GOVERNMENT --------	SOCIALIST REPUBLIC OF VIETNAM Independence - Freedom - Happiness ----------
No: 13/2023/ND-CP	*Hanoi, April 17, 2023*

DECREE

PROTECTION OF PERSONAL DATA

Pursuant to the Law on Government Organization dated June 19, 2015; Law amending and supplementing a number of articles of the Law on Government Organization and the Law on Local Government Organization dated November 22, 2019;

Pursuant to the Civil Code dated November 24, 2015;

Pursuant to the Law on National Security dated December 3, 2004;

Pursuant to the Law on Cyber Security dated June 12, 2018;

At the request of the Minister of Public Security;

The Government promulgates the Decree on personal data protection.

Chapter I

GENERAL PROVISIONS

Article 1. Scope of regulation and subjects of application

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

2. This Decree applies to:

a) Vietnamese agencies, organizations and individuals;

b) Foreign agencies, organizations and individuals in Vietnam;

c) Vietnamese agencies, organizations and individuals operating abroad;

d) Foreign agencies, organizations, and individuals directly participating in or related to personal data processing activities in Vietnam.

Article 2. Explanation of terms

In this Decree, the following terms are understood as follows:

1. Personal data is information in the form of symbols, letters, numbers, images, sounds or similar forms in the electronic environment that is associated with a specific person or helps identify a specific person. can. Personal data includes basic personal data and sensitive personal data.

2. Information that helps identify a specific person is information formed from an individual's activities that, when combined with other stored data and information, can identify a specific person.

3. Basic personal data includes:

a) Surname, middle name, birth name, other names (if any);

b) Date, month and year of birth; date, month, year of death or disappearance;

c) Gender;

d) Place of birth, place of birth registration, permanent residence, temporary residence, current residence, hometown, contact address;

d) Nationality;

e) Image of the individual;

g) Phone number, ID card number, personal identification number, passport number, driver's license number, license plate number, personal tax code number, social insurance number, insurance card number medical;

h) Marital status;

i) Information about family relationships (parents, children);

k) Information about individuals' digital accounts; Personal data reflecting activities and history of activities in cyberspace;

l) Other information associated with a specific person or helping to identify a specific person that is not specified in Clause 4 of this Article.

4. Sensitive personal data is personal data associated with an individual's privacy rights that, when violated, will directly affect the individual's legitimate rights and interests, including:

a) Political opinions, religious opinions;

b) Health status and private life recorded in medical records, excluding information about blood type;

c) Information related to racial origin and ethnic origin;

d) Information about inherited or acquired genetic characteristics of individuals;

d) Information about the individual's physical attributes and biological characteristics;

e) Information about the individual's sex life and sexual orientation;

g) Data on crimes and criminal acts collected and stored by law enforcement agencies;

h) Customer information of credit institutions, foreign bank branches, payment intermediary service providers, and other licensed organizations, including: customer identification information according to the provisions of law law, account information, deposit information, deposited assets information, transaction information, information about organizations and individuals that are guarantors at credit institutions, bank branches, organizations providing intermediary payment services;

i) Data on the individual's location determined through location services;

k) Other personal data specified by law are special and require necessary security measures.

5. Personal data protection is the activity of preventing, detecting, stopping, and handling violations related to personal data according to the provisions of law.

6. Data subject is the individual to whom the personal data reflects.

7. Personal data processing is one or more activities affecting personal data, such as: collection, recording, analysis, confirmation, storage, editing, disclosure, combination, access, retrieve, retrieve, encrypt, decrypt, copy, share, transmit, provide, transfer, delete, destroy personal data or other related actions.

8. The consent of the data subject is the clear, voluntary, affirmative expression of permission to process the data subject's personal data.

9. Personal Data Controller is the organization or individual that decides the purposes and means of processing personal data.

10. Personal Data Processor is an organization or individual that processes data on behalf of the Data Controller, through a contract or agreement with the Data Controller.

11. Controller and processor of personal data is the organization or individual that simultaneously decides the purpose, means and directly processes personal data.

12. Third party is an organization or individual other than the Data Subject, Personal Data Controller, Personal Data Processor, Personal Data Controller and Processor that is allowed to process personal data core.

13. Automatic personal data processing is a form of personal data processing carried out by electronic means to evaluate, analyze and predict the activities of a specific person, such as: habits, interests, trust levels, behavior, location, trends, abilities, and other circumstances.

14. Transferring personal data abroad is the activity of using cyberspace, equipment, electronic means or other forms to transfer personal data of Vietnamese citizens to a location outside the territory of Vietnam. Socialist Republic of Vietnam or use a location outside the territory of the Socialist Republic of Vietnam to process personal data of Vietnamese citizens, including:

a) Organizations, businesses, and individuals transfer personal data of Vietnamese citizens to organizations, businesses, and management departments abroad for processing in accordance with the purposes agreed by the data subject ;

b) Processing of personal data of Vietnamese citizens by automated systems located outside the territory of the Socialist Republic of Vietnam by the Personal Data Controller, the Data Controller and Processor individual, the Party Processes personal data in accordance with the purpose agreed to by the data subject.

Article 3. Principles of personal data protection

1. Personal data is processed in accordance with the law.

2. Data subjects are informed about activities related to the processing of their personal data, unless otherwise provided by law.

3. Personal data will only be processed for the purposes registered and declared by the Personal Data Controller, Personal Data Processor, Personal Data Controller and Processor, Third Party. Statement on processing of personal data.

4. Personal data collected must be appropriate and limited to the scope and purpose to be processed. Personal data may not be bought or sold in any form, unless otherwise prescribed by law.

5. Personal data is updated and supplemented in accordance with the processing purpose.

6. Personal data is subject to protection and security measures during processing, including protection against violations of regulations on personal data protection and prevention of loss. loss, destruction or damage due to incidents, using technical measures.

7. Personal data is only stored for a period of time consistent with the purpose of data processing, unless otherwise prescribed by law.

8. The Data Controller, the Controller and Processor of personal data is responsible for complying with the data processing principles set forth in Clauses 1 to 7 of this Article and demonstrating their compliance with those data processing principles.

