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

DECREE
On Personal Data Protection

Pursuant to the Law on Organization of the Government dated 19 June 2015; the Law Amending and Supplementing Certain Articles of the Law on Organization of the Government and the Law on Organization of Local Government dated 22 November 2019;

Pursuant to the Civil Code dated 24 November 2015;

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

Pursuant to the Law on Cybersecurity dated 12 June 2018;

At the proposal of the Minister of Public Security;

The Government hereby promulgates the Decree on Personal Data Protection.

Chapter I
GENERAL PROVISIONS

Article 1. Scope of regulation and subjects of application

1. This Decree provides for personal data protection and the responsibility for personal data protection 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 overseas;

d) Foreign agencies, organizations and individuals directly involved in or relating to the processing of personal data in Vietnam.

Article 2. Interpretations

In this Decree, the following terms and phrases shall be construed as follows:

1. Personal data means information in the form of symbols, letters, numbers, images, sounds or the like on an electronic medium that is associated with a particular person or helps to identify a particular person. Personal data includes basic personal data and sensitive personal data.

2. Information that helps to identify a particular person means information formed from his/her activities that, when combined with other stored data and/or information, can identify a particular person.

3. Basic personal data includes:

a) Family name, middle name and first name as stated in the birth certificate, and other name (if any);

b) Date of birth; date of death or disappearance;

c) Gender;

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

dd) Nationality;

e) Personal photos/ images;

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

h) Marital status;

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

k) Information about a person's digital account; personal data reflecting activities and history of activities in cyberspace;

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

4. Sensitive personal data means personal data associated with the rights to privacy of a person that, when violated, will directly affect his/her legitimate rights and interests, including:

a) Political views, religious views;

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

c) Information relating to racial or ethnic origin;

d) Information about inherited or acquired genetic characteristics of a person;

dd) Information about a person's physical attributes and/or biological characteristics;

e) Information about a person's sex life and/or sexual orientation;

g) Data on crimes and/or offenses collected and stored by law enforcement agencies;

h) Customer information of credit institutions, foreign bank branches, payment intermediary service providers, and other authorized organizations, including: customer identification information as prescribed by law, account information, deposit information, deposited asset information, transaction information, and/or information about organizations and/or individuals as guarantors at credit institutions, bank branches and/or payment intermediary service providers;

i) Location data of a person identified through location services;

k) Other personal data that is required by law to be specific and require necessary security measures.

5. Personal data protection means the prevention, detection, stopping and handling of violations relating to personal data in accordance with the law.

6. Data subject means a person reflected/identified by personal data.

7. Personal data processing means one or more activities affecting personal data, such as: collection, recording, analysis, confirmation, storage, correction, publicity, combination, access, retrieval, recovery, encryption, decryption, copying, sharing, transmission, provision, transference, deletion, and destruction of personal data or other related actions.

8. A data subject's consent means a clear, voluntary, and affirmative expression of his/her permission to process his/her personal data.

9. A Personal Data Controller means an organization or individual that determines the purposes for which and the means by which personal data is processed.

10. A Personal Data Processor means an organization or individual that performs data processing on behalf of the controller, under a contract or agreement with the controller.

11. A Personal Data Controller-Processor means an organization or individual that simultaneously determines the purposes for which and the means by which personal data is processed, and also directly processes personal data.

12. A third party means an organization or individual other than the data subject, the Personal Data Controller, the Personal Data Processor, and the Personal Data Controller-Processor that is permitted to process personal data.

13. Automated processing of personal data means a form of personal data processing performed by electronic means in order to evaluate, analyze and/or predict the activities of a particular person, such as: habits, hobbies, reliability, behavior, location, tendencies, capacities and other information.

14. Cross-border Transfer of personal data means the use of cyberspace, electronic devices and/or means or other forms to transfer personal data of Vietnamese citizens to a location outside the territory of the Socialist Republic of Vietnam or use a location located

outside the territory of the Socialist Republic of Vietnam to process personal data of Vietnamese citizens, including:

a) Organizations, enterprises and/or individuals transferring personal data of Vietnamese citizens to organizations, enterprises and/or management departments overseas for processing in accordance with the purposes agreed upon by the data subject;

b) Processing of personal data of Vietnamese citizens using automated systems located outside the territory of the Socialist Republic of Vietnam by the Personal Data Controller, Personal Data Controller-Processor, or Personal Data Processor in accordance with the purposes agreed upon by the data subject.

Article 3. Principles of personal data protection

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

2. The data subject is made aware of activities relating to the processing of his/her personal data, unless otherwise provided for by law.

3. Personal data is processed only for the purposes that have been registered and declared by the Personal Data Controller, Personal Data Processor, Personal Data Controller-Processor, and/or Third Party.

4. Personal data collected must be appropriate and limited within the scope and purposes of processing. Personal data may not be bought or sold in any form, unless otherwise provided by law.

