THE GOVERNMENT OF VIETNAM	THE SOCIALIST REPUBLIC OF VIETNAM
-------	Independence - Freedom - Happiness

No. 356/2025/ND-CP	*Hanoi, December 31, 2025*

DECREE

ELABORATING ON CERTAIN ARTICLES AND IMPLEMENTATION MEASURES OF LAW ON PERSONAL DATA PROTECTION

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

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

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

Pursuant to the Law on amendments to the Law on Bidding, Law on Public-Private Partnership Investment, Law on Customs, Law on Value-Added Tax, Law on Export and Import Duties, Law on Investment, Law on Public Investment, and Law on Management and Use of Public Property No. 90/2025/QH15;

At the request of the Minister of Public Security of Vietnam;

The Government of Vietnam hereby promulgates the Decree elaborating on certain articles and implementation measures of the Law on Personal Data Protection.

Chapter I

GENERAL PROVISIONS

Article 1. Scope

This Decree elaborates on Clauses 2 and 3 Article 2; Clause 5 Article 4; Clause 3 Article 6; Clause 5 Article 9; Clause 3 Article 17; Clause 7 Article 20; Clause 7 Article 21; Clause 4 Article 22; Clause 5 Article 23; Clause 3 Article 27; Clause 6 Article 30; Point b Clause 4 Article 31; Clause 3 Article 33; Article 35; Clause 4 Article 38 of the Law on Personal Data Protection, and provides for measures to implement the Law regarding the research and development of personal data protection solutions, personal data protection authorities, the National Information Portal for Personal Data Protection; responsibilities of ministries, central authorities, and local authorities for personal data protection; funding for ensuring personal data protection activities.

Article 2. Regulated entities

1. Vietnamese agencies, organizations, and individuals;

2. Foreign agencies, organizations, and individuals in Vietnam;

3. Foreign agencies, organizations, and individuals directly participating in or involved in the processing of personal data of Vietnamese citizens and persons of Vietnamese origin without determined nationality residing in Vietnam who have been issued with identification certificates.

Article 3. List of basic personal data

Basic personal data includes:

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

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

3. Gender;

4. Place of birth; place of birth registration; place of permanent residence registration; place of temporary residence registration; current place of residence; hometown; contact address;

5. Nationality;

6. Images of the individual;

7. Phone number; personal identification number; passport number; driver's license number; vehicle registration plate number;

8. Marital status;

9. Information on family relationships (parents, children, spouse);

10. Information on the individual's digital accounts;

11. Other information associated with a specific individual or capable of identifying a specific individual, other than the information prescribed in Article 4 of this Decree.

Article 4. List of sensitive personal data

1. Sensitive personal data includes:

a) Data revealing racial origin or ethnic origin;

b) Opinions on politics, religion, and belief;

c) Information on private life, personal secrets, and family secrets;

d) Health status;

dd) Biometric data and genetic characteristics;

e) Data revealing an individual's sexual life or sexual orientation;

g) Data on crimes and violations of law collected and stored by law enforcement agencies;

h) Location data of individuals determined through positioning services;

i) Login names and passwords for access to individuals' electronic identification accounts; images of ID cards, citizen ID cards, or 9-digit ID cards;

k) Login names and passwords for access to bank accounts; bank card information; data on transaction history of bank accounts; financial and credit information and other information relating to financial activities and transaction history, securities, and insurance of clients at credit institutions, foreign bank branches, intermediary payment service providers, securities institutions, insurers, and other authorized organizations;

l) Data monitoring behavior and activities related to the use of telecommunications services, social networks, online communication services, and other services in cyberspace;

m) Other personal data that are required by law to be kept confidential or to which strict confidentiality measures must be applied.

2. In the course of processing sensitive personal data, agencies and organizations shall establish regulations on access authorization and restriction, processing procedures, and confidentiality measures.

Chapter II

REQUIREMENTS AND CONDITIONS FOR PERSONAL DATA PROTECTION

Article 5. Exercise of rights of personal data subject matters

1. The personal data controlling party and the personal data processing and controlling party shall develop clear procedures and forms for the exercise of the rights of the personal data subject matter, in accordance with personal data processing activities and the responsibilities of relevant units, and ensure that the personal data subject matter is informed of the procedures for exercising the rights prescribed in Clause 1 Article 4 of the Law on Personal Data Protection.

2. Upon receipt of a request from the personal data subject matter for withdrawal of consent to personal data processing, restriction of personal data processing, or objection to personal data processing in accordance with the prescribed procedures, the personal data controlling party and the personal data processing and controlling party shall respond within 2 working days, fully provide the personal data subject matter with information on the procedures for cessation of personal data processing, and implement such cessation within 15 days, except for cases where personal data processing does not require the consent of the personal data subject matter as

prescribed in Article 19 of the Law on Personal Data Protection. Where it is necessary to request the personal data processing party or a third party to cease processing the personal data of the personal data subject matter, such cessation shall be carried out within 20 days.

Depending on the nature and complexity of the request, where an extension of the processing time is required, only 1 extension may be granted for a period not exceeding 15 days. The personal data controlling party and the personal data processing and controlling party shall notify the personal data subject matter of the reasons for the extension and assume the responsibility for demonstrating that such extension is necessary and reasonable.

3. Upon receipt of a request from the personal data subject matter to view, modify, or request modification of personal data, or to obtain provision of personal data in accordance with the prescribed procedures, the personal data controlling party and the personal data processing and controlling party shall respond within 2 working days, fully provide information on the relevant procedures, and implement such request within 10 days. Where it is necessary to request the personal data processing party or a third party to modify the personal data of the personal data subject matter, such modification shall be carried out within 15 days.

Depending on the nature and complexity of the request, where an extension of the processing time is required, only 1 extension may be granted for a period not exceeding 10 days. The personal data controlling party and the personal data processing and controlling party shall notify the personal data subject matter of the reasons for the extension and assume the responsibility for demonstrating that such extension is necessary and reasonable.

4. Upon receipt of a request from the personal data subject matter for deletion of personal data in accordance with the prescribed procedures, the personal data controlling party and the personal data processing and controlling party shall respond within 2 working days, fully provide information on the relevant procedures, and implement such deletion within 20 days. Where it is necessary to request the personal data processing party or a third party to provide, delete, or restrict the processing of the personal data of the personal data subject matter, such actions shall be carried out within 30 days.

Depending on the nature and complexity of the request, where an extension of the processing time is required, only 1 extension may be granted for a period not exceeding 20 days. The personal data controlling party and the personal data processing and controlling party shall notify the personal data subject matter of the reasons for the extension and assume the responsibility for demonstrating that such extension is necessary and reasonable.

5. Upon receipt of a request from the personal data subject matter for the implementation of solutions and measures to protect their personal data in accordance with the prescribed procedures, the competent authority or the agency, organization, and individual related to personal data processing shall respond within 2 working days, fully provide information on the relevant procedures, and implement such solutions and measures within 15 days.

Depending on the nature and complexity of the request, where an extension of the processing time is required, only 1 extension may be granted for a period not exceeding 15 days. The

personal data controlling party and the personal data processing and controlling party shall notify the personal data subject matter of the reasons for the extension and assume the responsibility for demonstrating that such extension is necessary and reasonable.

Article 6. Methods for expressing personal data subject matters' consent

1. Methods for obtaining the consent of the personal data subject matter shall ensure verifiability in identifying that the personal data subject matter has given consent, as well as the time and content of such consent, including:

a) In writing;

b) By recorded phone calls;

c) Consent syntax via mobile text messages;

d) Via email, websites, platforms, or applications with technical mechanisms established to obtain consent;

dd) Other appropriate methods that can be printed or reproduced in writing, including electronic forms or other verifiable formats.

2. The personal data controlling party and the personal data processing and controlling party shall store the consent of the personal data subject matter. In the event of a dispute, the burden of proof for the consent of the personal data subject matter shall rest with the personal data controlling party and the personal data processing and controlling party.

3. The personal data controlling party and the personal data processing and controlling party shall not establish default consent mechanisms or create unclear or misleading instructions that cause confusion between consent and non-consent for the personal data subject matter. Default settings shall ensure compliance with personal data protection principles and respect the rights of the personal data subject matter.

4. For obtaining consent to process sensitive personal data, the personal data subject matter shall be informed that the data to be processed constitutes sensitive personal data.

Article 7. Personal data transfer

1. Organizations and individuals transferring personal data under Points a, c, and d Clause 1 Article 17 of the Law on Personal Data Protection shall establish an agreement on the transfer of personal data with the personal data recipient, specifying the following contents:

a) Purposes of the transfer of personal data;

b) Categories of the personal data subject matter and the type of personal data transferred, consistent with the purposes of transfer;

c) Personal data processing time limits; requirements for deletion and destruction of personal data after completion of the purposes of transfer;

d) Legal grounds for the transfer of personal data;

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

e) Responsibilities for ensuring the exercise of the rights of the personal data subject matter;

g) Responsibilities for cooperation and compliance of the concerned parties in cases where violations of personal data protection regulations are detected.

2. The transfer of sensitive personal data shall be subject to physical confidentiality measures for storage and transmission devices, encryption measures, anonymization of personal data, and other confidentiality measures during the transfer process.

3. In cases where personal data is transferred under Points a and d Clause 1 Article 17 of the Law on Personal Data Protection, and fees are charged for providing services for the personal data subject matter or for serving the legitimate interests of the personal data subject matter, organizations and individuals shall comply with the following requirements:

a) Establish technical systems and transparent mechanisms enabling the personal data subject matter to give precise and explicit consent for each transfer, based on being fully informed of the purposes of transfer and the organizations or individuals receiving and processing personal data;

b) Process personal data solely for the purposes of transfer consented to by the personal data subject matter, in conformity with registered business lines;

c) Limit the type of personal data transferred to the scope necessary for the purposes of transfer;

d) Refrain from collecting, storing, or establishing repositories of personal data from personal data transfer activities for purposes other than those consented to by the personal data subject matter;

dd) Clearly determine the roles of the personal data controlling party, the personal data processing party, and third parties in personal data transfer activities;

e) Enter into agreements on the transfer and processing of personal data before the transfer, and commit to responsibilities and obligations toward the personal data subject matter.

4. In cases of sharing personal data among departments within the same agency or organization for personal data processing consistent with established processing purposes, such agency or organization shall develop procedures for controlling the sharing and use of personal data in compliance with regulations, and implement measures to prevent internal personnel from illegally sharing personal data with third parties.

5. Personal data shall be de-identified before being transacted on data exchanges.

6. Agencies, organizations, and individuals providing personal data under Clause 2 Article 15 of the Law on Personal Data Protection, based on specific requests of the personal data subject matter, shall not be regarded as engaging in personal data transfer and shall not be subject to this Article.

Article 8. Personal data protection in finance, banking, and credit information activities

1. Organizations and individuals operating in the fields of finance, banking, and credit information activities shall be responsible for applying standards and technical regulations on personal data protection; technical regulations on de-identification and anonymization of personal data promulgated and applied in Vietnam; conducting periodic assessments of compliance with personal data protection regulations once per year; and recording system logs of all personal data processing activities.

