons therefor.

Article 26 *Application files, sequence and procedures for re-issuance and replacement of certificates of satisfaction of conditions for business of personal data processing services [certificates]*

1. A certificate in the paper form which is lost or damaged shall be re-issued.

(a) If the applicant wishes to apply for re-issuance of the certificate in the paper form, the applicant shall send an application in accordance with Form No. 05 in the Appendix of this Decree online or directly or via postal services to the specialized agency for personal data protection.

(b) Within 5 working days from the date of receipt of the application in accordance with regulations, the specialized agency for personal data protection shall consider and re-issue the certificate; in the case of refusal, it must provide a written notice, specifying the reasons therefor.

2. A certificate shall be replaced when any information is incorrect or any content is changed.

(a) An application file shall comprise the following: application in accordance with Form No. 06 in the Appendix of this Decree; and data and documents proving the incorrect information or the change to the content stated in the issued certificate.

(b) The applicant shall submit one (1) set of an application file stated above online or directly or via postal services to the specialized agency for personal data protection. Within 5 working days from the date of receipt of a complete file stipulated in sub-clause (a) above, the specialized agency for personal data protection shall consider and decide to issue a replacement certificate; in the case of refusal, it must provide a written notice, specifying the reasons therefor.

Article 27 *Revocation of certificates of satisfaction of conditions for business of personal data processing services [certificates]*

1. A certificate shall be revoked in the following cases:

(a) Failing to satisfy one of the conditions prescribed in clauses 1 and 2 of article 26 of this Decree;

(b) Failing to conduct business of services for 12 months or more;

(c) Being dissolved or bankrupt in accordance with law;

(d) Failing to remedy a breach in respect of personal data protection, information safety,

cybersecurity or data security at the request of a competent State agency;

(dd) Proactively applying for suspension or termination of operation.

2. The specialized agency for personal data protection shall make a decision on revocation of the certificate in accordance with Form No. 07 in the Appendix of this Decree.

3. The personal data processing service business organization is responsible to surrender the issued certificate to the specialized agency for personal data protection within 5 working days from the date of receipt of the decision on revocation.

4. Upon issuance of the decision on revocation of the certificate, the specialized agency for personal data protection shall announce such decision on the national information portal on protection of personal data.

Article 28 *Contents of notice of breach of regulations on protection of personal data*

1. A notice of breach of the regulations on protection of personal data shall contain the following contents:

(a) Description of the nature of the breach, comprising the following: time, place, act, organization, individual, types of personal data and volume of relevant data;

(b) Contact details of the personal data protection division or personnel or of the organization or individual providing personal data protection services;

(c) Description of possible consequences and damage caused by the breach;

(d) Description of the measures given to resolve or mitigate harmful effects of the breach.

2. The personal data processor, the personal data controlling and processing party or a third party processor shall send the notice of the breach to the specialized agency for personal data protection or via the national information portal on protection of personal data in accordance with Form No. 08 in the Appendix of this Decree.

Article 29 *Notification of breach in respect of personal position data and biometric data*

1. Upon occurrence of a personal data breach in relation to position data or biometric data, the personal data processor or the personal data controlling and processing party shall be responsible:

(a) To provide a notice thereof to affected data subjects within no more than 72 hours from the time of discovery of the breach;

(b) To make a report to the competent State agency in accordance with article 28 of this Decree;

(c) To record, store and update the file on the breach for the purpose of serving the inspection, examination and resolution. The organization must store the file on the breach for a period of at least 5 years from the completion date of remedy of the breach.

2. The notice prescribed in clause 1(a) of this article must at least contain the following contents:

(a) Time and form of discovery of the breach;

(b) Type of affected data (position data, biometric data or both);

(c) Seriousness and possible risks to the lawful rights and interests of the data subjects;

(d) Measures which were, are being or will be taken to remedy the breach and mitigate damage;

(dd) Guidance for the data subjects to implement further measures for prevention and avoidance;

(e) Contact details of the personal data protection division or personnel or of the organization or individual providing personal data protection services; and the division which receives and resolves personal data incidents at the organization.