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

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

7. Personal data is only stored for a period suitable for the purposes of processing, unless otherwise provided for by law.

8. The [Personal] Data Controller and the Personal Data Controller-Processor are responsible for complying with the principles of processing personal data specified in Clauses 1 to 7 of this Article and demonstrating their compliance with these principles of processing personal data.

Article 4. Handling violations of regulations on personal data protection

Agencies, organizations and individuals that violate regulations on personal data protection, depending on the severity, may be subject to discipline, administrative sanctions, or criminal penalty as prescribed.

Article 5. State management in personal data protection

The Government shall unify the state management of personal data protection.

Contents of state management of personal data protection include:

1. Submit to the competent state agencies for promulgation or promulgate within its competence legal documents; direct and organize the implementation of legal documents on personal data protection.

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

3. Provide guidance to agencies, organizations and individuals on measures, processes and standards for protecting personal data in accordance with the law.

4. Propagate and educate on the law on personal data protection; communicate and disseminate knowledge and skills of personal data protection.

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

6. Inspect and examine the implementation of regulations on personal data protection; settle complaints and denunciations, and handle violations of regulations on personal data protection in accordance with the law.

7. Collect statistics, inform and report the situation of personal data protection and the implementation of the laws on personal data protection to the competent state agencies.

8. Engage in international cooperation on personal data protection.

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

The protection of personal data shall be carried out in accordance with the provisions of international treaties to which the Socialist Republic of Vietnam is a contracting party, other 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 the laws on personal data protection.

2. Participate in mutual legal assistance in personal data protection of other countries, including notification, request for complaint, investigation assistance and information exchange, with appropriate measures to protect personal data.

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

4. Organize bilateral and multilateral meetings, exchange experience on law-making and practices on personal data protection.

5. Transfer technology for personal data protection.

Article 8. Prohibited acts

1. Processing personal data contrary to the laws on personal data protection.

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

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

4. Obstructing personal data protection activities of the competent agencies.

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 made aware of the processing of their personal data, unless otherwise provided by law.

2. Right to consent

Data subjects may consent or refuse to consent the processing of their personal data, except for the cases specified in Article 17 of this Decree.

3. Right to access

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

4. Right to withdraw consent

Data subjects may withdraw their consent, unless otherwise provided by law.

5. Right to delete data

Data subjects may delete or request their personal data to be deleted, unless otherwise provided by law.

6. Right to restrict data processing

a) Data subjects may request restriction of the processing of their personal data, unless otherwise provided by law;

b) The restriction of data processing shall be carried out within 72 hours after the request of the data subject, with respect to all personal data that the data subject requests to be restricted, unless otherwise provided for by law.

7. Right to request the provision of data

Data subjects may request the Personal Data Controller or Personal Data Controller-Processor to provide their personal data, unless otherwise provided by law.

8. Right to object to data processing

a) Data subjects may object to the Personal Data Controller's or Personal Data Controller-Processor's processing of their personal data in order to prevent or limit the disclosure of personal data or the use of personal data for advertising and marketing purposes, unless otherwise provided by law;

b) The Personal Data Controller or Personal Data Controller-Processor shall fulfill the request of the data subject within 72 hours after receiving his/her request, unless otherwise provided for by law.

9. Right to complain, denounce and initiate lawsuits

Data subjects have the right to complain, denounce or initiate a lawsuit in accordance with the law.

10. Right to claim compensation of damages

Data subjects have the right to claim damages in accordance with the law when there is a violation of regulations on personal data protection with regard to their personal data, unless otherwise agreed by the parties or otherwise provided for by law.

11. Right to self-defense

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

Article 10. Obligations of data subjects

1. To protect their own personal data; to request other relevant organizations and individuals to protect their personal data.

2. To respect and protect the personal data of others.

3. To provide their personal data in a complete and accurate manner when giving consent to the processing of personal data.

4. To participate in propaganda and dissemination of skills of personal data protection.

5. To comply with the laws on personal data protection and participate in the prevention and combating of violations of regulations on personal data protection.

Section 2
PERSONAL DATA PROTECTION IN PROCESSING PERSONAL DATA

Article 11. Consent of data subjects

1. The consent of a data subject shall be required for all activities in the processing of personal data, unless otherwise provided for by law.

2. The consent of a data subject is only valid when it is voluntary and the data subject clearly knows the following:

a) The type of personal data to be processed;

b) The purposes of processing the personal data;

c) Organizations and/or individuals permitted to process the personal data;

d) His/her rights and obligations.

3. The consent of a data subject must be expressed clearly and specifically in writing, by voice, by ticking a consent box, in the syntax of consent via text message, by selecting the consent technical settings or by another action that shows his/her consent.

4. The consent must be made for a single purpose. When there are multiple purposes, the Personal Data Controller or Personal Data Controller-Processor shall list the purposes for the data subject to agree to one or more of the listed purposes.