Article 4. Handling violations of personal data protection regulations

Agencies, organizations and individuals that violate personal data protection regulations, depending on the severity, may be disciplined, administratively sanctioned, or criminally handled according to regulations.

Article 5. State management of personal data protection

The Government unifies state management of personal data protection.

The content of state management of personal data protection includes:

1. Submit to competent state agencies for promulgation or promulgate according to authority legal documents and direct and organize the implementation of legal documents on personal data protection.

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

3. Guide agencies, organizations and individuals on measures, processes and standards to protect personal data according to the provisions of law.

4. Propagate and educate about laws on personal data protection; communicate and disseminate knowledge and skills to protect personal data.

5. Develop, train and foster cadres, civil servants, public employees and people assigned to protect personal data.

6. Inspect and examine the implementation of legal regulations on personal data protection; Resolve complaints, denunciations and handle violations of the law on personal data protection according to the provisions of law.

7. Statistics, information, and reports on the situation of personal data protection and the implementation of laws on personal data protection to competent state agencies.

8. International cooperation on personal data protection.

Article 6. Application of the Personal Data Protection Decree, relevant laws and international treaties

The protection of personal data is carried out in accordance with the provisions of international treaties to which the Socialist Republic of Vietnam is a member, other provisions of relevant Laws and this Decree.

Article 7. International cooperation on personal data protection

1. Develop an international cooperation mechanism to facilitate the effective enforcement of laws on personal data protection.

2. Participate in mutual legal assistance on personal data protection of other countries, including notifications, requests for complaints, investigative assistance and exchange of information, with appropriate safeguards to protect personal data.

3. Organize conferences, seminars, scientific research and promote international cooperation activities in law enforcement to protect personal data.

4. Organize bilateral and multilateral meetings, exchange experiences in developing laws and practices to protect personal data.

5. Technology transfer to protect personal data.

Article 8. Prohibited acts

1. Processing personal data contrary to the provisions of law on personal data protection.

2. Processing personal data to create information and data aimed against the State of the Socialist Republic of Vietnam.

3. Processing personal data to create information and data that affects national security, social order and safety, and the legitimate rights and interests of other organizations and individuals.

4. Obstructing personal data protection activities of competent authorities.

5. Taking advantage of personal data protection activities to violate the law.

chapter II

PERSONAL DATA PROTECTION ACTIVITIES

Section 1. RIGHTS AND OBLIGATIONS OF DATA SUBJECTS

Article 9. Rights of data subjects

1. Right to know

Data subjects are informed about the processing of their personal data, unless otherwise provided by law.

2. Right to consent

The data subject may or may not agree to the processing of his or her personal data, except for the cases specified in Article 17 of this Decree .

3. Access rights

Data subjects have access to view, edit or request correction of their personal data, unless otherwise provided by law.

4. Right to withdraw consent

The data subject has the right to withdraw his or her consent, unless otherwise provided by law.

5. Right to data deletion

The data subject has the right to erase or request the deletion of his or her personal data, unless otherwise provided by law.

6. Right to restrict data processing

a) Data subjects are requested to restrict the processing of their personal data, unless otherwise provided by law;

b) Restriction of data processing is carried out within 72 hours after the data subject's request, with all personal data that the data subject requests to be restricted, unless otherwise required by law. other.

7. Right to provide data

The data subject may request the Personal Data Controller, the Personal Data Controller and Processor to provide himself/herself with his/her personal data, unless otherwise provided by law.

8. Right to object to data processing

a) The data subject has the right to object to the Personal Data Controller, the Personal Data Controller and Processor processing his or her personal data in order to prevent or limit the disclosure or use of personal data. for advertising and marketing purposes, unless otherwise provided by law;

b) The Personal Data Controller, the Personal Data Controller and Processor shall carry out the data subject's request within 72 hours after receiving the request, unless otherwise provided by law.

9. Right to complain, denounce and sue

Data subjects have the right to complain, denounce or sue in accordance with the law.

10. Right to claim compensation for damages

Data subjects have the right to request compensation for damages according to the provisions of law when violations of regulations on protecting their personal data occur, unless the parties agree otherwise or the law provides otherwise. .

11. Right to self-defense

Data subjects have the right to self-protect according to the provisions of the Civil Code , other relevant laws and this Decree, or request competent agencies and organizations to implement civil rights protection methods according to stipulated in Article 11 of the Civil Code .

Article 10. Obligations of data subjects

1. Protect your personal data; Request other relevant organizations and individuals to protect their personal data.

2. Respect and protect the personal data of others.

3. Provide complete and accurate personal data when agreeing to process personal data.

4. Participate in propagating and disseminating personal data protection skills.

5. Implement legal regulations on personal data protection and participate in preventing and combating violations of personal data protection regulations.

Section 2. PROTECTION OF PERSONAL DATA DURING THE PROCESSING OF PERSONAL DATA

Article 11. Consent of the data subject

1. The consent of the data subject applies to all activities in the processing of personal data, unless otherwise provided by law.

2. The data subject's consent is only valid when the data subject voluntarily and clearly knows the following contents:

a) Type of personal data processed;

b) Purpose of processing personal data;

c) Organizations and individuals allowed to process personal data;

d) Rights and obligations of data subjects.

3. The consent of the data subject must be expressed clearly and specifically in writing, voice, checking the consent box, text consent syntax, selecting consent technical settings or through another action that demonstrates this.

4. The consent must be given for the same purpose. When there are multiple purposes, the Personal Data Controller, Personal Data Controller and Processor lists the purposes so that the data subject agrees to one or more of the stated purposes.

5. The data subject's consent must be expressed in a format that can be printed, reproduced in writing, including in electronic or verifiable format.

6. Silence or non-response of the data subject is not considered consent.

7. The data subject may give partial or conditional consent.

8. For the processing of sensitive personal data, the data subject must be informed that the data to be processed is sensitive personal data.

9. The data subject's consent is valid until the data subject decides otherwise or when a competent state agency requests it in writing.

10. In case of dispute, the responsibility of proving the consent of the data subject lies with the Personal Data Controller, the Party that controls and processes the personal data.

11. Through authorization according to the provisions of the Civil Code , organizations and individuals can, on behalf of the data subject, carry out procedures related to the processing of the data subject's personal data with the Party. Controller of personal data, the Controller processes and processes personal data in cases where the data subject has clearly known and consented in accordance with the provisions of Clause 3 of this Article, unless otherwise provided by law.