2. Organizations and individuals operating in the fields of finance, banking, and credit information activities that act as the personal data controlling party or the personal data processing and controlling party, when obtaining consent from the personal data subject matter, shall ensure that the following contents are specified:

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

b) Sources of collection of personal data and relevant parties involved in the collection and sharing of personal data;

c) Duration of storage of personal data;

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

3. Within a period not exceeding 72 hours from the time of detecting leakage or loss of sensitive personal data of the personal data subject matter in the fields of finance, banking, and credit information activities, the organization or individual that directly collects personal data of the personal data subject matter shall be responsible for notifying the personal data protection authority and the personal data subject matter. The contents of such notification shall at least include the contents prescribed in Clause 1 Article 28 of this Decree.

Article 9. Personal data protection in big data processing

1. Big data processing containing personal data refers to personal data processing activities conducted on a large scale, based on a continuous basis, integrated from multiple different sources, and capable of analyzing behavior, predicting trends, or classifying users.

2. In cases of big data processing containing personal data, relevant agencies, organizations, and individuals shall have the following responsibilities:

a) Comply with personal data protection regulations throughout the data processing process, starting from the commencement of processing;

b) Collect, process, and store personal data strictly within an appropriate scope and in accordance with specific and clearly defined purposes;

c) Develop policies on storage, deletion, and destruction of personal data that are appropriate and compliant with the law;

d) Organize periodic training, dissemination, and awareness-raising activities on personal data confidentiality and personal data protection measures for employees, particularly personnel directly involved in personal data processing; and enhance awareness of the importance of personal data protection within the organization;

dd) Enter into agreements with third parties, partners, and service providers to ensure full compliance with personal data protection regulations;

e) Establish appropriate notification and explanation mechanisms for the personal data subject matter regarding the use of their personal data in big data analytics systems.

3. Agencies, organizations, and individuals shall apply personal data protection measures during big data processing, including:

a) Applying measures to ensure cybersecurity, data confidentiality, and the prevention of personal data leakage during the storage, processing, and transmission of personal data;

b) Using strong authentication methods, requiring at least multi-factor authentication (passwords, PIN codes combined with one-time passwords, digital signature devices, or biometric factors), appropriate to the level of sensitivity of personal data; and implementing access authorization to ensure that only authorized persons may access personal data;

c) Implementing encryption and anonymization of personal data (being the process of separating data identifying a specific individual for separate storage and protection, whereby personal data after such process is used for processing without the ability to identify a specific individual) during the transfer and provision of personal data, except where specialized laws provide otherwise or where processing requires data in plaintext form for crime prevention and combat, anti-money laundering, assurance of national security, or settlement of clients' complaints and disputes. In such cases, agencies and organizations shall apply additional confidentiality measures to ensure that personal data is not accessed or used illegally;

d) Conducting continuous supervision and using supervision tools to monitor personal data access activities and detect abnormal behavior;

dd) Conducting periodic inspections and assessments of cybersecurity and data confidentiality to detect, prevent, and remedy security vulnerabilities.

Article 10. Personal data protection in artificial intelligence systems and metaverse

1. Organizations and individuals may use personal data for the research and development of self-learning algorithms, artificial intelligence systems, and other automated systems, provided that compliance with personal data protection regulations is ensured.

2. Data derived from artificial intelligence inference results, where such data can be used to identify or assist in identifying a specific individual, shall be subject to personal data protection measures in accordance with the law.

3. The personal data controlling party and the personal data processing and controlling party shall be responsible for notifying the personal data subject matter of automated personal data processing, explaining the operating principles of the algorithms and their impacts on the legitimate rights and interests of the personal data subject matter, and providing options enabling the personal data subject matter to exercise the right to opt out.

4. The metaverse is a digital universe combining aspects of social media, online gaming, augmented reality (AR), virtual reality (VR), the Internet, and cryptocurrencies, enabling users to interact through virtual reality technologies.

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

a) Researching, developing, and implementing systems that meet cybersecurity standards and comprehensive data protection standards for artificial intelligence systems, with particular emphasis on information confidentiality, algorithm reliability, system stability, and cyberattack prevention capacity;

b) Establishing mechanisms for supervising the operation of artificial intelligence systems in two aspects: supervision by competent state authorities, and accountability toward the personal data subject matter of the personal data controlling party and the personal data processing and controlling party.

c) Developing personal data protection mechanisms in accordance with appropriate standards and developing supervision systems and early-warning mechanisms for cybersecurity threats;

d) Establishing mechanisms to control and prevent the abuse of artificial intelligence systems and the metaverse for activities infringing on national security or social order and safety;

dd) Conducting periodic assessments of compliance with personal data protection regulations once per year.

6. The personal data subject matter shall have the right to modify, anonymize, and delete identification profiles, including in cases where platforms store behavioral history.

Article 11. Personal data protection in blockchain

1. Relevant agencies, organizations, and individuals shall comply with personal data protection regulations when processing personal data within blockchain, during the research and development of products, services, applications, and systems that use blockchain, and during the processing of personal data.

2. Agencies, organizations, and individuals shall apply personal data protection measures when processing personal data in blockchain, including:

a) Applying only encryption algorithms, hashing algorithms, and digital signature algorithms that ensure safety;

b) Refraining from directly storing personal data on the blockchain, and only storing such data where personal data has been de-identified or where hash values of personal data are stored;

c) Conducting periodic assessments of compliance with personal data protection regulations once per year.

Article 12. Personal data protection in cloud computing

1. Relevant agencies, organizations, and individuals shall apply technical and organizational measures to prevent unauthorized access to personal data when implementing cloud computing services.

2. Organizations and individuals entering into contracts related to personal data processing with cloud computing service providers shall have the following responsibilities:

a) Specify in the contract compliance with the laws of Vietnam on personal data protection, provide information on the personal data protection unit and personnel, and comply with administrative procedures related to personal data protection in accordance with the law;

b) Identify personal data processing flows, the roles of the concerned parties in cloud computing service provision, and corresponding responsibilities;

c) Require confidentiality measures and technical and organizational measures, which shall be clearly stipulated in the contract;

d) Immediately notify the concerned parties of any changes that may affect personal data;

dd) Comply with personal data processing time limits and requirements for deletion and destruction of personal data;

e) Ensure the exercise of the rights of the personal data subject matter;

g) Fully implement technical measures to ensure that access to personal data is reasonably delegated.

3. Cloud computing service providers shall:

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

b) Require subcontractors to comply with personal data protection regulations and obligations in accordance with the law;

c) Apply technical and organizational measures at a level appropriate to the scale and extent of their personal data processing;

d) Conducting periodic assessments of compliance with personal data protection regulations once per year.

4. Personal data in cloud computing shall be encrypted both at rest and in transit, together with strict access authorization.

Article 13. Conditions applicable to personal data protection personnel and personal data protection units in agencies and organizations

1. The designation of personal data protection personnel or a personal data protection unit shall be made through an official written document of the relevant agency or organization, specifying the assignment, functions, tasks, entitlements, and other requirements relating to personal data protection within that agency or organization.

2. Personal data protection personnel designated by an agency or organization shall satisfy the following competency conditions:

a) Holding at least a college-level degree or higher;

b) Having at least 2 years of working experience (from the time of graduation) related to one of the following fields: legal affairs, information technology, cybersecurity, data security, risk management, compliance control, and personnel management/organization;

c) Having received training and advanced training in legal knowledge and professional skills relating to personal data protection.

3. Where an agency or organization establishes a personal data protection unit, personnel within such unit shall satisfy the competency conditions specified in Clause 2 of this Article.

4. Agencies and organizations shall be responsible for assessing and selecting personnel for personal data protection.

5. Agencies and organizations shall enter into agreements on responsibility for confidentiality with personal data protection personnel, and may agree on cases of liability exemption where violations or damage occur to protected personal data.

6. Agencies and organizations that designate personal data protection personnel or establish a personal data protection unit shall be responsible for providing training and advanced training in personal data protection knowledge and skills for such personnel.

Article 14. Tasks of personal data protection units and personal data protection personnel within agencies and organizations

1. A personal data protection unit shall:

a) Organize the development of policies, procedures, regulations, and forms to ensure compliance with personal data protection laws;

b) Organize the exercise of the rights of the personal data subject matter;

c) Periodically organize assessments of the organization's compliance with personal data protection laws through compliance assessment reports on the performance of statutory obligations, to propose measures to enhance compliance effectiveness and to prevent and control risks in personal data processing activities;

d) Prepare dossiers for impact assessments of cross-border transfer of personal data and impact assessments of personal data processing; receive and report violations of personal data protection; and fulfill other requirements of competent authorities in accordance with regulations;

dd) Develop plans and implement periodic training and advanced training in personal data protection within the agency or organization;

e) Organize the implementation of technical confidentiality measures for personal data, standards and regulations on personal data protection, and emergency response plans for personal data protection incidents;

g) Conduct research and propose decisions related to personal data protection.

2. Personal data protection personnel shall:

a) Advise on the development of policies, procedures, regulations, and forms to ensure compliance with personal data protection laws;

b) Participate in the exercise of the rights of the personal data subject matter;

c) Participate in periodic activities assessing compliance with personal data protection laws and propose measures to enhance compliance effectiveness and to prevent and control risks;

d) Prepare dossiers for impact assessments of cross-border transfer of personal data and impact assessments of personal data processing; receive and report violations of personal data protection; and fulfill other requirements of competent authorities in accordance with regulations;

dd) Participate in programs and training courses on personal data protection;

e) Participate in the implementation of technical confidentiality measures for personal data, standards and regulations on personal data protection, and emergency response plans for personal data protection incidents.

Article 15. Individuals providing personal data protection services

1. An individual providing personal data protection services is a person who satisfies the competency conditions specified in Clause 2 of this Article and is hired by an agency or organization to serve as personal data protection personnel.

2. An individual providing personal data protection services shall satisfy the following competency conditions:

a) Holding at least a college-level degree or higher;

b) Having at least 3 years of working experience (from the time of graduation) related to one of the following fields: legal affairs, personal data processing, cybersecurity, data security, risk management, and compliance control;

c) Having received training and in-depth training in legal knowledge and professional skills relating to personal data protection.

3. Agencies or organizations wishing to hire an individual providing personal data protection services shall review the competency conditions specified in Clause 2 of this Article, enter into a contract for the use of personal data protection personnel, and disclose information about such personal data protection personnel to the personal data subject matter and relevant parties.

4. An individual providing personal data protection services shall:

a) Provide services strictly within the scope and tasks stipulated in the contract or agreement;

b) Refrain from abusing the provision of services to commit violations of the law;

c) Perform the deletion and destruction of personal data processed during service provision after completion of the contract and in accordance with the law.

Article 16. Organizations providing personal data protection services

1. An organization providing personal data protection services:

a) Is an organization or enterprise whose functions, tasks, or business lines fall within technology, legal services, or technology and legal consulting, and which is hired by an agency or organization to advise on compliance with personal data protection regulations and to perform personal data protection tasks in accordance with agreements;

b) Has at least 3 personnel satisfying the competency conditions specified in Clause 2 Article 15 of this Decree;

c) Has provided products and services related to confidentiality, cybersecurity, information technology, standards assessment, or consulting on personal data protection.

2. An organization providing personal data protection services shall prepare a competency dossier demonstrating its capacity to protect personal data and provide it for agencies or organizations wishing to use its services. The dossier shall specify business lines and fields, scale, scope, and experience in service provision, service provision policies, standards, qualifications, personnel capacity, and other relevant supporting documents.

3. Agencies or organizations wishing to hire personal data protection services shall review the competency dossier, enter into service contracts and personal data processing agreements with the personal data protection organization, and disclose information about such organization to the personal data subject matter and relevant parties.