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

6. The silence or non-response of the data subject is not considered as 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 consent of a data subject is valid until the data subject decides otherwise or the competent state agency requests otherwise in writing.

10. In the event of a dispute, the responsibility for proving the consent of the data subject lies on the Personal Data Controller or Personal Data Controller-Processor.

11. With authorization in accordance with the provisions of the Civil Code, organizations and/or individuals may act on behalf of the data subject to carry out procedures relating to the processing of his/her personal data with the Personal Data Controller or Personal Data Controller-Processor in the event that the data subject clearly knows and give consent as prescribed in Clause 3 of this Article, unless otherwise provided for by law.

Article 12. Withdrawal of consent

1. Withdrawal of consent does not affect the legality of the data processing that was consented to prior to the withdrawal of consent.

2. Withdrawal of consent must be in a format that can be printed or reproduced in writing, including in electronic form or verifiable format.

3. Upon receiving a request for withdrawal of consent from a data subject, the Personal Data Controller or Personal Data Controller-Processor shall notify the data subject of possible consequences and damages when the consent is withdrawn.

4. After implementing the provisions in Clause 2 of this Article, the Personal Data Controller, the Personal Data Processor, the Personal Data Controller-Processor, and any Third Party must stop processing and request relevant organizations and individuals to stop processing the data of the data subject withdrawing his/her consent.

Article 13. Notice of personal data processing

1. The notice is made once before processing personal data.

2. The contents of the notice given to the data subject about personal data processing include:

a) The purpose(s) of processing;

b) The type of personal data to be processed in relation to the purposes of processing specified in Point a, Clause 2 of this Article;

c) The method of processing;

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

dd) Potential unexpected consequences and/or damages;

e) The start time and the end time of personal data processing.

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

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

a) The data subject clearly knows and fully agrees with the contents specified in Clauses 1 and 2 of this Article before agreeing to the Personal Data Controller's or Personal Data Controller- Processor's collection of personal data in accordance with the provisions in Article 9 of this Decree;

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

Article 14. Provision of personal data

1. The data subject may request the Personal Data Controller or Personal Data Controller-Processor to provide to the data subject his/her own personal data.

2. The Personal Data Controller or Personal Data Controller-Processor may:

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

b) Provide personal data of the data subject on his/her behalf to other organizations and/or individuals with his/her agreement to such representation and authorization, unless otherwise provided for by law.

3. The provision of personal data of the data subject is to be carried out by the Personal Data Controller or Personal Data Controller-Processor within 72 hours after the request of the data subject, unless otherwise provided by law.

4. The Personal Data Controller or Personal Data Controller-Processor may not provide personal data in the following cases:

a) [When the provision] causes harm to national defense, national security, and/or social order and safety;

b) When the provision of personal data of the data subject may affect the safety, and/or physical or mental health of others;

c) When the data subject does not agree to the provision, or representation, or authorization of the receipt of personal data.

5. Forms of request to provide personal data:

a) The data subject directly or by authorizing another person comes to the headquarters of the Personal Data Controller or Personal Data Controller-Processor to request provision of personal data.

The request receiver is responsible for guiding the requestor to fill in the request form for provision of personal data.

If the requestor is illiterate or disabled and cannot write the request, the request receiver shall be responsible for helping to fill in the request form for provision of personal data;

b) The written request for provision of personal data, made under Forms No. 01 and No. 02 attached in the Appendix to this Decree shall be sent via electronic network, by post or fax to the Personal Data Controller or Personal Data Controller-Processor.

6. The request form for provision of personal data must be written in Vietnamese, including the following main contents:

a) Full name; place of residence, address; identity card number, citizen identification card number or passport number of the requestor; fax number, telephone, email address (if any);

b) Personal data requested, including the name of the document, file or material;

c) Form of provision of personal data;

d) Reasons and purposes for requesting provision of personal data.

7. The request for provision of personal data specified in Clause 2 of this Article must be accompanied by the written consent of the relevant individual or organization.

8. Receipt of requests for provision of personal data

a) The Personal Data Controller or Personal Data Controller-Processor are responsible for receiving requests for provision of personal data and monitoring the process and list of the provision of personal data according to the requests;

b) If the requested personal data does not fall under its authority, the Personal Data Controller or Personal Data Controller-Processor receiving the request must notify and direct the requestor to the competent agency, or clearly notify its inability to provide personal data.

9. Handling requests for provision of personal data

Upon receiving a valid request for provision of personal data, the Personal Data Controller or Personal Data Controller-Processor responsible for providing personal data shall notify the time limit, location, and form of provision of personal data; actual expenses for printing, copying, photocopying and sending information by post and/or fax (if any), and payment method and payment term; and provide personal data according to the order and procedures specified in this Article.