Article 12. Withdrawal of consent

1. Withdrawal of consent does not affect the lawfulness of data processing consented to before the withdrawal of consent.

2. The withdrawal of consent must be expressed in a format that can be printed, reproduced in writing, including in electronic or verifiable format.

3. Upon receiving the data subject's request to withdraw consent, the Personal Data Controller and the Personal Data Controller and Processor notify the data subject of the possible consequences and damages. occurs when consent is withdrawn.

4. After implementing the provisions in Clause 2 of this Article, the Data Controller, Data Processor, Data Controller and Processor, Third Party must stop and request organizations and individuals to concerned to stop processing the data of the data subject who has withdrawn consent.

Article 13. Notice of processing of personal data

1. Notification is done once before proceeding with personal data processing activities.

2. Content of notification to data subjects about personal data processing:

a) Processing purpose;

b) The type of personal data used is related to the processing purposes specified in Point a, Clause 2 of this Article;

c) How to handle;

d) Information about other organizations and individuals related to the processing purposes specified in Point a, Clause 2 of this Article;

d) Unwanted consequences and damages are likely to occur;

e) Start time and end time of data processing.

3. The notification to the data subject must be in a format that can be printed, reproduced in writing, including in electronic or verifiable format.

4. The Personal Data Controller and the Personal Data Controller and Processor do not need to comply with the provisions of Clause 1 of this Article in the following cases:

a) The data subject has clearly known and fully agreed to the content specified in Clauses 1 and 2 of this Article before giving consent to the personal data controller and the personal data processing party. collect personal data, in accordance with the provisions of Article 9 of this Decree ;

b) Personal data is processed by competent state agencies for the purpose of serving the activities of state agencies in accordance with the provisions of law.

Article 14. Providing personal data

1. The data subject shall request the Personal Data Controller, the Personal Data Controller and Processor to provide himself/herself with his/her personal data.

2. Personal Data Controller, Personal Data Controller and Processing Party:

a) Provide personal data of the data subject to other organizations and individuals with the consent of the data subject, unless otherwise prescribed by law;

b) On behalf of the data subject, provide the data subject's personal data to another organization or individual when the data subject agrees to allow representation and authorization, unless otherwise prescribed by law. .

3. The provision of personal data of the data subject is carried out by the Personal Data Controller, the Personal Data Controller and Processor within 72 hours after the data subject's request, except in cases where the law provides otherwise.

4. Personal Data Controller, Personal Data Controller and Processor does not provide personal data in the case of:

a) Causing harm to national defense, national security, social order and safety;

b) Providing personal data of the data subject may affect the safety, physical or mental health of others;

c) The data subject does not agree to provide, allow representation or authorization to receive personal data.

5. Form of request to provide personal data:

a) The data subject directly or authorizes another person to go to the headquarters of the Personal Data Controller, the Personal Data Controller and Processor to request personal data.

The person receiving the request is responsible for guiding the requesting organization or individual to fill out the contents of the Request to Provide Personal Data Form.

In case the organization or individual requesting information is illiterate or has a disability and is unable to write the request, the person receiving the request for information is responsible for helping fill out the contents of the Data Request Form. personal data;

b) Send a request to provide personal data according to Form No. 01 , 02 in the Appendix to this Decree via electronic network, postal service, fax to the Personal Data Controller, the Controller and Processing Party. personal data management.

6. The request to provide personal data must be expressed in Vietnamese and include the following main contents:

a) Full name; place of residence, address; ID card number, citizen identification card or passport number of the requester; fax number, phone number, email address (if any);

b) Personal data requested to be provided, clearly indicating the name of the document, profile, or document;

c) Form of providing personal data;

d) Reason and purpose of request to provide personal data.

7. In case of request to provide personal data specified in Clause 2 of this Article, it must be accompanied by written consent of the individual or organization concerned.

8. Receive requests for personal data

a) The Personal Data Controller and the Personal Data Controller and Processor are responsible for receiving requests to provide personal data and monitoring the process and list of personal data provision as requested. ;

b) In case the personal data requested is not within its jurisdiction, the Personal Data Controller and the Personal Data Controller and Processor receiving the request must notify and guide the requesting organization or individual. request to the competent authority or clearly notify the inability to provide personal data.

9. Resolve requests to provide personal data

Upon receiving a valid request to provide personal data, the Personal Data Controller, the Personal Data Controller and Processor shall be responsible for providing personal data with notice of the time limit,

location, form of personal data provision; Actual costs for printing, copying, photocopying, sending information via postal and fax services (if any) and payment method and deadline; Provide personal data according to the order and procedures specified in this Article.

Article 15. Correction of personal data

1. Data subject:

a) Have access to view and edit your personal data after it has been collected by the Personal Data Controller, the Personal Data Controller and Processor according to your consent, unless otherwise provided by law. other rule;

b) In case direct editing is not possible for technical or other reasons, the data subject requests the Personal Data Controller, the Personal Data Controller and Processor to edit the personal data. his cause.

2. The Personal Data Controller, the Personal Data Controller and Processor edits the personal data of the data subject after obtaining the consent of the personal data subject as soon as possible or in accordance with regulations of specialized law. In case this cannot be done, notify the data subject 72 hours after receiving the data subject's request to edit personal data.

3. The Personal Data Processor, the Third Party may edit the personal data of the data subject after receiving written consent from the Personal Data Controller, the Personal Data Controller and Processor. copy and knowing that the consent of the data subject has been obtained.

Article 16. Storage, deletion, destruction of personal data

1. The data subject may request the Personal Data Controller, the Personal Data Controller and Processor to delete his or her personal data in the following cases:

a) Realizing that it is no longer necessary for the agreed collection purpose and accepting possible damages when requesting data deletion;

b) Withdraw consent;

c) Object to the processing of data and the Controller of personal data, the Controller and processor of personal data do not have a legitimate reason to continue processing;

d) Personal data is not processed for the agreed purpose or the processing of personal data is in violation of the law;

d) Personal data must be deleted according to the provisions of law.