4. Depending on actual needs, an agency or organization may concurrently designate personal data protection personnel, establish a personal data protection unit, and hire individuals or organizations providing personal data protection services.

5. Based on agreements with the agency or organization hiring personal data protection services, an organization providing personal data protection services shall perform the tasks of a personal data protection unit for such agency or organization.

6. An organization providing personal data protection services shall:

a) Provide services strictly within the scope and tasks stipulated in the contract or agreement;

b) Refrain from abusing the provision of services to commit violations of the law;

c) Perform the deletion and destruction of personal data processed during service provision after completion of the contract and in accordance with the law.

Chapter III

DOSSIERS AND PROCEDURES RELATING TO PERSONAL DATA

Article 17. Cross-border personal data transfer

1. The personal data controlling party, personal data processing and controlling party, personal data processing party, and third parties shall carry out cross-border transfer of personal data in the following cases:

a) Personal data storage activities involving the transfer of personal data collected and stored in Vietnam to server systems located outside the territory of the Socialist Republic of Vietnam or to cloud computing services of foreign service providers;

b) Activities involving the transfer of personal data from agencies, organizations, or individuals in Vietnam to receiving organizations or individuals located overseas;

c) Personal data processing activities in which personal data collected in Vietnam is transferred to platforms outside the territory of the Socialist Republic of Vietnam for further processing.

2. The personal data protection authority shall decide to require the cross-border data transferring party to cease cross-border transfer of personal data in the following cases:

a) Where transferred personal data is discovered to be used for activities infringing on national defense or national security;

b) Where violations of personal data protection regulations occur that may cause harm to national defense or national security.

3. In cases other than those specified in Points a, b, and c Clause 6 Article 20 of the Law on Personal Data Protection, the following cases are not required to conduct an impact assessment of cross-border transfer of personal data:

a) Journalism and communication activities in accordance with the law;

b) Cross-border transfer of personal data that has been disclosed in accordance with the law;

c) Emergencies where it is genuinely necessary to provide personal data across borders to protect life, health, or property safety of individuals or to perform tasks and obligations as prescribed by law;

d) Cross-border transfer of personal data for cross-border personnel management in accordance with labor rules and regulations, and collective labor agreements as prescribed by law;

dd) Provision of personal data across borders for contract conclusion or for carrying out procedures related to cross-border transportation, logistics, remittance, payment, accommodation, visa applications, or scholarship applications.

Article 18. Conditions, procedures, and dossier components for impact assessment of cross-border transfer of personal data

1. Agencies, organizations, and individuals carrying out the cross-border transfer of personal data as prescribed in Clause 1 Article 20 of the Law on Personal Data Protection shall prepare a dossier for the impact assessment of the cross-border transfer of personal data in accordance with this Article.

2. The dossier for the impact assessment of the cross-border transfer of personal data shall include:

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

b) A copy of the personal data transfer contract or document evidencing binding obligations and responsibilities between organizations and individuals transferring and receiving personal data across borders;

c) Policies, procedures, regulations, forms, and other relevant documents on personal data protection of the agency, organization, or individual carrying out the cross-border transfer of personal data.

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

a) Information and contact details of the personal data transferring party, the personal data receiving party, the personal data processing party, and other parties related to the cross-border transfer of personal data;

b) Contact details of the personal data protection unit and personal data protection personnel; personal data protection service providers (if any) of the personal data transferring party and the personal data receiving party;

c) Description and explanation of the purposes of the cross-border transfer of personal data, the types of personal data transferred across borders, detailed activities relating to the cross-border transfer and processing of personal data, and a diagram of personal data processing flows;

d) Description and explanation of the obtaining of consent from the personal data subject matter, policies on storage, deletion, and destruction of personal data;

dd) Plans for ensuring personal data safety after the cross-border transfer, the applied personal data protection measures, and the applied personal data protection standards;

e) System diagrams and description of functions of systems storing and processing personal data after receipt of personal data transferred across borders;

g) Procedures for the onward transfer or provision of personal data by the cross-border personal data receiving party to third parties;

h) Results of self-assessment of compliance with personal data protection regulations by the agency, organization, or individual carrying out the cross-border transfer of personal data;

i) Assessment of the level of personal data protection of the personal data receiving party; the degree of impact and risks arising from the cross-border transfer and processing of personal data; potential adverse consequences or damages; and measures to mitigate or eliminate such risks.

4. The dossier for the impact assessment of the cross-border transfer of personal data shall be kept readily available for inspection and assessment by the personal data protection authority.

The cross-border personal data transferring party shall submit 1 original complete dossier online, in person, or by post to the personal data protection authority, together with Form No. 01a/01b in the Appendix of this Decree, within 60 days from the date of commencement of the cross-border transfer of personal data.

5. The personal data protection authority shall assess and issue results indicating whether the dossier for the impact assessment of the cross-border transfer of personal data meets or fails to meet requirements within 15 days.

6. Where the dossier for the impact assessment of the cross-border transfer of personal data is incomplete or non-compliant, the personal data protection authority shall assess and request the cross-border personal data transferring party to complete the dossier within 30 days. Where the transferring party fails to complete the dossier in accordance with regulations, the personal data protection authority shall consider applying regulations on penalties for administrative violations in the field of personal data protection in accordance with the law.

7. The cross-border personal data transferring party shall update and supplement the dossier for the impact assessment of the cross-border transfer of personal data in accordance with Article 20 of this Decree.

Article 19. Conditions, procedures, and dossier components for impact assessment of personal data processing

1. The personal data controlling party, the personal data processing and controlling party, and the personal data processing party shall prepare and retain their dossier for the impact assessment of personal data processing from the time personal data processing commences.

2. The dossier for the impact assessment of personal data processing of the personal data controlling party, the personal data processing and controlling party, and the personal data processing party shall include:

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

b) A copy of the contract or agreement on personal data processing, demonstrating binding obligations and responsibilities among organizations and individuals involved in personal data processing;

c) Policies, procedures, regulations, forms, and other relevant documents on personal data protection of the personal data controlling party, the personal data processing and controlling party, and the personal data processing party.

3. The report on the impact assessment of personal data processing shall include the following contents:

a) Information and contact details of the personal data controlling party, the personal data processing and controlling party, the personal data processing party, and third parties;

b) Contact details of the personal data protection unit and personal data protection personnel; personal data protection service providers (if any) of the personal data controlling party, the personal data processing and controlling party, the personal data processing party, and third parties;

c) Description and explanation of the purposes of personal data processing, the types of personal data processed, detailed personal data processing activities, and a personal data flow diagram;

d) Description and explanation of the obtaining of consent from the personal data subject matter, policies on storage, deletion, and destruction of personal data;

dd) Plans for ensuring personal data safety, personal data protection measures, system design diagrams, and the applied personal data protection standards;

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

g) Assessment of the level of impact and risks arising from personal data processing activities; potential adverse consequences or damages; and measures to mitigate or eliminate such risks.

4. The dossier for the impact assessment of personal data processing shall be kept readily available for inspection and assessment by the personal data protection authorities, and 1 original copy shall be submitted online, in person, or by post to the personal data protection authority together with Form No. 02a/02b in the Appendix of this Decree within 60 days from the date personal data processing is carried out.

5. The personal data protection authority shall assess and issue results indicating whether the dossier for impact assessment of personal data processing meets or fails to meet requirements within 15 days.

6. Where the dossier for the impact assessment of personal data processing is incomplete or non-compliant, the personal data protection authority shall assess and request the personal data controlling party, the personal data processing and controlling party, or the personal data

processing party to complete the dossier within 30 days. In the event of failure to complete the dossier in accordance with regulations, the personal data protection authority shall consider applying regulations on penalties for administrative violations in the field of personal data protection.

7. The personal data controlling party, the personal data processing and controlling party, and the personal data processing party shall update and supplement the dossier for the impact assessment of personal data processing in accordance with Article 20 of this Decree.

Article 20. Updating of dossiers for impact assessment of personal data processing and dossiers for impact assessment of cross-border transfer of personal data

1. The dossier for cross-border transfer of personal data and the dossier for the impact assessment of personal data processing shall be updated periodically every 6 months from the date of initial submission in the following cases:

a) Where new purposes for cross-border transfer of personal data or new purposes for personal data processing arise;

b) Where the personal data controlling party, the personal data processing and controlling party, the personal data processing party, and/or third parties arise or are changed.

2. The following changes shall be updated immediately within 10 days:

a) When an agency, organization, or unit undergoes reorganization, operational termination, dissolution, or bankruptcy in accordance with the law;

b) Where there is a change in information relating to personal data protection service providers;

c) Where business lines, professions, or services related to personal data processing that have been registered in the dossier for the impact assessment of personal data processing or the dossier for the impact assessment of the cross-border transfer of personal data arise or are changed.

3. The updating of the dossier for the impact assessment of personal data processing and the dossier for the impact assessment of the cross-border transfer of personal data shall be carried out in accordance with Form No. 03a/03b in the Appendix of this Decree and submitted online, in person, or by post to the personal data protection authority.

Article 21. Personal data processing services

1. Services providing and operating automated systems and software to process personal data on behalf of the personal data controlling party or the personal data processing and controlling party.

2. Services for scoring, rating, and assessing the creditworthiness of the personal data subject matter.

3. Services for collecting and processing personal data online from websites, applications, software, and social networks.

4. Services for collecting and processing personal data through websites, applications, and software for health care and health monitoring, as well as healthcare services.

5. Services for collecting and processing personal data through educational applications and software with supervision elements such as attendance tracking, video recording, behavior scoring, and emotion recognition.

6. Services for analysis and utilization of personal data, including: using analytical tools to identify information, trends, and patterns from personal data; applying data mining methods to extract value from personal data, predict user behavior, or optimize services.

7. Services for encrypting personal data during transmission and storage.

8. Services for automated personal data processing based on big data technology, artificial intelligence, blockchain, and the metaverse.

9. Platform application services providing personal location data.

Article 22. Conditions for organizations engaged in personal data processing services

1. Being an organization or enterprise established and operating in accordance with the law of Vietnam and satisfying the conditions prescribed in this Article.

2. Conditions relating to personnel:

a) Ensuring that the head responsible for professional matters related to personal data processing of the organization is a Vietnamese citizen permanently residing in Vietnam;

b) Having a management and executive team meeting professional requirements for personal data processing;

c) Having at least 3 personnel satisfying the competency conditions specified in Clause 2 Article 13 of this Decree;

3. Having infrastructure, equipment systems, facilities, and technology suitable for personal data processing services.

4. Having satisfactory results for the dossier for the impact assessment of personal data processing and the dossier for the impact assessment of the cross-border transfer of personal data in cases involving cross-border transfer of personal data.

Article 23. Responsibilities of organizations providing personal data processing services

1. Fully comply with the law on personal data protection, and with the responsibilities and obligations of the personal data processing and controlling party and the personal data processing party.

2. Establish a personal data protection risk management framework appropriate to the services provided.

3. Conduct periodic assessments of the current compliance status and credibility level in personal data protection once per year.

4. Apply relevant standards and technical regulations concerning data security, personal data protection, and cybersecurity.

5. Develop regulations related to the responsibilities and entitlements of the organization for personal data processing.

6. Ensure that personal data processing is conducted for the correct purposes; limit the collection, transfer, and storage of personal data in accordance with the law; and prevent unauthorized access, collection, use, disclosure, or similar risks in personal data processing activities.