Article 15. Correction of personal data

1. Data subjects:

a) Can access to view and correct/edit their personal data after collection by the Personal Data Controller or Personal Data Controller-Processor with their consent, unless otherwise provided for by law;

b) If it is not possible to directly correct/edit [their personal data] for technical reasons or for other reasons, the data subject may request the Personal Data Controller or Personal Data Controller-Processor to correct/edit their personal data.

2. The Personal Data Controller or Personal Data Controller-Processor shall correct/edit the personal data of the data subject after obtaining the consent of the personal data subject as soon as possible or in accordance with the specialized laws. If it is not possible, the data subject must be notified 72 hours after the receipt of his/her request for correction of his/her personal data.

3. The Personal Data Processor or a Third Party may correct/edit the personal data of the data subject after obtaining the written consent of the Personal Data Controller or Personal Data Controller-Processor and fully knowing that the consent of the data subject has been obtained.

Article 16. Storage, deletion and destruction of personal data

1. Data subjects may request the Personal Data Controller or the Personal Data Controller-Processor to delete their personal data in the following cases:

a) The data subjects find it is no longer necessary for the agreed purpose of collection and accepts any possible damages upon the request for data deletion;

b) The data subjects withdraw their consent;

c) The data subjects object to the processing of data and the Personal Data Controller or Personal Data Controller-Processor does not have a legitimate reason to continue processing;

d) The personal data is not processed in accordance with the agreed purpose or the processing of personal data is in violation of the law;

dd) The personal data must be deleted in accordance with the law.

2. Data deletion shall not apply at the request of the data subject in the following cases:

a) The law does not allow the deletion of the data;

b) The personal data is processed by a competent state agency for the purpose of serving the operation of the state agency in accordance with the law;

c) The personal data has been publicly disclosed in accordance with the law;

d) The personal data is processed for the purpose of serving requirements of the law, scientific research or statistics in accordance with the law;

dd) In the event of an emergency of national defense, national security, social order and safety, major disasters, or dangerous epidemics; when there is a risk of threatening national security and national defense but not to the extent of declaring a state of emergency; to prevent and combat riots and terrorism; to prevent and combat crimes and law violations;

e) In response to an emergency situation that threatens the life, health or safety of the data subject or others in an emergency.

3. In the event that an enterprise is divided, separated, merged, consolidated or dissolved, personal data shall be transferred in accordance with the law.

4. In the event of division, separation or merger of agencies, organizations or administrative bodies, or reorganization or transformation of the ownership form of state enterprises, personal data shall be transferred in accordance with the law.

5. Data deletion shall be carried out within 72 hours upon the request of the data subject with respect to all personal data collected by the Personal Data Controller or Personal Data Controller-Processor, unless otherwise provided by law.

6. The Personal Data Controller, Personal Data Controller-Processor, Personal Data Processor, and/or Third Party shall store personal data in a form appropriate to its operations

and have measures to protect personal data in accordance with the law.

7. The Personal Data Controller, Personal Data Controller-Processor, Personal Data Processor, and/or Third Party shall irrecoverably delete data in the following cases:

a) The data is processed for improper purposes or the purpose of processing personal data has been fulfilled with the consent of the data subject;

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

c) The Personal Data Controller, Personal Data Controller-Processor, Personal Data Processor, or Third Party is dissolved or no longer operates or declares bankruptcy or has its business activities terminated in accordance with the law.

Article 17. Cases where processing of personal data does not require the consent of the data subject

1. In an emergency situation, when relevant personal data needs be processed immediately to protect the life and health of the data subject or others. It is the responsibility of the Personal Data Controller, Personal Data Controller-Processor, Personal Data Processor, or a Third Party to prove this case.

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

3. Processing of personal data by a competent state agency in the event of an emergency of national defense, national security, social order and safety, major disaster, or dangerous epidemic; when there is a risk of threatening security and national defense but not to the extent of declaring a state of emergency; to prevent and combat riots and terrorism; to prevent and combat crimes and law violations in accordance with the law.

4. To fulfill the contractual obligations of the data subject with relevant agencies, organizations, and individuals as prescribed by law.

5. To serve 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 may carry out audio and/or video recording and process personal data obtained from audio or video recording activities in public places for the purpose of protecting national security, social order and safety, or the legitimate rights and interests of organizations and individuals as prescribed by law without the consent of the data subject. When carrying out audio and/or video recording, it is the responsibility of competent agencies and organizations to notify the data subject so that he/she can understand that he/she is being recorded or filmed, unless otherwise provided for by law.

Article 19. Processing of personal data of persons declared missing or deceased

1. The processing of personal data related to the personal data of a person who is declared missing or deceased must be consented to by his/her spouse or his/her adult child/children. In the absence of such persons, the consent must be obtained from the father or mother of the person declared missing or deceased, except for the cases specified in Articles 17 and 18 of this Decree.