2. Data deletion will not apply upon request of the data subject in the following cases:

a) The law does not allow data deletion;

b) Personal data is processed by a competent state agency for the purpose of serving the operations of the state agency in accordance with the provisions of law;

c) Personal data has been made public in accordance with the law;

d) Personal data is processed to serve legal requirements, scientific research, and statistics in accordance with the law;

d) In case of emergency regarding national defense, national security, social order and safety, major disasters, dangerous epidemics; when there is a threat to security and national defense but not to the extent

of declaring a state of emergency; preventing and combating riots, terrorism, preventing and combating crime and law violations;

e) Respond to emergency situations that threaten the life, health or safety of data subjects or other individuals.

3. In case an enterprise divides, splits, merges, consolidates, or dissolves, personal data is transferred according to the provisions of law.

4. In case of division, separation, merger of agencies, organizations, administrative units and reorganization or conversion of ownership form of state-owned enterprises, personal data is transferred according to the provisions of law.

5. Data deletion is carried out within 72 hours after the data subject's request for all personal data collected by the Personal Data Controller, the Personal Data Controller and Processor. Yes, unless otherwise provided by law.

6. Personal Data Controllers, Personal Data Controllers and Processors, Personal Data Processors, Third Parties store personal data in a form appropriate to their operations and have measures to protect personal data according to the provisions of law.

7. Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, Third Party irreversibly erases in case of:

a) Processing data for improper purposes or having completed the purpose of processing personal data agreed by the data subject;

b) The storage of personal data is no longer necessary for the activities of the Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, Third Party;

c) Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, Third Party is dissolved or no longer operating or declares bankruptcy or is terminated conduct business according to the provisions of law.

Article 17. Processing of personal data in cases where the consent of the data subject is not required

1. In an emergency, it is necessary to immediately process relevant personal data to protect the life and health of the data subject or other people. It is the responsibility of the Personal Data Controller, Personal Data Processor, Personal Data Controller and Processor, Third Party to prove this case.

2. Disclosure of personal data in accordance with the law.

3. Data processing by competent state agencies in case of emergency situations related to national defense, national security, social order and safety, major disasters, dangerous epidemics; when there is a threat to security and national defense but not to the extent of declaring a state of emergency; prevent and combat riots, terrorism, prevent and combat crimes and violations of the law according to the provisions of law.

4. To perform the data subject's contractual obligations with relevant agencies, organizations and individuals according to the provisions of law.

5. Serving the activities of state agencies as prescribed by specialized laws.

Article 18. Processing of personal data obtained from audio and video recording activities in public places

Competent agencies and organizations are allowed to record audio, video and process personal data obtained from audio and video recording activities in public places for the purpose of protecting national security and social order and safety. associations, legitimate rights and interests of organizations and individuals according to the provisions of law without the consent of the subject. When making audio or video recordings, competent agencies and organizations are responsible for notifying the subject so that they understand that they are being audio or video recorded, unless otherwise prescribed by law.

Article 19. Processing personal data of people declared missing or dead

1. The processing of personal data related to the personal data of a person declared missing or deceased must have the consent of that person's spouse or adult children, in the absence of such persons. For this purpose, the consent of the father or mother of the person declared missing or deceased must be obtained, except for the cases specified in Article 17 and Article 18 of this Decree .

2. If all the people mentioned in Clause 1 of this Article are not present, it is considered that there is no consent.

Article 20. Processing of children's personal data

1. Processing of children's personal data is always carried out in accordance with the principle of protecting the rights and in the best interests of children.

2. The processing of children's personal data must have the child's consent in cases where the child is 7 years of age or older and has the consent of the parent or guardian as prescribed, except in cases where in accordance with the provisions of Article 17 of this Decree . Personal Data Controllers, Personal Data Processors, Personal Data Controllers and Processors, Third Parties must verify the age of children before processing their personal data.

3. Stop processing children's personal data, irreversibly delete or destroy children's personal data in the event of:

a) Process data for improper purposes or have completed the purpose of processing personal data agreed to by the data subject, unless otherwise prescribed by law;

b) The child's father, mother or guardian withdraws consent to process the child's personal data, unless otherwise provided by law;

c) At the request of a competent authority when there is sufficient evidence to prove that the processing of personal data affects the legitimate rights and interests of children, unless otherwise prescribed by law. .

Article 21. Protection of personal data in the business of marketing services and introducing advertising products

1. Organizations and individuals providing marketing and advertising product introduction services may only use customers' personal data collected through their business activities to provide marketing and introduction services. recommend advertising products with the consent of the data subject.

2. Processing of customers' personal data to provide marketing services and introduce advertising products must be approved by the customer, on the basis that the customer clearly knows the content, method and form. , frequency of product introduction.

3. Organizations and individuals providing marketing services and introducing advertising products are responsible for proving the use of personal data of customers whose products are introduced in accordance with the provisions of Clauses 1 and 2. This.

Article 22. Illegal collection, transfer, buying and selling of personal data

1. Organizations and individuals involved in processing personal data must apply personal data protection measures to prevent unauthorized collection of personal data from service systems and equipment. his service.

2. Setting up software systems, technical measures or organizing activities to collect, transfer, buy and sell personal data without the consent of the data subject is a violation of the law.

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

1. In case a violation of personal data protection regulations is detected, the Personal Data Controller, the Personal Data Controller and Processor shall notify the Ministry of Public Security (Department of Cyber Security and the Department of Personal Data). , combating crimes using high technology) no later than 72 hours after the violation occurs according to Form No. 03 in the Appendix to this Decree. In case of notification after 72 hours, the reason for late notification must be included.

2. The Personal Data Processor must notify the Personal Data Controller as quickly as possible after becoming aware of a violation of personal data protection regulations.

3. Content of notice of violation of regulations on personal data protection:

a) Describe the nature of the violation of personal data protection regulations, including: time, location, behavior, organization, individual, types of personal data and quantity of data involved ;

b) Contact details of the employee assigned to protect data or the organization or individual responsible for protecting personal data;

c) Describe the possible consequences and damages of violating personal data protection regulations;

d) Describe the measures taken to resolve and minimize the harmful effects of violations of personal data protection regulations.

4. In case it is not possible to fully notify the contents specified in Clause 3 of this Article, the notification may be carried out in batches and stages.