7. When acting as a personal data processing party, the organization shall require the personal data controlling party to obtain consent from the personal data subject matter in accordance with regulations before providing services, and ensure that the personal data subject matter is informed of the types of personal data processed, the processing purposes, as well as the organization providing personal data processing services.

8. Organizations providing personal data processing services shall perform organization identity authentication in accordance with the law on electronic identification and authentication.

Article 24. Authority to issue, re-issue, replace, and revoke certificates of eligibility for providing personal data processing services

1. The Ministry of Public Security of Vietnam shall issue, re-issue, replace, and revoke certificates of eligibility for providing personal data processing services.

2. The Minister of Public Security of Vietnam shall assign the personal data protection authorities to carry out the issuance, re-issuance, replacement, and revocation of certificates of eligibility for providing personal data processing services in accordance with regulations.

Article 25. Dossiers and procedures for issuing certificates of eligibility for providing personal data processing services

1. The dossier for applying for a certificate of eligibility for providing personal data processing services includes:

a) An application for the Certificate of eligibility for providing personal data processing services using Form No. 04 in the Appendix of this Decree;

b) A copy of the enterprise registration certificate;

c) A document designating a personal data protection unit or a contract for the use of personal data protection services in accordance with regulations;

d) A proposal for the issuance of the Certificate of eligibility for providing personal data processing services;

dd) Diplomas and other documents proving the qualifications of personnel specified in Point c Clause 2 Article 22 of this Decree;

e) The organization is not required to submit the document specified in Point b of this Clause if a state authority can access it on a database.

2. The proposal for the issuance of the certificate of eligibility for providing personal data processing services includes the following contents:

a) Necessity and objectives;

b) Proposed contents and fields for approval;

c) Business lines, business fields, and business plans;

d) Expected scale of personal data processing activities;

dd) Personal data protection risk management framework;

e) Periodic compliance status and credibility assessment plan for personal data protection;

g) Application of standards and technical regulations related to data security and personal data protection;

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

i) Responsibilities and entitlements of the organization in personal data processing;

k) Qualified personnel in accordance with regulations.

3. The organization shall submit 1 set of the application dossier for the certificate of eligibility for providing personal data processing services online, in person, or by post to the personal data protection authority.

The personal data protection authority shall assess whether the application dossier meets requirements or does not meet requirements within 10 days. If the dossier is incomplete or non-compliant, the personal data protection authority shall notify the organization in writing, specifying the reasons, and request supplementation and completion of the dossier within 15 days.

4. Within 30 days from the date of receipt of a complete and valid dossier, the personal data protection authority shall appraise, review, and decide the issuance of the certificate of eligibility for providing personal data processing services using Form No. 05 in the Appendix of this Decree. The certificate of eligibility for providing personal data processing services shall be issued in both physical and electronic forms. The physical form shall be issued in cases where the dossier is submitted in person or by post, or upon request when the dossier is submitted online through the public service portal. In case of refusal, the personal data protection authority shall notify the organization in writing and specify the reasons.

Article 26. Dossiers and procedures for re-issuing and replacing certificates of eligibility for providing personal data processing services

1. Re-issuance shall be applied in cases where the physical certificate of eligibility for providing personal data processing services is lost or damaged:

a) Where an organization requests re-issuance of the physical certificate, it shall submit an application using Form No. 05 in the Appendix of this Decree online, in person, or by post to the personal data protection authority.

b) Within 5 working days from the date of receipt of a valid application, the personal data protection authority shall review and re-issue the certificate of eligibility for providing personal data processing services; in case of refusal, a written notice specifying the reasons shall be issued.

2. Replacement shall be applied in cases of incorrect information or changes to the contents of the certificate of eligibility for providing personal data processing services:

a) The dossier includes: an application using Form No. 06 in the Appendix of this Decree; and documents and materials proving the incorrect information or changes to the contents stated in the issued certificate.

b) The organization shall submit 1 set of the above dossier online, in person, or by post to the personal data protection authority. Within 5 working days from the date of receipt of a complete dossier as prescribed in Point a of this Clause, the personal data protection authority shall review and decide the replacement of the certificate of eligibility for providing personal data processing services; in case of refusal, a written notice specifying the reasons shall be issued.

Article 27. Revocation of certificates of eligibility for providing personal data processing services

1. The certificate of eligibility for providing personal data processing services shall be revoked in the following cases:

a) Failure to satisfy any of the conditions specified in Clauses 1 and 2 Article 26 of this Decree;

b) Failure to conduct business activities for 12 months or more;

c) Dissolution or bankruptcy in accordance with law;

d) Failure to remedy violations related to personal data protection, information safety, cybersecurity, or data security at the request of a competent state authority;

dd) Voluntary request for suspension or termination of operations.

2. The personal data protection authority shall decide the revocation of the certificate of eligibility for providing personal data processing services using Form No. 07 in the Appendix of this Decree.

3. The organization providing personal data processing services shall return the issued certificate to the personal data protection authority within 5 working days from the date of receipt of the revocation decision.

4. Upon the issuance of a decision on the revocation of the certificate of eligibility for providing personal data processing services, the personal data protection authority shall announce it on the National Information Portal for Personal Data Protection.

Article 28. Contents of notification of violations of personal data protection regulations

1. A notification of violations of personal data protection regulations includes the following contents:

a) Description of the nature of the violation of personal data protection regulations, including time, location, conduct, organizations and individuals involved, types of personal data, and the volume of related data;

b) Contact details of the personal data protection unit, personnel, or personal data protection service providers;

c) Description of possible consequences and damage resulting from the violation of personal data protection regulations;

d) Description of measures proposed to remedy and mitigate the harm caused by the violation of personal data protection regulations.

2. The personal data controlling party, the personal data processing and controlling party, and the third-party processing party shall submit notifications of violations of personal data protection

regulations to the personal data protection authority or via the National Information Portal for Personal Data Protection using Form No. 08 in the Appendix of this Decree.

Article 29. Notification of violations involving personal location data and biometric data

1. Upon a personal data violation incident involving location data or biometric data, the personal data controlling party or the personal data processing and controlling party shall:

a) Notify the affected personal data subject matter within no more than 72 hours from the time the violation is detected;

b) Report to the competent state authority in accordance with Article 28 of this Decree;

c) Record, store, and update violation dossiers for inspection, examination, and handling purposes. Organizations shall retain violation dossiers for a minimum period of 5 years from the date the incident is fully remedied.

2. The notification to the personal data subject matter prescribed in Point a Clause 1 of this Article shall include at least the following contents:

a) The time and method of detection of the violation;

b) The type of data affected (location data, biometric data, or both);

c) The level of severity and potential risks to the legitimate rights and interests of the personal data subject matter;

d) Measures that have been, are being, and will be implemented to remedy the incident and mitigate damage;

dd) Instructions for the personal data subject matter to implement subsequent preventive and protective measures;

e) Contact information of the personal data protection unit or personnel, or personal data protection service providers; and the unit responsible for receiving and handling personal data incidents within the organization.

3. In cases where an organization or individual is unable to notify all affected personal data subject matters within the time limit specified in Clause 1 of this Article due to technical or emergency reasons, it shall:

a) Make a public notification via the organization’s official electronic means, including its website or application;

b) Send notifications to the relevant personal data subject matters immediately once technical conditions permit.

4. Where an organization or individual fails to provide timely notification or deliberately delays or evades the notification obligation, such conduct shall be considered for handling of violations in accordance with the law.

Chapter IV

IMPLEMENTATION OF PERSONAL DATA PROTECTION

Article 30. Responsibilities for implementing international cooperation in personal data protection

1. Personal data protection authorities shall assist the Ministry of Public Security of Vietnam in implementing international cooperation in personal data protection.

2. Ministries, ministerial agencies, and governmental agencies shall carry out international cooperation in personal data protection in sectors and fields under their management in accordance with the law and their assigned functions and tasks.

3. Provincial People's Committees shall implement international cooperation in personal data protection in accordance with the law and their assigned functions and tasks.

Article 31. Inspection of personal data protection activities

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

a) Where there are grounds to suspect violations of the law on personal data protection;

b) Upon directives of competent authorities or persons responsible for state management of personal data protection;

c) When performing state management in accordance with the law.

2. Subjects of inspection of personal data protection activities include:

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

b) Personal data processing service providers;

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

d) Agencies, organizations, and individuals related to cases or incidents involving violations of personal data protection regulations.

3. Contents of inspection of personal data protection activities include:

a) The current status of compliance with personal data protection requirements;

b) Activities related to personal data processing impact assessments and cross-border personal data transfer impact assessments;

c) Business activities concerning the provision of personal data processing services.

4. Personal data protection authorities shall issue inspection decisions and notify the inspection subjects specified in Clause 2 of this Article, at least 15 days in advance, of the time, contents, and composition of the inspection team. In cases of ad hoc inspections conducted to promptly verify, detect, and prevent violations of the law on personal data protection, personal data protection authorities may conduct inspections immediately without prior notice.

5. Inspection subjects shall fully prepare the inspection contents in accordance with Clause 3 of this Article and specific requirements stated in the inspection decisions issued by the personal data protection authorities.

Article 32. Research and development of personal data protection solutions

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

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

2. Methods for appraising software and equipment for personal data protection to meet prescribed standards;

3. Methods for testing hardware and software supplied to ensure the correct performance of intended functions;

4. Recording and management of compliance with personal data protection regulations;

5. Settlement of risks of leakage or loss of personal data;

6. Technical initiatives to enhance awareness and skills related to personal data protection;

7. Processing of personal data for statistical and scientific purposes;

8. Solutions enabling the personal data subject matter to control their own personal data, provide and share data under selective disclosure mechanisms, and apply advanced and strategic technologies in accordance with international standards and technical regulations;

9. Personal data protection standards;

10. Other personal data protection solutions in accordance with the law.

Article 33. Contents of state management of personal data protection

1. Promulgating, within assigned authority, or submitting to competent state authorities for promulgation, legislative documents on personal data protection; and organizing the implementation of the law on personal data protection.

2. Developing and organizing the implementation of strategies, policies, schemes, projects, programs, and plans on personal data protection.

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

4. Disseminating and educating on the law on personal data protection; conducting communications and dissemination of knowledge and skills related to personal data protection.

5. Building, training, fostering, and developing human resources for personal data protection.

6. Conducting inspection, examination, commendation, settlement of complaints and denunciations, and handling of violations of the law on personal data protection in accordance with the law.

7. Conducting statistics, information collection, and reporting on the status of personal data protection and implementation of the law on personal data protection to the competent state authorities.

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

9. Conducting international cooperation in personal data protection.

Article 34. Responsibilities of Ministry of Public Security of Vietnam

1. Assist the Government of Vietnam in ensuring consistent state management of personal data protection.

2. Develop, promulgate, or submit to competent state authorities for promulgation, and guide the implementation of legislative documents guiding the implementation of the law on personal data protection.

3. Guide and implement personal data protection activities, and protect the rights of personal data subject matters against acts that violate the law on personal data protection.

4. Take charge and cooperate with the Ministry of Science and Technology of Vietnam in developing standards and technical regulations on personal data protection, as well as technical

regulations on de-identification and anonymization of personal data to be promulgated and applied in Vietnam.

5. Develop, manage, and operate the National Information Portal for Personal Data Protection.

6. Implement dissemination, communications, and legal education activities, and provide guidelines and training to enhance knowledge and skills on personal data protection for personal data protection forces.