2. In the absence of all the persons mentioned in Clause 1 of this Article, 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 done 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 be consented to by the child in cases where the child is a full 7 years of age or older and must [also] be consented to by the parent or guardian as prescribed, except for cases specified by the provisions of Article 17 of this Decree. The Personal Data Controller, Personal Data Controller-Processor, Personal Data Processor, or a Third Party must verify the age of children before processing children's personal data.

3. Children's personal data must be stopped from processing, and must be irrecoverably deleted or destroyed in the following cases:

a) The data is processed for improper purposes or the purpose of processing personal data has been fulfilled with the consent of the data subject, unless otherwise provided for by law;

b) The child's parent or guardian withdraws his/her consent to the processing of the child's personal data, unless otherwise provided for by law;

c) At the request of a competent functional authority when there are sufficient grounds to prove that the processing of personal data affects children's legitimate rights and interests, unless otherwise provided for by law.

Article 21. Protection of personal data in the business of services of marketing and/or introduction of advertising products

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

2. The processing of a customer's personal data to provide services of marketing and/or introduction of advertising products must be done with the consent of the customer, on the basis that the customer is well aware of the contents, methods, forms, and frequency of product introduction.

3. Organizations and individuals providing services of marketing and/or introduction of advertising products are responsible for proving that the use of personal data of customers to whom products are introduced is in accord with the provisions of Clauses 1 and 2 of this

Article.

Article 22. Unauthorized/ illegal collection, transfer, purchase and sale of personal data

1. Organizations and individuals involved in personal data processing must apply personal data protection measures to prevent unauthorized/illegal collection of personal data from the systems and equipment used for their services.

2. It is a violation of law to set up software systems, technical measures or organize activities of collecting, transferring, purchasing or selling personal data without the consent of data subjects.

Article 23. Notice on violation of regulations on personal data protection

1. When detecting a violation of regulations on personal data protection, the Personal Data Controller or Personal Data Controller-Processor shall notify the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) within 72 hours after the violation occurs according to Form No. 03 in the Appendices to this Decree. If the notice is made after 72 hours, the reason for the delayed/late notice must be attached.

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

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

a) Description of the nature of the breach of regulations on personal data protection, including: time, place, act, organization, individual, types of personal data and amount/ size of relevant data;

b) Contact details of the employee assigned the task of data protection or the organization or individual responsible for the protection of personal data;

c) Description of possible consequences and/or damages of the violation of regulations on personal data protection;

d) Description of the measures taken to address and minimize the harm of violations of regulations on personal data protection.

4. In cases where it is not possible to fully report the contents specified in Clause 3 of this Article, the notice may be made in batches and/or stages.

5. The Personal Data Controller or Personal Data Controller-Processor must make a written Confirmation of the occurrence of violations of regulations on personal data protection, and coordinate with the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) to handle the violations.

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

a) Detecting violations of the law on personal data;

b) Personal data is processed for incorrect purposes, not in accordance with the original agreement between the data subject and the Personal Data Controller or Personal Data Controller-Processor, or in contravention of the provisions of law;

c) The rights of the data subject are not protected or not properly implemented;

d) Other cases as prescribed by law.

Section 3
IMPACT ASSESSMENT AND CROSS-BORDER TRANSFER OF PERSONAL DATA

Article 24. Impact assessment of personal data processing

1. The Personal Data Controller or Personal Data Controller-Processor shall make and keep its Personal Data Processing Impact Assessment Record from the time it starts processing personal data.

The Personal Data Processing Impact Assessment Record of the Personal Data Controller or Personal Data Controller-Processor shall contain:

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

b) Full names 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 or Personal Data Controller-Processor;

c) The purpose of the personal data processing;

d) The categories of personal data to be processed;

dd) Organizations and/or individuals receiving personal data, including organizations and/or individuals outside of Vietnam;

e) Instances/ Cases of cross-border transfer of personal data;

g) The period of time/ time for processing personal data; the envisaged period of time/ estimated time for deleting or destroying personal data (if any);

h) A description of the personal data protection measures applied;

i) Assessment of the impact of the processing of personal data; potential unexpected consequences and/or damages, and measures to minimize or eliminate such risk or harm.

2. The Personal Data Processor shall make and keep a Personal Data Processing Impact Assessment Record in the case of implementation of a contract with the Personal Data Controller. The Personal Data Processing Impact Assessment Record of the Personal Data Processor shall contain:

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

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

c) A description of the processing activities and the categories of personal data processed under the contract with the Personal Data Controller;

d) The period of time/time for processing personal data; the envisaged period of time/ estimated time for deleting or destroying personal data (if any);

dd) Instances/ Cases of cross-border transfer of personal data;

e) A general description of the personal data protection measures applied;

g) Potential unexpected consequences and/or damages, and measures to minimize or eliminate such risk or harm.

3. The Personal Data Processing Impact Assessment Record specified in Clauses 1 and 2 of this Article is made in writing with legal validity by the Personal Data Controller, the Personal Data Controller-Processor or the Personal Data Processor.