5. The Party that controls personal data and the Party that controls and processes personal data must make a record confirming the occurrence of a violation of personal data protection regulations, in coordination with the Ministry of Public Security (Department of Cyber Security and Crime Prevention using High Technology) handles violations.

6. Organizations and individuals notify the Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention and Control) when detecting the following cases:

a) Detect legal violations against personal data;

b) Personal data is processed for the wrong purpose, not in accordance with the original agreement between the data subject and the Personal Data Controller, the Personal Data Controller and Processor or violates the provisions of law. the law;

c) The data subject's rights are not guaranteed or are not implemented properly;

d) Other cases as prescribed by law.

Section 3. IMPACT ASSESSMENT AND TRANSFER OF PERSONAL DATA OVERSEAS

Article 24. Impact assessment of personal data processing

1. The Personal Data Controller, the Personal Data Controller and Processor shall establish and maintain a Record assessing the impact of processing of their personal data from the time the processing of personal data begins. .

Records assessing the impact of personal data processing by the Personal Data Controller, the Personal Data Controller and Processor, including:

a) Information and contact details of the Personal Data Controller and the Personal Data Controller and Processor;

b) Full name and contact details of the organization assigned to perform the task of protecting personal data and the personal data protection officer of the Personal Data Controller, Data Controller and Processor. personal data;

c) Purpose of processing personal data;

d) Types of personal data processed;

d) Organizations and individuals receiving personal data, including organizations and individuals outside Vietnam;

e) In case of transferring personal data abroad;

g) Personal data processing time; Estimated time to delete or destroy personal data (if any);

h) Description of the personal data protection measures applied;

i) Assess the impact of personal data processing; Unwanted consequences and damage are likely to occur, and measures to minimize or eliminate such risks and harms.

2. The Personal Data Processor shall prepare and maintain a Personal Data Processing Impact Assessment Record in case of performance of a contract with the Personal Data Controller. Records assessing the impact of processing personal data by the Personal Data Processor, including:

a) Information and contact details of the Personal Data Processor;

b) Full name and contact details of the organization assigned to process personal data and the employee processing personal data of the Personal Data Processor;

c) Description of processing activities and types of personal data processed under the contract with the Personal Data Controller;

d) Personal data processing time; Estimated time to delete or destroy personal data (if any);

d) In case of transferring personal data abroad;

e) General description of the personal data protection measures applied;

g) Unwanted consequences and damages that are likely to occur, and measures to minimize or eliminate such risks and harms.

3. Records of impact assessment of personal data processing specified in Clauses 1 and 2 of this Article are established in legally valid documents of the Personal Data Controller, the Controller and Processor. personal data or Personal Data Processor.

4. Records assessing the impact of personal data processing must always be available to serve the inspection and assessment activities of the Ministry of Public Security and sent to the Ministry of Public Security (Department of Cyber Security and Crime Prevention for use). high technology) 01 original copy according to Form No. 04 in the Appendix to this Decree within 60 days from the date of processing personal data.

5. The Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention and Control) evaluates and requests the Personal Data Controller, Personal Data Controller and Processor, and Data Processor Completed personal data Dossier to assess the impact of processing personal data in case the dossier is not complete and in accordance with regulations.

6. The Personal Data Controller, the Personal Data Controller and Processor, and the Personal Data Processor update and supplement the Personal Data Processing Impact Assessment Profile when there are changes about the content of the dossier sent to the Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention and Control) according to Form No. 05 in the Appendix to this Decree.

Article 25. Transfer of personal data abroad

1. Personal data of Vietnamese citizens is transferred abroad in case the Party transferring data abroad prepares a Dossier to assess the impact of transferring personal data abroad and carries out procedures according to regulations. in Clauses 3, 4 and 5 of this Article. Parties transferring data abroad include Personal Data Controllers, Personal Data Processors and Controllers, Personal Data Processors, Third Parties.

2. Documents assessing the impact of transferring personal data abroad, including:

a) Information and contact details of the Data Transferring Party and the Receiving Party of Vietnamese citizens' personal data;

b) Full name and contact details of the organization or individual in charge of the Data Transferring Party related to the transfer and receipt of personal data of Vietnamese citizens;

c) Describe and explain the objectives of the personal data processing activities of Vietnamese Citizens after being transferred abroad;

d) Describe and clarify the type of personal data transferred abroad;

d) Describe and clearly state compliance with personal data protection regulations in this Decree, details of personal data protection measures applied;

e) Assess the impact of personal data processing; Unwanted consequences and damages that are likely to occur, and measures to reduce or eliminate such risks and harms;

g) The consent of the data subject as prescribed in Article 11 of this Decree on the basis of clearly knowing the feedback and complaint mechanism when problems or requests arise;

h) There is a document showing the binding and responsibilities between organizations and individuals transferring and receiving personal data of Vietnamese citizens regarding the processing of personal data.

3. Documents assessing the impact of transferring personal data abroad must always be available to serve the inspection and assessment activities of the Ministry of Public Security.

The party transferring data abroad sends 01 original copy of the dossier to the Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention) according to Form No. 06 in the Appendix to this Decree within 60 days . from the date of processing of personal data.

4. The data transfer party notifies the Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention) with information about the data transfer and contact details of the organization and individual in charge of the transfer. text after the data transfer is successful.

5. The Ministry of Public Security (Department of Cyber Security and High-Tech Crime Prevention and Control) evaluates and requests the Party transferring data abroad to complete the Dossier assessing the impact of transferring personal data abroad. in case the dossier is not complete and in accordance with regulations.

6. The party transferring data abroad updates and supplements the Dossier assessing the impact of transferring personal data abroad when there is a change in the content of the dossier sent to the Ministry of Public Security (Department of Cyber Security and Security). prevention and combat of crimes using high technology) according to Form No. 05 in the Appendix to this Decree. The time to complete the application for the Party transferring data abroad is 10 days from the date of request.

7. Based on the specific situation, the Ministry of Public Security decides to inspect the transfer of personal data abroad once a year, except in cases where violations of the law on personal data protection are detected. individuals in this Decree or allow incidents of exposure or loss of personal data of Vietnamese citizens to occur.