3. Where an organization or individual is unable to notify all affected personal data subjects within the period stipulated in clause 1 of this article for a technical or emergency reason, such organization or individual must:

(a) Provide a public announcement by the official electronic means of the organization via its website or application;

(b) Send a notice to the related personal data subjects as soon as the technical conditions permit.

4. Where an organization or individual fails to provide a notice within the stipulated period or intentionally delays or avoids the obligation of notification, such organization or individual shall be considered and shall be subject to a penalty for breach in accordance with law.

Chapter IV

IMPLEMENTATION OF PERSONAL DATA PROTECTION WORK

Article 30 *Responsibility to implement international cooperation on protection of personal data*

1. The specialized agency for personal data protection is responsible to assist the Ministry of Public Security in implementing international cooperation on protection of personal data.

2. Ministries, ministerial equivalent agencies and Government agencies shall implement international cooperation on protection of personal data in the industries and sectors within the scope of their management in accordance with law and in accordance with their assigned functions and duties.

3. Provincial people's committees shall implement international cooperation on protection of personal data in accordance with law and their assigned functions and duties.

Article 31 *Inspection of personal data protection activities*

1. The personal data protection activities shall be inspected regularly or on an ad hoc basis in the following cases:

(a) There are grounds for suspecting a breach of the law on protection of personal data;

(b) As instructed by an agency or person having the authority to exercise the State administration of personal data protection;

(c) In order to exercise the State administration in accordance with law.

2. Entities subject to inspection of personal data protection activities shall comprise:

(a) Agencies, organizations and individuals engaged in the personal data processing activities;

(b) Organizations and individuals conducting business of personal data processing services;

(c) Agencies, organizations and individuals required to conduct personal data processing impact assessment and cross-border personal data transfer impact assessment;

(d) Agencies, organizations and individuals involved in cases and matters in breach of the regulations on protection of personal data.

3. Contents of inspection of personal data protection work:

(a) Current status of implementation of the personal data protection work;

(b) Activities of personal data processing impact assessment and cross-border personal data transfer impact assessment;

(c) Activities of personal data processing service business.

4. The specialized agency for personal data protection shall issue a decision on inspection and provide a 15-day notice to any entity subject to the inspection as stipulated in clause 2 of this article of the time, contents and composition of the inspection team. In the case of an unscheduled inspection for the purpose of promptly verifying, discovering or preventing the breach of the law on protection of personal data, the specialized agency for personal data protection shall have the right to immediately conduct the inspection without prior notice.

5. The entity subject to inspection must prepare all the contents of inspection in compliance with clause 3 of this article and as specifically requested in the decision on inspection issued by the specialized agency for personal data protection.

Article 32 *Research and development of solutions for personal data protection*

Agencies, organizations, enterprises and individuals shall participate in research, development and application of solutions for protection of personal data, including:

1. Development of systems of software and equipment for protection of personal data.

2. Methods of appraisal of software and equipment for protection of personal data which satisfy standards.

3. Methods of checking whether hardware and software provided perform their functions correctly.

4. Recognition and management of the compliance with the regulations on protection of personal data.

5. Resolution of risks of revelation and loss of personal data.

6. Technical initiatives to increase awareness and skills of protection of personal data.

7. Processing of personal data for servicing statistics and scientific work.

8. Solutions provided to personal data subjects to control their personal data, provide and share data in accordance with selective disclosure mechanisms, and apply high technologies and strategic technologies in conformity with international standards and regulations.

9. Standards for protection of personal data.

10. Other solutions for protection of personal data in accordance with law.

Article 33 *Contents of State administration of protection of personal data*

1. Issuing in accordance with authority or submitting to competent State agencies for issuance of legal instruments on protection of personal data; organizing implementation of the law on protection of personal data.

2. Formulating and organizing implementation of strategies, policies, proposals, projects, programs and plans on protection of personal data.

3. Providing guidelines to agencies, organizations and individuals on measures, procedures, standards and regulations on protection of personal data in accordance with law.

4. Disseminating and educating the law on protection of personal data; communicating and popularizing knowledge and skills of protection of personal data.

5. Building, training, retraining and developing human resources in respect of protection of personal data.

6. Conducting check and inspection, granting commendations and rewards, resolving complaints and denunciations, and dealing with breaches of the law on protection of personal data in accordance with law.