4. The Personal Data Processing Impact Assessment Record must always be available for inspection and evaluation by the Ministry of Public Security and one original copy thereof must be sent to the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) according to Form No. 04 in the Appendices to this Decree within 60 days from the date of processing of personal data.

5. The Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) shall evaluate, and request the Personal Data Controller, the Personal Data Controller-Processor or the Personal Data Processor to complete the Personal Data Processing Impact Assessment Record if the record is incomplete and not in accordance with regulations.

6. The Personal Data Controller, the Personal Data Controller-Processor or the Personal Data Processor shall update and supplement the Personal Data Processing Impact Assessment Record when there is a change in the contents of the Record sent to the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) according to Form No. 05 in the Appendices to this Decree.

Article 25. Cross-border Transfer of personal data

1. Personal data of Vietnamese citizens can be cross-border transferred if the Data Transferring Party makes a Record of Impact Assessment of Cross-border transfer of personal data and carries out the procedures as prescribed in Clauses 3, 4 and 5 of this Article. The parties transferring data outside of Vietnam include the Personal Data Controller, the Personal Data Controller-Processor, the Personal Data Processor or a Third Party.

2. A Record of Impact Assessment of Cross-border transfer of personal data shall contain:

a) Information and contact details of the Party transferring and the Party receiving

personal data of Vietnamese citizens;

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

c) Description and explanation of the objectives of the activities of processing personal data of Vietnamese citizens after being cross-border transferred;

d) Description and clarification of the categories of personal data being cross-border transferred;

dd) Description and clear statement of compliance with regulations on personal data protection in this Decree, detailing the personal data protection measures applied;

e) Assessment of the impact of the processing of personal data; potential unexpected consequences and/or damages, and measures to minimize or eliminate such risk or harm;

g) The consent of the data subject as prescribed in Article 11 of this Decree, on the basis of being well aware of the response and complaint mechanism when incidents or requests arise;

h) A document showing the binding and responsibility between organizations and individuals that transfer and receive personal data of Vietnamese citizens for the processing of personal data.

3. The Record of Impact Assessment of Cross-border transfer of personal data must always be available to serve the inspection and evaluation activities of the Ministry of Public Security.

The party cross-border transferring data shall send 01 original of the Record to the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) according to Form 06 in the Appendices to this Decree within 60 days from the date of processing of personal data.

4. The Data Transferring Party shall notify the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) in writing of information about the data transfer and contact details of the organization and/or individual in charge after the data transfer has taken place successfully.

5. The Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) shall evaluate and request the Data Transferring Party to complete the Record of Impact Assessment of Cross-border transfer of personal data if the Record is incomplete and not in accordance with regulations.

6. The party cross-border transferring data shall update and supplement the Record of Impact Assessment of Cross-border transfer of personal data when there is a change in the contents of the Record sent to the Ministry of Public Security (Department of Cybersecurity and High-Tech Crime Prevention) according to Form No. 05 in the Appendices to this Decree. The time limit to complete the Record for the Party cross-border transferring data is 10 days from the date of request.

7. Based on the specific situation, the Ministry of Public Security shall decide to inspect the cross-border transfer of personal data once a year, except for cases of detecting violations of the law on protection of personal data specified in this Decree or cases of disclosure or loss of personal data of Vietnamese citizens.

8. The Ministry of Public Security shall decide to request the party cross-border transferring data to stop cross-border transferring personal data in the following cases:

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

b) When the party cross-border transferring personal data fails to comply with the provisions of Clauses 5 and 6 of this Article;

c) When the party cross-border transferring data allows an incident of disclosure or loss of personal data of Vietnamese citizens to occur.

Section 4

MEASURES AND CONDITIONS TO ENSURE PROTECTION OF PERSONAL DATA

Article 26. Measures to protect personal data

1. Personal data protection measures shall be applied from the very beginning and throughout the processing of personal data.

2. Measures to protect personal data shall include:

a) Management measures taken by organizations or individuals related to the processing of personal data;

b) Technical measures taken by organizations or individuals related to the processing of personal data;

c) Measures taken by competent state management agencies in accordance with this Decree and relevant laws;

d) Investigation and procedural measures taken by competent state agencies;

dd) Other measures as prescribed by law.

Article 27. Basic personal data protection

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

2. Developing and promulgating personal data protection policy, clearly stating what needs to be done according to the provisions of this Decree.

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

4. Checking network security for the system and the means and equipment in service of personal data processing before processing, irrecoverable deletion or destruction of devices containing personal data.

Article 28. Protection of sensitive personal data

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

2. Designating a department with the function of protecting personal data, designating personnel in charge of personal data protection and discussing information about the department and individual in charge of personal data protection with the Agency specializing in the protection of personal data. If the Personal Data Controller, Personal Data Controller-Processor, Personal Data Processor or a Third Party are individuals, information of the implementing individual shall be discussed.