8. The Ministry of Public Security decides to request the Party transferring data abroad to stop transferring personal data abroad in the following cases:

a) When it is discovered that the transferred personal data is used in activities that violate the national interests and security of the Socialist Republic of Vietnam;

b) The party transferring data abroad does not comply with the provisions in Clauses 5 and 6 of this Article;

c) Allowing incidents of exposure or loss of personal data of Vietnamese citizens to occur.

Section 4. MEASURES AND CONDITIONS TO ENSURE THE PROTECTION OF PERSONAL DATA

Article 26. Personal data protection measures

1. Personal data protection measures are applied right from the beginning and throughout the processing of personal data.

2. Personal data protection measures, including:

a) Management measures implemented by organizations and individuals involved in processing personal data;

b) Technical measures implemented by organizations and individuals related to personal data processing;

c) Measures implemented by competent state management agencies according to the provisions of this Decree and relevant laws;

d) Investigation and litigation measures implemented by competent state agencies;

d) Other measures as prescribed by law.

Article 27. Basic personal data protection

1. Apply the measures specified in Clause 2, Article 26 of this Decree .

2. Develop and promulgate regulations on personal data protection, clearly stating what needs to be done according to the provisions of this Decree.

3. Encourage the application of personal data protection standards appropriate to the fields, industries, and activities related to personal data processing.

4. Check network security for systems and means and equipment serving personal data processing before processing, irreversibly deleting or destroying devices containing personal data.

Article 28. Protection of sensitive personal data

1. Apply the measures specified in Clause 2, Article 26 and Article 27 of this Decree .

2. Designate a department with the function of protecting personal data, designate personnel in charge of protecting personal data, and exchange information about the department and individual in charge of protecting personal data with the Agency specializes in protecting personal data. In case the Personal Data Controller, Personal Data Controller and Processor, Data Processor, or Third Party is an individual, the information of the performing individual shall be exchanged.

3. Notify the data subject that the data subject's sensitive personal data is processed, except for the cases specified in Clause 4, Article 13, Article 17 and Article 18 of this Decree .

Article 29. Agency in charge of personal data protection and National Information Portal on personal data protection

1. The agency in charge of protecting personal data is the Department of Cyber Security and High-Tech Crime Prevention - Ministry of Public Security, which is responsible for helping the Ministry of Public Security carry out state management of data protection. personal data.

2. National information portal on personal data protection:

a) Provide information about the Party's guidelines, guidelines and policies, and the State's laws on personal data protection;

b) Propagate and disseminate policies and laws on personal data protection;

c) Update information and personal data protection situation;

d) Receive information, records, and data on personal data protection activities through cyberspace;

d) Provide information on the results of assessment of personal data protection work of relevant agencies, organizations and individuals;

e) Receive notices of violations of regulations on personal data protection;

g) Warn and coordinate warnings about risks and acts of violating personal data according to the provisions of law;

h) Handle violations of personal data protection according to the provisions of law;

i) Carry out other activities according to the provisions of law on personal data protection.

Article 30. Conditions to ensure personal data protection activities

1. Personal data protection force:

a) A specialized force to protect personal data is arranged at the Agency specialized in protecting personal data;

b) Departments and personnel with the function of protecting personal data are designated in agencies, organizations, and enterprises to ensure implementation of regulations on personal data protection;

c) Organizations and individuals are mobilized to participate in protecting personal data;

d) The Ministry of Public Security develops specific programs and plans to develop human resources to protect personal data.

2. Agencies, organizations and individuals are responsible for propagating and disseminating knowledge, skills, and raising awareness of personal data protection for agencies, organizations and individuals.

3. Ensure facilities and operating conditions for the Agency in charge of protecting personal data.

Article 31. Funding to ensure personal data protection activities

1. Financial sources for personal data protection include the state budget; Support from domestic and foreign agencies, organizations and individuals; Revenue from providing personal data protection services; international aid and other legal revenue sources.

2. Funding for personal data protection of state agencies is guaranteed by the state budget, arranged in the annual state budget estimates. The management and use of funds from the state budget is carried out in accordance with the law on state budget.

3. Funds for protecting personal data of organizations and businesses are arranged and implemented by organizations and businesses themselves according to regulations.

Chapter III

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS

Article 32. Responsibilities of the Ministry of Public Security

1. Help the Government unify the implementation of state management on personal data protection.

2. Guide and implement personal data protection activities, protect the rights of data subjects against violations of legal regulations on personal data protection, propose to promulgate Protection Standards Personal data protection and applicable recommendations.

3. Build, manage and operate the National Information Portal on personal data protection.

4. Evaluate the results of personal data protection work of relevant agencies, organizations and individuals.

5. Receive documents, forms, and information on personal data protection according to the provisions of this Decree.

6. Promote measures and conduct research for innovation in the field of personal data protection, and implement international cooperation on personal data protection.

7. Inspect, examine, resolve complaints and denunciations, and handle violations of regulations on personal data protection according to the provisions of law

Article 33. Responsibilities of the Ministry of Information and Communications

1. Direct media agencies, press, organizations and businesses in the field of management to protect personal data according to the provisions of this Decree.

2. Develop, guide and implement measures to protect personal data, ensure network information security for personal data in information and communication activities according to assigned functions and tasks .

3. Coordinate with the Ministry of Public Security in inspecting, examining and handling violations of the law on personal data protection.

Article 34. Responsibilities of the Ministry of National Defense

Manage, inspect, examine, supervise, handle violations and apply personal data protection regulations to agencies, organizations and individuals under the management of the Ministry of National Defense according to regulations legal regulations and assigned functions and tasks.

Article 35. Responsibilities of the Ministry of Science and Technology

1. Coordinate with the Ministry of Public Security in developing Personal Data Protection Standards and recommendations for applying Personal Data Protection Standards.

2. Research and discuss with the Ministry of Public Security on measures to protect personal data to keep up with the development of science and technology.

Article 36. Responsibilities of ministries, ministerial-level agencies, and agencies under the Government

1. Implement state management of personal data protection for management sectors and fields according to the provisions of law on personal data protection.