7. Providing statistics, information and reports on the situation of protection of personal data and the implementation of the law on protection of personal data to competent State agencies.

8. Organizing preliminary review, final review and scientific research on protection of personal data; researching and applying scientific and technological advances in respect of protection of personal data.

9. Implementing international cooperation on protection of personal data.

Article 34 *Responsibilities of the Ministry of Public Security*

1. To assist the Government to uniformly exercise the State administration of protection of personal data.

2. To preside over formulating and issuing or submitting to competent State agencies for issuance and provision of guidelines for implementation of legal instruments guiding implementation of the law on protection of personal data.

3. To provide guidelines for and implement activities of protection of personal data and protection of rights of data subjects from breaches of the law on protection of personal data.

4. To preside over coordinating with the Ministry of Science and Technology to formulate standards and technical regulations on protection of personal data; and technical regulations on de-identification of personal data and anonymization of personal data to be promulgated and applied in Vietnam.

5. To build, manage and operate the national information portal on protection of personal data.

6. To implement dissemination, popularization and education of law and to provide guidelines and training on knowledge and skills of protection of personal data for personal data protection forces.

7. To conduct evaluation, preliminary review and final review of results of personal data protection by related agencies, organizations and individuals.

8. To promote scientific research on protection of personal data; to research and apply scientific and

technological advances in respect of protection of personal data for the purpose of innovation in the personal data protection sector.

9. To implement international cooperation activities in respect of protection of personal data.

Article 35 *Responsibilities of the Ministry of National Defence*

1. To coordinate with the Ministry of Public Security and related agencies and organizations to arrange forces and means to protect personal data, and discover and prevent breaches of the regulations on protection of personal data within the scope of its management.

2. Within the scope of assigned functions and duties, to preside over coordinating with the Ministry of Public Security to conduct evaluation of results of personal data protection by agencies, organizations and individuals within the scope of its management; to promote the application of measures for protection of personal data; to research and apply advanced security technologies to the processing and protection of personal data for serving the national defence activities; and to implement international cooperation on protection of personal data within the scope of its management in accordance with law.

3. To organize dissemination, popularization and education of the law on and knowledge and skills of protection of personal data for officers, regular military personnel, and State officials, employees and staff within the scope of its management.

4. To check, inspect, supervise and deal with breaches of the regulations on protection of personal data with respect to agencies, organizations and individuals within the scope of management of the Ministry of National Defence in accordance with law and its assigned functions and duties.

Article 36 *Responsibilities of the Ministry of Science and Technology*

1. To coordinate with the Ministry of Public Security to formulate standards and technical regulations on protection of personal data; and technical regulations on de-identification of personal data and anonymization of personal data to be promulgated and applied in Vietnam.

2. To coordinate with the Ministry of Public Security and related agencies to research, develop, master and apply measures for protection of personal data using advanced technologies, high technologies and strategic technologies, and to form personal data protection solutions, products and services during the development of digital government, digital economy and digital society through scientific and technological programs.

Article 37 *Responsibilities of ministries, ministerial equivalent agencies and Government agencies*

1. To exercise the State administration of personal data protection with respect to industries and sectors within the scope of their management in accordance with law.

2. To formulate and implement contents and duties of personal data protection in this Decree.

3. To supplement regulations on protection of personal data during the formulation and implementation of duties of ministries and branches.

4. To arrange personal data protection personnel and divisions in units under their management; to ensure satisfaction of capability [requirements], and conformity with working positions and professional requirements on protection of personal data in accordance with law.

5. To arrange funds for personal data protection activities in accordance with the current delegation of authority to manage budgets.

6. To organize dissemination and popularization of the law and training on professional matters and skills of protection of personal data for State officials, employees and staff and units within the scope of their management.

7. To coordinate with the Ministry of Public Security to check, inspect, supervise and deal with breaches of the regulations on protection of personal data within the scope of their management.

8. To coordinate with the Ministry of Public Security and the Ministry of Science and Technology to formulate guidelines on and implement application of standards and technical regulations on protection of personal data with respect to units, organizations and individuals within the scope of their management.

Article 38 *Responsibilities of people's committees of provinces and cities under central authority*

1. To exercise the State administration of personal data protection with respect to industries and sectors under their management in accordance with the law on protection of personal data.