7. Conduct assessments, preliminary reviews, and final reviews of the results of personal data protection activities of relevant agencies, organizations, and individuals.

8. Promote scientific research on personal data protection; research and apply scientific and technological advances related to personal data protection for innovation.

9. Implement international cooperation activities in personal data protection.

Article 35. Responsibilities of Ministry of National Defense of Vietnam

1. Cooperate with the Ministry of Public Security of Vietnam and relevant agencies and organizations in deploying forces and equipment to protect personal data, and to detect and prevent acts violating regulations on personal data protection within its management scope.

2. Within assigned functions and tasks, take charge and cooperate with the Ministry of Public Security of Vietnam in assessing the results of personal data protection activities of agencies, organizations, and individuals under its management; promote the application of personal data protection measures; research and apply advanced security technologies in the processing and protection of personal data for national defense activities; and conduct international cooperation in personal data protection within its management scope in accordance with the law.

3. Organize dissemination, communications, and legal education on personal data protection, as well as knowledge and skills training in personal data protection for commissioned officers, professional soldiers, cadres, civil servants, and public employees under its management.

4. Conduct inspection, examination, supervision, and handling of violations of regulations on personal data protection with respect to agencies, organizations, and individuals under the management scope of the Ministry of National Defense of Vietnam in accordance with the law and assigned functions and tasks.

Article 36. Responsibilities of Ministry of Science and Technology of Vietnam

1. Cooperate with the Ministry of Public Security of Vietnam in developing standards and technical regulations on personal data protection, as well as technical regulations on de-identification and anonymization of personal data to be promulgated and applied in Vietnam.

2. Cooperate with the Ministry of Public Security of Vietnam and relevant agencies in researching, developing, mastering, and applying personal data protection measures utilizing advanced, high-level, and strategic technologies, and in forming personal data protection solutions, products, and services in the course of developing the digital government, digital economy, and digital society through scientific and technological programs.

Article 37. Responsibilities of ministries, ministerial agencies, and governmental agencies

1. Perform the state management of personal data protection for sectors and fields within their management scope in accordance with the law.

2. Develop and implement contents and tasks concerning personal data protection prescribed in this Decree.

3. Incorporate personal data protection regulations in the development and implementation of tasks of ministries and sectors.

4. Arrange personnel and establish personal data protection units within units under their management; ensure that capacity requirements are met and are appropriate to job positions and professional requirements for personal data protection in accordance with the law.

5. Allocate funding for personal data protection activities in accordance with the current budget regulations.

6. Organize dissemination and education of the law, and advanced training in professional matters and skills for cadres, civil servants, public employees, and units under their management concerning personal data protection.

7. Cooperate with the Ministry of Public Security of Vietnam in the inspection, examination, supervision, and handling of violations of regulations on personal data protection within their management scope.

8. Cooperate with the Ministry of Public Security of Vietnam and the Ministry of Science and Technology of Vietnam in developing guidelines and implementing the application of standards and technical regulations on personal data protection for agencies, organizations, and individuals under their management.

Article 38. Responsibilities of People's Committees of provinces

1. Perform the state management of personal data protection for sectors and fields within their management in accordance with the law on personal data protection

2. Implement the regulations on personal data protection prescribed in this Decree.

3. Arrange personnel and establish personal data protection units within units under their management; ensure that capacity requirements are met and are appropriate to job positions and professional requirements for personal data protection in accordance with the law.

4. Allocate funding for personal data protection activities in accordance with the current budget regulations.

5. Organize dissemination and communications of the law, and knowledge and skills concerning personal data protection for cadres, civil servants, public employees, citizens, and enterprises within their areas.

6. Organize advanced training to enhance capacity for personnel engaged in personal data protection work at all administrative levels; integrate personal data protection content into administrative reform and digital transformation programs.

7. Develop statistical systems, aggregate information, and submit periodic reports on the local status of personal data protection to the personal data protection authorities in accordance with regulations.

Article 39. Personal data protection authorities and National Information Portal for Personal Data Protection

1. Personal data protection authorities are units under the Ministry of Public Security of Vietnam, responsible for assisting the Minister of Public Security of Vietnam in performing the state management function concerning personal data protection.

2. The National Information Portal for Personal Data Protection serves as a platform for providing information to disseminate the CPV's guidelines and policies and the State's personal data protection laws; supporting guidance, enhancing awareness, and improving personal data protection skills for agencies, organizations, and individuals; receiving and handling feedback and petitions from relevant agencies, organizations, and individuals; and carrying out other activities in accordance with the law on personal data protection.

Article 40. Funding for ensuring personal data protection activities

1. Funding for the implementation of personal data protection includes the state budget, contributions from domestic and foreign agencies, organizations, and individuals, revenue from the provision of personal data protection services, international aid, and other legal sources of revenue.

2. Funding for personal data protection activities of state agencies is covered by the state budget and allocated in the annual state budget estimates. The management and use of state budget funding are carried out in accordance with the law on the state budget.

3. Funding for personal data protection activities of organizations and enterprises shall be allocated by the organizations and enterprises themselves and implemented in accordance with regulations.

Chapter V

IMPLEMENTATION

Article 41. Regulations on application of Clause 2 and Clause 3 of Article 38 of Law on Personal Data Protection

1. Small-sized enterprises and startups may choose whether or not to implement Article 21, Article 22, and Clause 2 Article 33 of the Law on Personal Data Protection for a period of 5 years from the effective date of the Law on Personal Data Protection, except for those providing personal data processing services, directly processing sensitive personal data, or processing personal data from the time their scale reaches 100 thousand or more personal data subject matters, based on the accumulated total volume of personal data processed.

2. Household businesses and micro-enterprises are not required to comply with Article 21, Article 22, and Clause 2 Article 33 of the Law on Personal Data Protection, excluding those providing personal data processing services, directly processing sensitive personal data, or processing personal data from the time their scale reaches 100 thousand or more personal data subject matters, based on the accumulated total volume of personal data processed.

Article 42. Entry into force and implementation responsibilities

1. This Decree comes into force as of January 1, 2026.

2. Decree No. 13/2023/ND-CP dated April 17, 2023 of the Government of Vietnam shall cease to have effect from the effective date of this Decree.

3. Amendments to Clause 2 Article 16 of Decree No. 165/2025/ND-CP dated June 30, 2025 of the Government of Vietnam:

“2. The protection of core data and important data constituting personal data shall be implemented in accordance with the Law on Personal Data Protection and documents elaborating such Law.

In cases of cross-border transfer or processing of core data and important data that constitutes personal data, the governing body of core data and important data shall prepare dossiers for personal data processing impact assessment and cross-border personal data transfer impact assessment in accordance with the law on personal data protection, and not be required to conduct risk assessment or impact assessment for cross-border data transfer or processing as prescribed in this Decree.”

4. The Ministry of Public Security of Vietnam shall provide guidelines, inspect, and urge the implementation of this Decree.

5. Ministers, Directors of ministerial agencies, Directors of governmental agencies, Presidents of People's Committees of provinces, and relevant agencies, organizations, and individuals shall implement this Decree.

ON BEHALF OF THE GOVERNMENT
PP. PRIME MINISTER
DEPUTY PRIME MINISTER

Nguyen Hoa Binh

APPENDIX

LIST OF DOSSIERS AND FORMS
(Enclosed with Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam)

Form No. 01a	Notification of submission of dossier for cross-border personal data transfer impact assessment (for organizations)
Form No. 01b	Notification of submission of dossier for cross-border personal data transfer impact assessment (for organizations)
Form No. 02a	Notification of submission of dossier for personal data processing impact assessment (for organizations)
Form No. 02b	Notification of submission of dossier for personal data processing impact assessment (for individuals)
Form No. 03a	Notification of update of impact assessment dossier (for organizations)
Form No. 03b	Notification of update of impact assessment dossier (for individuals)
Form No. 04	Application for issuance of the Certificate of eligibility for providing personal data processing services
Form No. 05	Decision on issuance of the Certificate of eligibility for providing personal data processing services

Form No. 06	Application for re-issuance or replacement of the Certificate of eligibility for providing personal data processing services
Form No. 07	Decision on revocation of the Certificate of eligibility for providing personal data processing services
Form No. 08	Notification of violations of regulations on personal data protection
Form No. 09	Report on cross-border personal data transfer impact assessment
Form No. 10	Report on personal data processing impact assessment

Form No. 01a

NAME OF ORGANIZATION

No.:.....

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Location, date

NOTIFICATION
OF SUBMISSION OF DOSSIER FOR CROSS-BORDER PERSONAL DATA TRANSFER IMPACT ASSESSMENT

To: The personal data protection authority, Ministry of Public Security of Vietnam.

In compliance with regulations on personal data protection, ...[1] hereby submits to the personal data protection authority, Ministry of Public Security of Vietnam, the dossier for cross-border personal data transfer impact assessment, as follows:

1. Information on the organization/enterprise

- Vietnamese trading name - Vietnamese abbreviated name: .....

- English trading name - English abbreviated name: .....

- Address of headquarters: .....

- Address of transaction office: .....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment registration certificate No.: …… issued by …… on ……(date) at …

- Tax identification number: .....

- Phone number: ..... Website: .....

- Personal data protection unit/personnel or personal data protection service provider of the personal data transferring party: .....

Full name: .....

Position: .....

Contact phone number (landline and mobile): .....

Email: .....

2. Dossier for cross-border personal data transfer impact assessment *(including forms, documents, written materials, and enclosed images)*

a) .....

b) .....

3. Commitment

.....[2] hereby commits to taking responsibility for the accuracy and legality of the dossier for cross-border personal data transfer impact assessment and the enclosed documents, and commits to fully complying with the law.

ON BEHALF OF THE
ORGANIZATION/ENTERPRISE
(Signature, full name, seal)

---

[1] Name of organization/enterprise.

[2] Name of organization/enterprise.

Form No. 01b

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Location, date

NOTIFICATION
OF SUBMISSION OF DOSSIER FOR CROSS-BORDER PERSONAL DATA TRANSFER IMPACT ASSESSMENT

To: The personal data protection authority, Ministry of Public Security of Vietnam.

In compliance with regulations on personal data protection, I hereby submit to the personal data protection authority, Ministry of Public Security of Vietnam, the dossier for cross-border personal data transfer impact assessment, as follows:

1. Information on the applicant

- Full name: .....

- Address: .....

9-digit ID card/Citizen ID card/Passport No.:.....

Issued on …… / …… / …… at .....

- Phone number:.....

- Email:.....

- Affiliated organization (if any): .....

2. Dossier for cross-border personal data transfer impact assessment *(including forms, documents, written materials, and enclosed images)*

a) .....

b) .....

3. Commitment

I hereby commit to taking responsibility for the accuracy and legality of the contents of the dossier and the enclosed documents, and commit to fully complying with the law.

APPLICANT

(Signature, full name)

Form No. 02a

NAME OF ORGANIZATION **-------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:.....	*Location, date*

NOTIFICATION
OF SUBMISSION OF DOSSIER FOR PERSONAL DATA PROCESSING IMPACT ASSESSMENT

To: The personal data protection authority, Ministry of Public Security of Vietnam

In compliance with regulations on personal data protection, ...[1] hereby submits to the personal data protection authority, Ministry of Public Security of Vietnam, the dossier for personal data processing impact assessment, as follows:

1. Information on the organization/enterprise

- Name of organization/enterprise (Vietnamese - foreign language):.....