2. Develop and implement the contents and tasks of personal data protection in this Decree.

3. Supplement regulations on personal data protection in developing and implementing tasks of ministries and branches.

4. Arrange funding for personal data protection activities according to current budget management decentralization.

5. Issue an Open Data List in accordance with personal data protection regulations.

Article 37. Responsibilities of the People's Committees of provinces and centrally run cities

1. Implement state management of personal data protection for management sectors and fields according to the provisions of law on personal data protection.

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

3. Arrange funding for personal data protection activities according to current budget management decentralization.

4. Issue an Open Data List in accordance with personal data protection regulations.

Article 38. Responsibilities of the Personal Data Controller

1. Implement organizational and technical measures and appropriate safety and security measures to prove that data processing activities have been carried out in accordance with the law on personal data protection , review and update these measures when necessary.

2. Record and store system logs of personal data processing.

3. Notify violations of regulations on personal data protection as prescribed in Article 23 of this Decree .

4. Select a Personal Data Processor that is consistent with its clear mandate and only work with a Personal Data Processor that has appropriate safeguards in place.

5. Ensure the rights of data subjects as prescribed in Article 9 of this Decree .

6. The Personal Data Controller is responsible to the data subject for damages caused by the processing of personal data.

7. Coordinate with the Ministry of Public Security and competent state agencies in protecting personal data, providing information to serve the investigation and handling of violations of legal regulations on personal data protection core.

Article 39. Responsibilities of the Party processing personal data

1. Only receive personal data after having a contract or agreement on data processing with the Personal Data Controller.

2. Process personal data in accordance with the contract or agreement signed with the Personal Data Controller.

3. Fully implement personal data protection measures specified in this Decree and other relevant legal documents.

4. The Party processing personal data is responsible to the data subject for damages caused by the processing of personal data.

5. Delete and return all personal data to the Personal Data Controller after finishing processing the data.

6. Coordinate with the Ministry of Public Security and competent state agencies in protecting personal data, providing information to serve the investigation and handling of violations of legal regulations on personal data protection core.

Article 40. Responsibilities of the Controller and Data Processor

Fully implement the regulations on the responsibilities of the Personal Data Controller and the Personal Data Processor.

Article 41. Responsibilities of Third Parties

Fully implement the regulations on personal data processing responsibilities as prescribed in this Decree.

Article 42. Responsibilities of relevant organizations and individuals

1. Have measures to protect your personal data and be responsible for the accuracy of the personal data you provide.

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

3. Timely notify the Ministry of Public Security of violations related to personal data protection activities.

4. Coordinate with the Ministry of Public Security in handling violations related to personal data protection activities.

Chapter IV

TERMS ENFORCEMENT

Article 43. Implementation effect

1. This Decree takes effect from July 1, 2023.

2. Micro-enterprises, small enterprises, medium-sized enterprises, and startups have the right to choose to exempt themselves from regulations on appointing individuals and personal data protection departments during the first 2 years from when establishing a business.

3. Micro-enterprises, small enterprises, medium-sized enterprises, and start-up enterprises directly engaged in personal data processing activities do not apply the provisions of Clause 2 of this Article.

Article 44. Responsibility for implementation

1. The Minister of Public Security urges, inspects and guides the implementation of this Decree.

2. Ministers, Heads of ministerial-level agencies, Heads of Government agencies, Chairmen of People's Committees of provinces and centrally run cities are responsible for implementing this Decree./.

TM. KT GOVERNMENT
. DEPUTY
PRIME MINISTER

Tran Luu Quang

Recipient:
- Party Central Committee Secretariat;
- Prime Minister, Deputy Prime Ministers;
- Ministries, ministerial-level agencies, and agencies under the Government;
- People's Councils and People's Committees of provinces and centrally run cities;
- Central Office and Party Committees;
- Office of the General Secretary;
- Office of the President;
- Nationalities Council and Committees of the National Assembly;
- Congress office;
- People's Procuratorate of the Supreme;
- Supreme People's Court;
- State audit;
- National Financial Supervisory Commission;
- Social Policy Bank;
- Vietnam Development Bank;
- Central Committee of Vietnam Fatherland Front;
- Central agency of unions;
- Office of Government: BTCN, PCNs, Assistant to the President, General Director of the Electronic Information Portal, Departments, Bureaus, affiliated units, Official Gazette;
- Saved: VT, KSTT (2b)

TM.

Appendix

(Attached to Decree No. 13/2023/ND-CP dated April 17, 2023 of the Government)

Model number 01	Personal data request form (for individuals)
Model number 02	Request form to provide personal data (for organizations and businesses)
Model number 03	Notice of violation of regulations on personal data protection
Model number 04	Notice of submission of personal data processing impact assessment records

Model number 05	Notification of changes in profile content
Model number 06	Records assessing the impact of transferring personal data abroad

Model number 01

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

....., day month Year.....

REQUEST FOR PERSONAL DATA

(For individuals)

Dear:..... ...

1. Full name of individual requesting personal data:..... .....

....

2. Representative/Guardian [1] :..... .....

3. ID card number/Citizen identification card/Passport..... .....

Issued on...../...../..... at..... ....

4. Place of residence [2] :..... ....

5. Phone number [3] .....; Fax.....; Email:..... .

6. Personal data requested to be provided [4] :..... .....

7. Purpose of request for provision:..... .....

8. Second request to provide personal data:

a) First time b) Other:..... (specify the number of times requested to provide information

content mentioned above)

9. Number of copies [5] :..... ....

10. Methods of receiving personal data:

□ Receive at the requested location

□ Received by post (specify the receiving address):..... .....

□ Fax (specify fax number):..... .....

□ Receive via electronic network (specify receiving address):..... .....

□ Other forms (specify):..... .....

11. Attached documents (in case of conditions):..... .....

REQUESTER
(Sign, write full name)

Model number 02

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

....., day month Year.....

REQUEST FOR PERSONAL DATA

(For organizations and businesses)

Dear:.....

1. Name of organization or enterprise:..... .....

....

2. Representative of organization or enterprise [1] : [6] : ....

3. ID card number/Citizen identification card/Passport..... .....

Issued on...../...../..... at..... ....