3. Notifying the data subject that the sensitive personal data of the data subject shall be processed, except for the cases specified in Clause 4, Article 13, Article 7 and Article 18 of this Decree.

Article 29. Agency in charge of personal data protection and national portal on personal data protection

1. The agency in charge of personal data protection is the Department of Cybersecurity and High-Tech Crime Prevention under the Ministry of Public Security, which is responsible for assisting the Ministry of Public Security in performing the state management of personal data protection.

2. The national portal on personal data protection shall:

a) Provide information on the guidelines and policies of the [Communist] Party and laws of the State on personal data protection;

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

c) Update information and situation of personal data protection;

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

dd) Provide information on results of evaluation of personal data protection of relevant agencies, organizations and individuals;

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

g) Warn and coordinate in warning about risks and acts of infringing personal data in accordance with the law;

h) Handle violations of personal data protection in accordance with the law;

i) Perform other activities in accordance with the law on personal data protection.

Article 30. Conditions for ensuring the protection of personal data

1. Personal data protection forces:

a) The personal data protection task force is located at the Agency in charge of personal data protection;

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

c) Organizations and individuals are mobilized to participate in the protection of personal data;

d) The Ministry of Public Security shall develop specific programs and plans to develop human resources for personal data protection.

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

3. Physical facilities and operating conditions for the Agency in charge of personal data protection are ensured.

Article 31. Funds for personal data protection activities

1. Financial sources for personal data protection include the state budget; support from domestic and foreign agencies, organizations and individuals; revenues from the provision of personal data protection services; international aid and other legitimate sources of revenue.

2. Funds for personal data protection of state agencies shall be guaranteed by the state budget and shall be included in the annual state budget estimates. The management and use of funds from the state budget must comply with the law on state budget.

3. Funds for personal data protection of organizations and enterprises shall be arranged and implemented by organizations and enterprises themselves according to regulations.

Chapter III
RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS

Article 32. Responsibilities of the Ministry of Public Security

1. To assist the Government in performing unified state management of personal data protection.

2. To provide guidance and implement personal data protection activities, protect the rights of data subjects against acts of violating the provisions of the law on personal data protection, and propose the promulgation of Standards for personal data protection and recommendations for application.

3. To set up, manage and operate the national portal on personal data protection.

4. To evaluate results of personal data protection of relevant agencies, organizations and individuals.

5. To receive records, forms and information on personal data protection according to the provisions of this Decree.

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

7. To inspect, examine, and settle complaints and denunciations, and handle violations of regulations on personal data protection in accordance with the law.

Article 33. Responsibilities of the Ministry of Information and Communications

1. To direct media agencies, press, organizations and enterprises under its management to implement personal data protection according to the provisions of this Decree.

2. To develop, provide guidance and implement measures for personal data protection, and ensure network information security for personal data in information and communication activities according to the assigned functions and tasks.

3. To 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

To manage, inspect, examine, supervise, and handle violations and apply regulations on personal data protection to agencies, organizations and individuals under the management of the Ministry of National Defense in accordance with the law and assigned functions and tasks.

Article 35. Responsibilities of the Ministry of Science and Technology

1. To coordinate with the Ministry of Public Security in developing Personal Data Protection Standards and recommendations for the application of Personal Data Protection Standards.

2. To research and discuss with the Ministry of Public Security on measures for personal data protection to keep up with the development of science and technology.

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

1. To perform state management of personal data protection for sectors and fields under their management according to the provisions of the law on personal data protection.

2. To develop and implement the contents and tasks of personal data protection specified in this Decree.

3. To supplement regulations on personal data protection in the formulation and

implementation of tasks of ministries and sectors.

4. To allocate funds for personal data protection activities according to the current budget management decentralization/ hierarchy.

5. To promulgate an Open Data List in accordance with regulations on personal data protection.

Article 37. Responsibilities of the People's Committees of the provinces and cities under direct management of the Central Government

1. To perform state management of personal data protection in the sectors and fields under their management according to the provisions of the law on protection of personal data.

2. To implement regulations on personal data protection specified in this Decree.

3. To allocate funds for personal data protection activities according to the current budget management decentralization/hierarchy.

4. To promulgate an Open Data List in accordance with regulations on personal data protection.

Article 38. Responsibilities of the Personal Data Controller

1. To 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, and to review and update these measures as necessary.

2. To record and store system logs of personal data processing.

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

4. To select a Personal Data Processor in accordance with a clear mandate and work only with a Personal Data Processor that has appropriate protection measures in place.

5. To 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. To coordinate with the Ministry of Public Security and state agencies having competence in personal data protection, to provide information for investigation and handling of violations of the law on personal data protection.