- Address of headquarters:.....

- Address of transaction office:.....

- Type of enterprise (domestic/foreign):.....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment registration certificate No.: …… issued by …… on ……(date) at …

- Tax identification number:.....

- Legal representative:.....

- Phone number: ..... Website:.....

- Personal data protection unit/personnel or personal data protection service provider:.....

Full name:.....

Position:.....

Contact phone number (landline and mobile):.....

Email:.....

2. Dossier for personal data processing impact assessment *(including forms, documents, written materials, and enclosed images)*

a) .....

b) .....

3. Commitment

.....[2] hereby commits to taking responsibility for the accuracy and legality of the dossier for personal data processing impact assessment and the enclosed documents, and commits to fully complying with the law.

ON BEHALF OF THE ORGANIZATION/ENTERPRISE
(Signature, full name, seal)

---

[1] Name of organization/enterprise.

[2] Name of organization/enterprise.

Form No. 02b

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

....., Location, date

NOTIFICATION
OF SUBMISSION OF DOSSIER FOR PERSONAL DATA PROCESSING IMPACT ASSESSMENT

To: The personal data protection authority, Ministry of Public Security of Vietnam.

In compliance with regulations on personal data protection, I hereby submit to the personal data protection authority, Ministry of Public Security of Vietnam, the dossier for personal data processing impact assessment, as follows:

1. Information on the applicant

- Full name: .....

- Address: .....

9-digit ID card/Citizen ID card/Passport No.:.....

Issued on …… / …… / …… at .....

- Phone number:.....

- Email:.....

- Affiliated organization (if any): .....

2. Dossier for personal data processing impact assessment *(including forms, documents, written materials, and enclosed images)*

a) .....

b) .....

3. Commitment

I hereby commit to taking responsibility for the accuracy and legality of the contents of the dossier and the enclosed documents, and commit to fully complying with the law.

APPLICANT
(Signature, full name)

Form No. 03a

NAME OF ORGANIZATION **-------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:.....	*Location, date*

NOTIFICATION
OF AMENDMENTS TO DOSSIER .....[1]

To: The personal data protection authority, Ministry of Public Security of Vietnam.

In compliance with regulations on personal data protection,.....[2] hereby submits to the personal data protection authority, Ministry of Public Security, the dossier for personal data processing impact assessment, as follows:

1. Information on the organization/enterprise

- Name of organization /enterprise:.....

- Address of headquarters:.....

- Address of transaction office:.....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment registration certificate No.: …… issued by …… on ……(date) at …

- Tax identification number: .....

- Phone Number: ..... Website.....

- Personnel responsible for personal data protection:.....

Full name:.....

Title:.....

Contact phone number (landline and mobile):.....

Email:.....

2. Brief description of the amended content of the dossier

- Amended content:.....

- Reason for amendment:.....

3. Enclosed documents

a) .....

b) .....

4. Commitment

.....[3] hereby commits to taking responsibility for the accuracy and legality of the amended content and the enclosed documents, and commits to fully complying with the law.

ON BEHALF OF THE
ORGANIZATION/ENTERPRISE
(Signature, full name, seal)

---

[1] Name of the dossier: Dossier for personal data processing impact assessment or dossier for cross-border personal data transfer impact assessment.

[2] Name of organization/enterprise.

[3] Name of organization/enterprise.

Form No. 03b

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

....., Location, date

NOTIFICATION
OF AMENDMENTS TO DOSSIER .....[1]

To: The personal data protection authority, Ministry of Public Security of Vietnam

In compliance with regulations on personal data protection, I hereby submit to the personal data protection authority, Ministry of Public Security of Vietnam, the dossier for personal data processing impact assessment, as follows:

1. Information on the applicant

- Full name:.....

- Address:.....

9-digit ID card/Citizen ID card/Passport No.:.....
Issued on …… / …… / …… at .....

- Phone number:.....

- Email:.....

- Affiliated organization (if any): .....

2. Brief description of the amended content of the dossier

- Amended content:.....

- Reason for amendment:.....

3. Enclosed documents

a) .....

b) .....

4. Commitment

I hereby commit to taking responsibility for the accuracy and legality of the contents of the dossier and the enclosed documents, and commit to fully complying with the law.

APPLICANT
(Signature, full name)

---

[1] Name of the dossier: Dossier for personal data processing impact assessment or dossier for cross-border personal data transfer impact assessment.

Form No. 04

NAME OF ORGANIZATION **-------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:.....	*Location, date*

APPLICATION
FOR ISSUANCE OF CERTIFICATE OF ELIGIBILITY FOR PROVIDING PERSONAL DATA PROCESSING SERVICES

To: Ministry of Public Security of Vietnam.

Pursuant to Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam, ...[1] hereby submits to the Ministry of Public Security of Vietnam an application for issuance of the Certificate of eligibility for providing personal data processing services, as follows:

1. Information on the organization applying for the Certificate

- Vietnamese trading name - Vietnamese abbreviated name:.....

- English trading name - English abbreviated name:.....

- Address of headquarters:.....

- Address of transaction office:.....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment registration certificate No.: …… issued by …… on ……(date) at …

- Tax identification number:.....

- Phone number: ..... Fax:.....

- Website: ..... Email:.....

- Name and contact address of the legal representative:

.....

- Personnel responsible for personal data protection:.....

(1) Full name:.....

Title:.....

Contact phone number:.....

Email:.....

(2) Full name:.....

Title:.....

Contact phone number:.....

Email:.....

(3) Full name:.....

Title:.....

Contact phone number:.....

Email:.....

2. List of personal data processing services for which Certificate is requested

No.	Name of service	Scope/field of provision
1		
2		

3. Application dossier for issuance of the Certificate

No.	Name of document	Quantity	Remarks
1			
2			
3			
...			

4. Commitment

.....[2] hereby commits to taking responsibility for the accuracy and legality of this application and the enclosed documents, and commits to fully complying with the law.

ON BEHALF OF THE
ORGANIZATION/ENTERPRISE
(Signature, full name, seal)

---

[1] Name of organization/enterprise.

[2] Name of organization/enterprise.

Form No. 05

MINISTRY OF PUBLIC SECURITY OF VIETNAM	**SOCIALIST REPUBLIC OF VIETNAM**
-------	**Independence - Freedom - Happiness**

No.:.....	*Location, date*

CERTIFICATE
OF ELIGIBILITY FOR PROVIDING PERSONAL DATA PROCESSING SERVICES
.....

Pursuant to Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam elaborating on certain articles and implementation measures of the Law on Personal Data Protection;

Pursuant to Decree No. 02/2025/ND-CP dated February 18, 2025 of the Government of Vietnam on functions, tasks, entitlements, and organizational structure of the Ministry of Public Security of Vietnam;

Based on the application dossier for issuance of the Certificate of eligibility for providing personal data processing services dated ... of ……[(1)];

At the request of .....

CERTIFICATES THAT

Article 1. .....[(1)] satisfies the conditions for providing personal data processing services, with the following information:

1. Trading name in Vietnamese or foreign language:

.....

2. Full name of the legal representative:.....

3. Enterprise registration certificate/Establishment decision No.: .....
issued on … (date); Issuing authority: .....

4. Tax identification number:.....

5. Address of headquarters in
Vietnam:.....

6. Phone number:.....

7. E-mail:.....

Article 2. .....[(1)] shall strictly comply with Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam, and other relevant laws.

Article 3. This Certificate of eligibility for providing personal data processing services shall take effect from the date of signing.

DIRECTOR OF THE AUTHORITY
(Signature, seal, full name and title)

[(1)] Name of the applying organization.

Form No. 06

NAME OF ORGANIZATION **-------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:.....	*Location, date*

APPLICATION
FOR RE-ISSUANCE/REPLACEMENT OF CERTIFICATE OF ELIGIBILITY FOR PROVIDING PERSONAL DATA PROCESSING SERVICES

To: Ministry of Public Security of Vietnam.

Pursuant to Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam elaborating on certain articles and implementation measures of the Law on Personal Data Protection;

Pursuant to the Certificate of eligibility for providing personal data processing services No. …… dated… issued by the Department of Cybersecurity and High-Tech Crime Prevention and Control, Ministry of Public Security of Vietnam;

.....[1] hereby submits to the Ministry of Public Security of Vietnam an application for re-issuance/replacement of the Certificate of eligibility for providing personal data processing services, as follows:

1. Information on the organization applying for the Certificate

- Vietnamese trading name - Vietnamese abbreviated name:.....

- English trading name - English abbreviated name:.....

- Address of headquarters:.....

- Address of transaction office:.....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment registration certificate No.: …… issued by …… on ……(date) at …

- Tax identification number:.....

- Phone number: ..... Fax: .....

- Website: ..... Email: .....

- Name and contact address of the legal representative:

.....

- Personnel responsible for personal data protection:.....

(1) Full name:.....

Title:.....

Contact phone number:.....

Email:.....

(2) Full name:.....

Title:.....

Contact phone number:.....

Email:.....

(3) Full name:.....

Title:.....

Contact phone number:.....

Email:.....

2. Content of re-issuance/amendment

- Reason for re-issuance/amendment of the Certificate:

.....

- Amended content of the Certificate:

.....

3. Enclosed documents

a) .....

b) .....

4. Commitment

.....[2] hereby commits to taking responsibility for the accuracy and legality of this application and the enclosed documents, and commits to complying with the law.

ON BEHALF OF THE
ORGANIZATION/ENTERPRISE
(Signature, full name, seal)

_____

[1] Name of organization/enterprise.

[2] Name of organization/enterprise.

Form No. 07

MINISTRY OF PUBLIC SECURITY OF VIETNAM	**SOCIALIST REPUBLIC OF VIETNAM**
-------	**Independence - Freedom - Happiness**

No.:.....	*Location, date*

DECISION

ON REVOCATION OF CERTIFICATE OF ELIGIBILITY FOR PROVIDING PERSONAL DATA PROCESSING SERVICES

.....

Pursuant to Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam elaborating on certain articles and implementation measures of the Law on Personal Data Protection;

Pursuant to Decree No. 02/2025/ND-CP dated February 18, 2025 of the Government of Vietnam on functions, tasks, entitlements, and organizational structure of the Ministry of Public Security of Vietnam;

At the request of .....

HEREBY DECIDES:

Article 1. The Certificate of eligibility for providing personal data processing services with the following information shall be revoked:

1. Certificate No.: …… issued on … (date)

2. Name of organization:.....

3. Full name of the legal representative:.....

4. Tax identification number:.....

5. Address of headquarters in Vietnam:.....

Article 2. This Decision comes into force as of its date of signing.

Article 3. The Department of Cybersecurity and High-Tech Crime Prevention and Control and the organization named in Article 1 shall implement this Decision.

DIRECTOR OF THE AUTHORITY
(Signature, seal, full name and title)

Form No. 08

NAME OF ORGANIZATION **-------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:.....	*Location, date*

NOTIFICATION
OF VIOLATIONS OF REGULATIONS ON PERSONAL DATA PROTECTION

To: The personal data protection authority, Ministry of Public Security of Vietnam.

In compliance with regulations on personal data protection, ...[1] hereby submits to the personal data protection authority, Ministry of Public Security of Vietnam, a notice of violation of personal data protection regulations, as follows:

1. Information on the organization/enterprise

- Name of organization /enterprise:.....