4. Headquarter address of the organization or enterprise:..... .....

5. Phone number [2] [7] .....; Fax.....; Email:.....

6. Personal data requested to be provided:..... .....

7. Purpose of request for provision:..... .....

8. Second request to provide personal data:

a) First time b) Other:..... (specify the number of times requested to provide information

content mentioned above)

9. Number of copies [3] : [8] : ....

10. Method of receiving documents, records and documents:

□ Receive at the place where information is requested

□ Received by post (specify the receiving address):..... .....

□ Fax (specify fax number):..... .....

□ Receive via electronic network (specify receiving address):..... .....

□ Other forms (specify):..... .....

11. Attached documents (in case of conditions):....

CLAIMANT [4] [9] *(Sign, write full name)*

Model number 03

ORGANIZATION NAME

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Number: *....., day month Year...*

NOTIFICATION

VIOLATION OF PERSONAL DATA PROTECTION REGULATIONS

To: Ministry of Public Security

(Department of Cyber Security and High-Tech Crime Prevention and Control, Ministry of Public Security)

Implement regulations on personal data protection,..... [1] [10] submit to the Ministry of Public Security a dossier assessing the impact of personal data processing , as follows:

1. Information about organizations and businesses

- Name of organization or enterprise:..... .....

- Head office address:..... .....

- Transaction office address:..... .....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment certificate No.:..... issued by.... date... month... year. .. in...

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

- Personnel responsible for protecting personal data:

First and last name:..... ....

Title:..... ....

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

Email:..... ....

2. Describe the violation of personal data protection regulations

- Time:..... ....

- Location:..... ....

- Behavior:..... ....

- Organizations, individuals, types of personal data and quantity of related data;

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

First and last name:..... ....

Title:..... ....

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

Email:..... ....

- Consequences:..... ....

- Measures to apply:..... .....

3. Attached documents

first..... ....

2..... ....

4. Commitment

(Name of agency, organization, business) hereby commits to: Be responsible before the law for the accuracy and legality of the information provided and accompanying documents.

Recipient:
- As above;
...

TM. ORGANIZATION, ENTERPRISE
(Sign, write full name, seal)

Model number 04

ORGANIZATION NAME

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Number:

....., day…. May...

NOTIFICATION

SUBMIT RECORDS FOR PERSONAL DATA PROCESSING IMPACT ASSESSMENT

To: Ministry of Public Security

(Department of Cyber Security and Crime Prevention using High Technology,

Police)

Implement regulations on personal data protection,..... [1][11] send to the Ministry of Public Security Dossier to assess the impact of personal data processing , as follows:

1. Information about organizations and businesses

- Name of organization or enterprise:..... .....

- Head office address:..... .....

- Transaction office address:..... .....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment certificate No.:..... issued by.... date... month... year. .. in...

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

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

First and last name:..... ....

Title:..... ....

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

Email:..... ....

2. Records of impact assessment of personal data processing

first..... ....

2..... ....

3. Commitment

(Name of agency, organization, business) hereby commits to: Be responsible before the law for the accuracy and legality of personal data processing impact assessment records and accompanying documents.

Recipient:
- As above;
...

TM. ORGANIZATION, ENTERPRISE
(Sign, write full name, seal)

Model number 05

ORGANIZATION NAME

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Number:

....., day…. May...

NOTIFICATION

CHANGING PROFILE CONTENT..... [1] [12]

To: Ministry of Public Security

(Via Department of Cyber Security and High-Tech Crime Prevention)

Implement regulations on personal data protection,..... [2] [13] send to the Ministry of Public Security Dossier to assess the impact of personal data processing , as follows:

1. Information about organizations and businesses

- Name of organization or enterprise:..... .....

- Head office address:..... .....

- Transaction office address:..... .....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment certificate No.:..... issued by.... date... month... year. .. in...

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

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

First and last name:..... ....

Title:..... ....

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

Email:..... ....

2. Brief description of changes to record content

- Changed content:..... .....

- Reason for change:..... ....

3. Attached documents

first..... ....

2..... ....

4. Commitment

(Name of agency, organization, enterprise) hereby commits to: Be responsible before the law for the accuracy and legality of the changed content and accompanying documents.

Recipient:
- As above;
...

TM. ORGANIZATION, ENTERPRISE
(Sign, write full name, seal)

Model number 06

ORGANIZATION NAME

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

Number:

....., day…. May...

PROFILE ASSESSING THE IMPACT OF TRANSFER OF PERSONAL DATA ABROAD

To: Ministry of Public Security

(Department of Cyber Security and High-Tech Crime Prevention and Control, Ministry of Public Security)

Implement regulations on personal data protection,..... [14] send to the Ministry of Public Security Dossier to assess the impact of transferring personal data abroad, as follows:

1. Information about organizations and businesses

- Name of organization or enterprise:..... .....

- Head office address:..... .....

- Transaction office address:..... .....

- Establishment decision/Enterprise registration certificate/Business registration certificate/Investment certificate No.:..... issued by.... date... month... year... . in...

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

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

First and last name:..... ....

Title:..... ....

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

Email:..... ....

2. Records assessing the impact of transferring personal data abroad

first..... ....

2..... ....

3. Commitment

(Name of agency, organization, enterprise) hereby commits to: Be responsible before the law for the accuracy and legality of the Dossier assessing the impact of transferring personal data abroad and accompanying documents.

Recipient:	**TM. ORGANIZATION, ENTERPRISE**
- As above;	*(Sign, write full name, seal)*
...	

---

[1] According to the provisions of the Civil Code on representatives and guardians for information requesters who are minors, people with limited civil capacity, or people who have lost capacity. Civilians, people with difficulty in cognition and behavior control...

[2] Enter the residence of the representative/guardian.

[3] Enter the phone number, fax, email of the representative/guardian.

[4] Clearly state the name of the data subject and relevant information to be provided.

[5] Print, copy, capture or file data.

1 According to the provisions of the Civil Code on representatives of organizations and businesses.

2 Write down the phone number, fax, email of the representative requesting information.

3 Print, copy, capture or file data.

4 The representative signs, clearly writes the full name and stamps the organization or enterprise.

1 Name of organization or business

1 Name of organization or business.

1 Document name: Personal data processing impact assessment profile or Impact assessment profile of transferring personal data abroad.

2 Name of organization or enterprise.

1 Name of organization or business