2. To implement the provisions on protection of personal data in this Decree.

3. To arrange personal data protection personnel and divisions in units under their management; to ensure satisfaction of capability [requirements], and conformity with working positions and professional requirements on protection of personal data in accordance with law.

4. To arrange funds for personal data protection activities in accordance with the current delegation of authority to manage budgets.

5. To organize dissemination and popularization of the law on and [improve] knowledge and skills of personal data protection for State officials, employees and staff, citizens and enterprises in their localities.

6. To organize training to increase capability of personnel engaged in the personal data protection work at administrative levels; to include contents of personal data protection in programs on administrative reform and digital transformation.

7. To establish systems of statistics and compilation [of data], and provide periodical reports on the situation of personal data protection in their localities to the specialized agency for personal data protection in accordance with regulations.

Article 39 *Specialized agency for personal data protection and national information portal on personal data protection*

1. The specialized agency for personal data protection is a unit under the Ministry of Public Security and is responsible to assist the Minister of Public Security in exercising the function of State administration of personal data protection.

2. The national information portal on personal data protection shall provide information to disseminate guidelines, orientations and policies of the Communist Party and the law of the State on personal data protection; support for providing guidelines and increasing awareness and skills of personal data protection for agencies, organizations and individuals; and receive and resolve reports and petitions from related agencies, organizations and individuals; and perform other activities in accordance with the law on protection of personal data.

Article 40 *Funds for ensuring personal data protection activities*

1. Funds for personal data protection shall comprise the State budget; contributions from domestic and foreign agencies, organizations and individuals; revenue from the provision of personal data

protection services; international aids and other lawful sources of revenue.

2. Funds for personal data protection of State agencies shall be guaranteed by the State budget, and included in the annual State budget estimate. The management and use of funds from the State budget shall be implemented in accordance with the law on State budget.

3. Funds for personal data protection of organizations and enterprises shall be arranged and implemented by such organizations and enterprises in accordance with regulations.

Chapter V

ORGANIZATION OF IMPLEMENTATION

Article 41 *Provisions on application of clauses 2 and 3 of article 38 of the Law on Protection of Personal Data*

1. Small enterprises and start-up enterprises may choose whether to implement the provisions in articles 21, 22 and 33.2 of the *Law on Protection of Personal Data* for a period of 5 years from the effective date of the *Law on Protection of Personal Data*, except for small enterprises and start-up enterprises engaged in business of personal data processing services, directly processing sensitive personal data or processing personal data from the time they reach a scale of 100,000 or more personal data subjects or more based on the accumulated total volume of processed personal data.

2. Business households and micro enterprises are not required to implement the provisions in articles 21, 22 and 33.2 of the *Law on Protection of Personal Data*, except for business households and micro enterprises engaged in business of personal data processing services, directly processing sensitive personal data or processing personal data from the time they reach a scale of 100,000 or more personal data subjects or more based on the accumulated total volume of processed personal data.

Article 42 *Effectiveness and responsibility for implementation*

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

2. Decree No. 13/2023/ND-CP dated 17 April 2023 of the Government on protection of personal data shall no longer be effective from the effective date of this Decree.

3. Clause 2 of article 16 of Decree No. 165/2025/ND-CP dated 30 June 2025 of the Government providing detailed regulations on a number of articles and measures for implementation of the *Law on Data* is amended as follows:

"2. Core data and important data being personal data shall be protected in accordance with the *Law on Protection of Personal Data* and documents providing detailed regulations for implementation.

In the case of cross-border transfer or processing of core data or important data being personal data, the administrator of core data or important data shall prepare a file on personal data processing impact assessment or cross-border personal data transfer impact assessment in accordance with the law on personal data protection; and is not required to conduct assessment of risks or assessment of impact of cross-border data transfer or processing in accordance with this Decree."

4. The Ministry of Public Security is responsible to guide, inspect and monitor the implementation of this Decree.

5. Ministers, heads of ministerial equivalent agencies and Government agencies, chairmen of people's committees of provinces and cities under central authority, and related agencies, organizations and individuals are responsible to implement this Decree.

ON BEHALF OF THE GOVERNMENT
FOR THE PRIME MINISTER
DEPUTY PRIME MINISTER

Nguyen Hoa Binh