- Address of headquarters:.....

- Address of transaction office:.....

- Establishment Decision/Enterprise Registration Certificate/Business Registration Certificate/Investment Registration Certificate No.: …… issued by …… on ……(date) at …

- Tax identification number:.....

- Phone number: ..... Website:.....

- Personnel responsible for personal data protection:

Full name:.....

Title:.....

Contact phone number:.....

Email:.....

2. Description of the violation of personal data protection regulations

- Time:.....

- Location:.....

- Violating act:.....

- Related organizations and individuals:.....

- Types of personal data and volume of related data:.....

- Personnel responsible for personal data protection:.....

Full name:.....

Title:.....

Contact phone number:.....

Email:.....

- Consequences incurred:.....

- Measures applied:.....

3. Enclosed documents

a) .....

b) .....

4. Commitment

.....[2] hereby commits to taking responsibility for the accuracy and legality of this notification and the enclosed documents, and commits to complying with the law.

ON BEHALF OF THE
ORGANIZATION/ENTERPRISE
(Signature, full name, seal)

---

[1] Name of organization/enterprise.

[2] Name of organization/enterprise.

Form No. 09

DOSSIER
FOR CROSS-BORDER PERSONAL DATA TRANSFER IMPACT ASSESSMENT

PART A. DOSSIER FOR CROSS-BORDER PERSONAL DATA TRANSFER IMPACT ASSESSMENT OF THE TRANSFERRING PARTY			
I. BASIC INFORMATION OF THE TRANSFERRING PARTY			
1	Name of organization/individual *(Vietnamese):*	1a	Name of organization/individual *(foreign language):*
1b	Abbreviated name of organization/individual:	1c	Tax identification number:
2	Address *(headquarters):*		
3	Phone number:		
4	Business lines involving personal data processing *(enclosed with corresponding business line registration codes):*		
5	Number of branches, representative offices:		
6	Email:		
7	Website:		
8	**Personal data protection unit/personnel of the organization or individual**		
8.1	**Organization providing personal data protection services** *(if any; enclosed with the service contract):*		
	Name of organization: Tax identification number: Legal representative: Address: Phone number:		

Email: Website:

8.2 Individual providing personal data protection services *(if any; enclosed with the service contract):*

No.	Full name	Affiliated organization	Phone number	Email

8.3 Internal personal data protection unit/personnel of the organization *(enclosed with a copy of the decision or document evidencing designation, assignment, and documents proving compliance with the conditions prescribed in Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam)*

Name of unit:

Phone number of unit: Email of unit:

Name of head of unit/Name of personnel: Position:

Mobile phone number: Personal email:

II. CROSS-BORDER PERSONAL DATA TRANSFER ACTIVITIES

1 1.1. Transfer of personal data collected and stored in Vietnam to server systems located outside of the territory of the Socialist Republic of Vietnam ☐

- Name of personal data subject matter: Quantity:

(Specify the types and groups of personal data subject matters, such as clients, employees, applicants, etc., together with the quantity as of the time of dossier submission)

1.2. Storage and processing of personal data on cloud computing services of foreign service providers ☐

- Name of personal data subject matter: Quantity:

....

1.3. Collection of personal data of individuals using services in Vietnam and transfer to platforms outside the territory of the Socialist Republic of Vietnam for further processing ☐

- Name of personal data subject matter: Quantity:

....

1.4. Cross-border transfer of personal data through partners or intermediary agents in Vietnam ☐

- Name of personal data subject matter: Quantity:

....

1.5. Other cases (specify such cases) ☐

- Name of personal data subject matter: Quantity:

....

2 Cross-border personal data transfer flow *(specify personal data subject matters, purposes of transfer, whether sensitive personal data is transferred, and corresponding post-transfer processing activities; model the process flow diagrams and*

	systems for cross-border transfer of personal data)		
3	**Types of personal data processed** Total number of types of basic personal data: Total number of types of sensitive personal data:		
3.1.	**Basic personal data** *(pursuant to Article 3 of Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam; tick √ the prescribed types of personal data)*		
	Surname, middle name, and given name		Contact address
	Alias (if any)		Nationality
	Date of birth		Image of the individual
	Date of death or missing date		Phone number
	Gender;		Personal identification number
	Place of birth		Passport number
	Place of birth registration		Driver's license number
	Place of permanent residence registration		Vehicle license plate number
	Place of temporary residence registration		Marital status
	Current residence		Information on family relationships (parents, children, spouses)
	Place of origin		Information on the individual's digital accounts
	Other information associated with or capable of identifying a specific individual not falling under the above categories		
3.2.	**Sensitive personal data** *(pursuant to Clause 1 Article 3 of Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam; tick √ the prescribed types of personal data)*		
	Data revealing racial origin or ethnic origin		Location data of individuals determined through positioning services
	Political opinions		Login names and passwords for access to individuals' electronic identification accounts
	Religious or belief-related opinions		Images of ID cards, citizen ID cards, 9-digit ID cards
	Information on private life, personal secrets, family secrets		Login names and passwords for access to bank accounts
	Health status		Information on bank cards, data on transaction history of bank accounts
	Biometric data and genetic characteristics		Financial and credit information and other information relating to financial activities and transaction history, securities, and insurance of clients at credit institutions, foreign bank branches, intermediary payment service providers, securities institutions, insurers, and other authorized organizations
	Data revealing sexual life or sexual orientation		Data monitoring behavior and activities related to the use of telecommunications services, social networks, online communication services, and other services in cyberspace

	Data on crimes and legal violations collected and stored by law enforcement agencies		Other personal data required by law to be kept confidential or to which strict confidentiality measures must be applied
4	**Provisions on storage of personal data** *(enclosed with documents evidencing personal data storage policies and regulations)*		
5	**Provisions on deletion and destruction of personal data** *(enclosed with documents evidencing personal data deletion and destruction policies and regulations)*		
6	**Transfer of personal data** *(pursuant to Article 17 of the Law on Personal Data Protection)*		
	Yes ☐ / No: ☐		
	Fee-based transfer of personal data:		
	Yes ☐ / No: ☐		
7	**Participation in transaction activities on data exchanges:**		
	Yes ☐ / No: ☐		
8	**Provision of personal data processing services:**		
	Yes ☐ / No: ☐		
	List of personal data processing services provided by the organization:		
	Services providing and operating automated systems and software to process personal data on behalf of the personal data controlling party or the personal data processing and controlling party		Services for analysis and utilization of personal data, including: using analytical tools to identify information, trends, and patterns from personal data; applying data mining methods to extract value from personal data, predict user behavior, or optimize services
	Services for scoring, rating, and assessing the creditworthiness of the personal data subject matter		Services for encrypting personal data during transmission and storage
	Services for collecting and processing personal data online from websites, applications, software, and social networks		Services for automated personal data processing based on big data technology, artificial intelligence, blockchain, and the metaverse
	Services for collecting and processing personal data through websites, applications, and software for health care and health monitoring, as well as healthcare services		Platform application services providing personal location data
	Services for collecting and processing personal data through educational applications and software with supervision elements such as attendance tracking, video recording, behavior scoring, and emotion recognition		
9	**Personal data protection measures**		
9.1	**Personal data safety assurance plan** *(specify the plans currently implemented to ensure personal data safety)*		
9.2	**Personal data protection measures** *(specify the technical measures, managerial measures, and training measures implemented; application of standards related to personal data protection; system design diagrams and corresponding protection measures)*		
9.3	**Inspection and assessment of cybersecurity and safety of information systems, equipment, and devices for personal data protection** *(specify contents, subjects, frequency, and purposes)*		
9.4	**Personal data safety assurance plan of the cross-border personal data receiving party**		

10	**Assessment of compliance with personal data protection regulations** *(specify the form, time, and results of the compliance assessment)*
III	**CROSS-BORDER PERSONAL DATA TRANSFER IMPACT ASSESSMENT**
1	**General assessment of the situation and business activities related to cross-border transfer of personal data** *(specify the necessity of cross-border personal data transfer activities within the organization's field of operation; the current status of the organization's personal data processing, including advantages, difficulties, and risks in cross-border personal data transfer)*
2	**Assessment of impacts of cross-border personal data transfer** *(assess each specific content and analyze each issue, including description of the current situation, requirement analysis, anticipated scenarios, causes, and solutions; assess the impacts (positive and negative) of proposed solutions; provide recommendations based on comparison of positive and negative impacts. Impacts shall be assessed using quantitative and qualitative methods, clearly stating potential consequences and unintended damage that may occur, as well as measures to mitigate or eliminate such risks and harm.)*
2.1.	**Impact on personal data subject matter:** assessed based on analysis of the potential direct impacts of personal data processing on the rights and interests of the personal data subject matter
	1. Identification of impacted aspects and issues
	2. Issue settlement objectives
	3. Personal data protection measures already applied and proposed to settle the issues
	4. Assessment of the effectiveness and impacts of the measures on directly affected subjects and other relevant subjects
	5. Recommendation of selected personal data protection measures
2.2	**Impact on the organization's information system security and safety:** assessed based on the potential direct influence of personal data processing activities on the confidentiality, integrity, and availability of the information system. The assessment focuses on factors related to the risks of data leakage, unauthorized access, unauthorized modification of data, system operation disruption, the adequacy of existing technical measures, and the potential emergence of security vulnerabilities during data processing**.**
	1. Identification of impacted aspects and issues
	2. Issue settlement objectives
	3. Personal data protection measures already applied and proposed to settle the issues
	4. Assessment of the effectiveness and impacts of the measures on directly affected subjects and other relevant subjects
	5. Recommendation of selected personal data protection measures
2.3	**Impact on national security and social order and safety:** assessed in cases involving processing and transfer of basic personal data of more than 100.000 personal data subject matters or sensitive personal data of more than 10.000 personal data subject matters. The assessment focuses on factors related to large-scale cross-border personal data transfers that may affect national security, social order and safety, and corresponding personal data protection measures.
	1. Identification of impacted aspects and issues
	2. Issue settlement objectives
	3. Personal data protection measures already applied and proposed to settle the issues
	4. Assessment of the effectiveness and impacts of the measures on directly affected subjects and other relevant subjects
	5. Recommendation of selected personal data protection measures
3	**Assessment of the level of personal data protection of the personal data receiving party**
3.1	**Methods of personal data processing and storage of the personal data receiving party** *(specify the method for each data processing flow)*

3.2	**Personal data safety assurance plan of the personal data receiving party** *(specify the plans currently implemented to ensure personal data safety)*
3.3	**Personal data protection measures of the personal data receiving party** *(specify the technical measures, managerial measures, and training measures implemented; application of standards related to personal data protection)*
3.4	**Assessment of processing and storage methods, assurance plans, and personal data protection measures of the personal data receiving party** *(assess the adequacy, appropriateness, and effectiveness of processing methods, personal data safety assurance plans, and personal data protection measures implemented; the level of compliance with personal data protection requirements under Vietnamese law; the capacity to prevent, detect, and respond to risks and personal data breach incidents; identify remaining risks and propose additional or remedial measures, if any)*
IV	**APPENDICES** *(List of names of enclosed documents, policies, procedures, regulations, and forms enclosed with this declaration dossier)*

PART B. INFORMATION ON RELATED PARTIES IN CROSS-BORDER PERSONAL DATA TRANSFER ACTIVITIES

I. INFORMATION ON THE PARTY ACTING ON BEHALF OF THE TRANSFERRING PARTY TO CARRY OUT CROSS-BORDER PERSONAL DATA TRANSFER *(To be declared in cases where an agreement allows another party to transfer personal data across borders directly)*

No.	Name of organization/individual	Tax identification number	Information on personal data protection unit/personnel	Contract/Agreement on cross-border personal data transfer (Number, date)	Cooperation services	Remarks *(Reasons, explanatory contents)*

II. INFORMATION ON THE CROSS-BORDER PERSONAL DATA RECEIVING PARTY *(To be declared in accordance with the relationship in the activities of transferring and receiving personal data)*

No.	Name of organization/individual	Tax identification number	Information on personal data protection unit/personnel	Contract/Agreement on cross-border personal data transfer *(Number, date)*	Cooperation services	Remarks *(Reasons, explanatory contents)*

III. INFORMATION ON OTHER PARTIES *(Other parties involved in cross-border personal data transfer activities)*

No.	Name of organization/individual	Tax identification number	Information on personal data protection unit/personnel	Relevant contract/agreement *(Number, date)*	Cooperation services	Remarks *(Reasons, explanatory contents)*

Form No. 10

DOSSIER
FOR PERSONAL DATA PROCESSING IMPACT ASSESSMENT

PART A. DOSSIER FOR PERSONAL DATA PROCESSING IMPACT ASSESSMENT OF THE SUBMITTING PARTY

I. BASIC INFORMATION ON THE SUBMITTING PARTY

1	Name of organization/individual *(Vietnamese):*	1a	Name of organization/individual *(foreign language):*
1b	Abbreviated name of organization/individual:	1c	Tax identification number:
2	Address *(headquarters):*		
3	Phone number:		
4	Business lines involving personal data processing *(enclosed with corresponding business line registration codes):*		
5	Number of branches, representative offices:		
6	Email:		
7	Website:		
8	**Personal data protection unit/personnel of the organization or individual**		
8.1	**Organization providing personal data protection services** *(if any; enclosed with the service contract):*		
	Name of organization: Tax identification number: Legal representative: Address: Phone number: Email: Website:		

8.2 **Individual providing personal data protection services** *(if any; enclosed with the service contract):*

No.	Full name	Affiliated organization	Phone number	Email

8.3 **Internal personal data protection unit/personnel of the organization** *(enclosed with a copy of the decision or document evidencing designation or assignment)*

Name of unit:

Phone number of unit: Email of unit:

Name of head of unit/Name of personnel: Position:

	Mobile phone number: Personal email:
II.	**PERSONAL DATA PROCESSING ACTIVITIES**
1	**Identification of the personal data processing role of the declaring party** **1.1. Personal data controlling party, Personal data processing and controlling party ☐** - Name of personal data subject matter: Quantity: - Name of personal data subject matter: Quantity: *(Specify the types of personal data subject matters, such as clients, employees, applicants, etc., together with the quantity as of the time of dossier submission)* **1.2. Personal data processing party** - Name of personal data subject matter: Quantity: -Name of personal data subject matter: Quantity: **1.3. Third party** - Name of personal data subject matter: Quantity: -Name of personal data subject matter: Quantity:
2	**Role-based personal data processing flow** *(specify personal data subject matters, processing purposes, types of basic personal data/sensitive personal data processed, and corresponding processing activities; model the process flow diagrams and systems for personal data processing)* 1.1. Personal data controlling party, Personal data processing and controlling party 1.2. Personal data processing party 1.3. Third party
3	**Types of personal data processed** Total number of types of basic personal data:

	Total number of types of sensitive personal data:		
3.1.	**Basic personal data** *(pursuant to Article 3 of Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam; tick √ the prescribed types of personal data)*		
	Surname, middle name, and given name		Contact address
	Alias (if any)		Nationality
	Date of birth		Image of the individual
	Date of death or missing date		Phone number
	Gender;		Personal identification number
	Place of birth		Passport number
	Place of birth registration		Driver's license number
	Place of permanent residence registration		Vehicle license plate number
	Place of temporary residence registration		Marital status
	Current residence		Information on family relationships (parents, children, spouses)
	Place of origin		Information on the individual's digital accounts
	Other information associated with or capable of identifying a specific individual not falling under the above categories		
3.2.	**Sensitive personal data** *(pursuant to Clause 1 Article 3 of Decree No. 356/2025/ND-CP dated December 31, 2025 of the Government of Vietnam; tick √ the prescribed types of personal data)*		
	Data revealing racial origin or ethnic origin		Location data of individuals determined through positioning services
	Political opinions		Login names and passwords for access to individuals' electronic identification accounts
	Religious or belief-related opinions		Images of ID cards, citizen ID cards, 9-digit ID cards
	Information on private life, personal secrets, family secrets		Login names and passwords for access to bank accounts
	Health status		Information on bank cards, data on transaction history of bank accounts
	Biometric data and genetic characteristics		Financial and credit information and other information relating to

			financial activities and transaction history, securities, and insurance of clients at credit institutions, foreign bank branches, intermediary payment service providers, securities institutions, insurers, and other authorized organizations
	Data revealing sexual life or sexual orientation		Data monitoring behavior and activities related to the use of telecommunications services, social networks, online communication services, and other services in cyberspace
	Data on crimes and legal violations collected and stored by law enforcement agencies		Location data of individuals determined through positioning services
	Data revealing racial origin or ethnic origin		Other personal data required by law to be kept confidential or to which strict confidentiality measures must be applied
4	**Consent of personal data subject matters** *(detailed description of contents, forms, and procedures for obtaining consent from each personal data subject matter, enclosed with relevant forms)*		
5	**Provisions on storage of personal data (***enclosed with documents evidencing personal data storage policies and regulations)*		
6	**Provisions on deletion and destruction of personal data** *(enclosed with documents evidencing personal data deletion and destruction policies and regulations)*		
7	**Transfer of personal data** *(pursuant to Article 17 of the Law on Personal Data Protection)*		
	Yes ☐ / No: ☐		
	Fee-based transfer of personal data:		
	Yes ☐ / No: ☐		
8	**Participation in transaction activities on data exchanges:**		
	Yes ☐ / No: ☐		
9	**Provision of personal data processing services:**		

	Yes ☐ / No: ☐		
	List of personal data processing services provided by the organization:		
	Services providing and operating automated systems and software to process personal data on behalf of the personal data controlling party or the personal data processing and controlling party		Services for analysis and utilization of personal data, including: using analytical tools to identify information, trends, and patterns from personal data; applying data mining methods to extract value from personal data, predict user behavior, or optimize services
	Services for scoring, rating, and assessing the creditworthiness of the personal data subject matter		Services for encrypting personal data during transmission and storage
	Services for collecting and processing personal data online from websites, applications, software, and social networks		Services for automated personal data processing based on big data technology, artificial intelligence, blockchain, and the metaverse
	Services for collecting and processing personal data through websites, applications, and software for health care and health monitoring, as well as healthcare services		Platform application services providing personal location data
	Services for collecting and processing personal data through educational applications and software with supervision elements such as attendance tracking, video recording, behavior scoring, and emotion recognition		
10	**Cross-border personal data transfer**		
	Yes ☐ / No: ☐		
11	**Personal data protection measures**		
11.1	**Personal data safety assurance plan** *(specify the plans currently implemented to ensure personal data safety)*		
11.2	**Personal data protection measures** *(specify the technical measures, managerial measures, and training measures implemented; application of standards related to personal data protection; system design diagrams and corresponding protection measures)*		
11.3	***Inspection and assessment of cybersecurity and safety of information systems, equipment, and devices for personal data protection*** *(specify contents, subjects, frequency, and*		

	purposes)
12	**Assessment of compliance with personal data protection regulations** *(specify the form, time, and results of the compliance assessment)*
III	**PERSONAL DATA PROCESSING IMPACT ASSESSMENT**
1	**General assessment of the situation and business activities related to the collection and processing of personal data** *(specify the necessity of personal data processing activities within the organization's field of operation; the current status of the organization's personal data processing, including advantages, difficulties, and risks in personal data processing)*
2	**Assessment of impacts of personal data processing** *(assess each specific content and analyze each issue, including description of the current situation, requirement analysis, anticipated scenarios, causes, and solutions; assess the impacts (positive and negative) of proposed solutions; provide recommendations based on comparison of positive and negative impacts. Impacts shall be assessed using quantitative and qualitative methods, clearly stating potential consequences and unintended damage that may occur, as well as measures to mitigate or eliminate such risks and harm.)*
2.1.	**Impact on personal data subject matter:** assessed based on analysis of the potential direct impacts of personal data processing on the rights and interests of the personal data subject matter
	1. Identification of impacted aspects and issues
	2. Issue settlement objectives
	3. Personal data protection measures already applied and proposed to settle the issues
	4. Assessment of the effectiveness and impacts of the measures on directly affected subjects and other relevant subjects
	5. Recommendation of selected personal data protection measures
2.2	**Impact on the organization's information system security and safety:** assessed based on the potential direct influence of personal data processing activities on the confidentiality, integrity, and availability of the information system. The assessment focuses on factors related to the risks of data leakage, unauthorized access, unauthorized modification of data, system operation disruption, the adequacy of existing technical measures, and the potential emergence of security vulnerabilities during data processing.
	1. Identification of impacted aspects and issues
	2. Issue settlement objectives
	3. Personal data protection measures already applied and proposed to settle the issues
	4. Assessment of the effectiveness and impacts of the measures on directly affected subjects and other relevant subjects

	5. Recommendation of selected personal data protection measures
2.3	**Impact on national security and social order and safety:** assessed in cases involving the processing of basic personal data of more than 100.000 personal data subject matters or sensitive personal data of more than 10.000 personal data subject matters. The assessment focuses on factors related to large-scale personal data processing that may affect national security, social order and safety, and corresponding personal data protection measures.
	1. Identification of impacted aspects and issues
	2. Issue settlement objectives
	3. Personal data protection measures already applied and proposed to settle the issues
	4. Assessment of the effectiveness and impacts of the measures on directly affected subjects and other relevant subjects
	5. Recommendation of selected personal data protection measures
IV	**APPENDICES** *(List of names of enclosed documents, policies, procedures, regulations, and forms enclosed with this declaration dossier)*

PART B. INFORMATION ON RELATED PARTIES IN PERSONAL DATA PROCESSING ACTIVITIES

I. INFORMATION ON THE PERSONAL DATA CONTROLLING PARTY *(To be declared in accordance with the relationship in the activities of processing personal data)*

No.	**Name of organization/individual**	**Tax identification number**	**Information on personal data protection unit/personnel**	**Personal data processing contract/agreement** *(Number, date)*	**Cooperation services**	**Remarks** *(Reasons, explanatory contents)*

II. INFORMATION ON THE PERSONAL DATA PROCESSING PARTY *(To be declared in accordance with the relationship in the activities of processing personal data)*

No.	**Name of organization/individual**	**Tax identification number**	**Information on personal data protection unit/personnel**	**Personal data processing contract/agreement** *(Number, date)*	**Cooperation services**	**Remarks** *(Reasons, explanatory contents)*

III. INFORMATION ON THIRD PARTIES *(To be declared in accordance with the relationship in the activities of processing personal data)*

No.	Name of organization/individual	Tax identification number	Information on personal data protection unit/personnel	Personal data processing contract/agreement *(Number, date)*	Cooperation services	Remarks *(Reasons, explanatory contents)*