Article 39. Responsibilities of the Personal Data Processor

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

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

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

4. The Personal Data Processor is responsible to the data subject for damages caused by its processing of personal data.

5. Delete, return all personal data to the Personal Data Controller after finishing its processing of [personal] data.

6. Cooperate with the Ministry of Public Security and the state authorities in protecting personal data, providing information for investigation and handling of violations of the law on protection of personal data.

Article 40. Responsibilities of the Personal Data Controller-Processor

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

Article 41. Responsibilities of Third Parties

Fully comply with regulations on responsibilities for processing personal data as prescribed in this Decree.

Article 42. Responsibilities of relevant organizations and individuals

1. Apply measures to protect their own personal data, assume responsibility for the accuracy of personal data provided by them.

2. Comply with regulations on protection of personal data in this Decree.

3. Timely report to the Ministry of Public Security with regard to violations related to personal data protection activities.

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

Chapter IV
IMPLEMENTATION

Article 43. Effect

1. This Decree takes effect from 01 July 2023.

2. Micro-enterprises, small enterprises, medium-sized enterprises and start-up enterprises have the option to waive the regulations regarding assignment of an individual and personal data protection division for the first 2 years as from the establishment of their business.

3. Micro-enterprises, small enterprises, medium-sized enterprises and start-up enterprises directly engaged in personal data processing activities will not be exempted from being subject to the provisions of Clause 2 of this Article.

Article 44. Implementation responsibilities

1. The Minister of Public Security directs, examines and provides guidance on the implementation of this Decree.

2. Ministers, directors of ministerial-level agencies, directors of government-affiliated agencies, chairpersons of People's Committees of provinces and municipalities are responsible for implementation of this Decree.

Recipients:
- Secretariat of the Communist Party's Central Committee;
- Prime Minister, Deputy Prime Ministers;
- Ministries, ministerial-level authorities, government-affiliated authorities;
- People's Councils and People's Committees of provinces and municipalities;
- Central Office and Divisions of the Communist Party Committee;
- Office of the General Secretary;
- Office of the President;
- Council for Ethnic Minorities and Committees of the National Assembly;
- Office of the National Assembly;
- People's Supreme Procuracy;
- Supreme People's Court;
- State Audit Office;
- National Financial Supervisory Commission;
- Bank for Social Policies;
- Vietnam Development Bank;
- Central Committee of Vietnam Fatherland Front;
- Central Body of Unions;
- Government Office: Minister Chairman of Government Office, Vice Chairpersons of Government Office, Assistants to Prime Minister, General Director of the Government Office's Portal, Departments, Bureaus, affiliated agencies, Official Gazette;
- Filed: Archives, Procedure Control (2b)TM

FOR THE GOVERNMENT
FOR THE PRIME MINISTER
DEPUTY PRIME MINISTER

[Signed and sealed]

Tran Luu Quang

Appendix

(Attached to Government's Decree No. 13/2023/ND-CP dated 17 April 2023)

Form No. 01	Request form for provision of personal data (for individual)
Form No. 02	Request form for provision of personal data (for organizations, enterprises)
Form No. 03	Notice on violation of regulations on personal data protection
Form No. 04	Notice on submission of Personal Data Processing Impact Assessment Record
Form No. 05	Notice on change of Record contents
Form No. 06	Record of Impact Assessment of Cross-border Transfer of Personal Data

Form No. 01

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom – Happiness

..., date……

REQUEST FOR PROVISION OF PERSONAL DATA

(For individual)

To: …..

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

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

3. ID Card / Citizen Identity Card / Passport No. .....

Issued on .../..... /….. by .....

4. Residence[2]:.....

5. Telephone[3] ..... ; Fax .....; Email: .....

6. Personal data requested[4]: .....

7. Purpose(s) of the request:.....

8. Request for provision of personal data for the:

a) first time b) other: ..... (specify the number of times that the request with the above contents has been submitted)

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

10. Method for receiving personal data:

□ Receiving at the place of request

□ Receiving via post office (please specify the receipt address): .....

□ Fax (please specify the facsimile number): .....

□ Receiving via electronic network (please specify the receiving [electronic] address):

□ Other (please specify):.....

11. Attached documents (in case of provision [of personal data] with conditions):....

REQUESTOR

(sign, specify full name)

[1] In accordance with the provisions set out on Civil Code on representatives and guardians of requestors of information who are minors, persons with limited civil act capacity, persons having lost their civil act capacity, persons having cognitive and behavioral difficulties, etc.

[2] Write the place of residence of the representative/guardian.

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

[4] Write name of data subject and relevant information to be provided.

[5] Printed copy, photocopy, duplicate or file of data.

Form No. 02

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom – Happiness

..., date……..

REQUEST FOR PROVISION OF PERSONAL DATA

(For organization or enterprise)

To: …..

1. Name of organization, enterprise:.....

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

3. ID Card / Citizen Identity Card / Passport No. .....

Issued on ...../...../…… by .....

4. Head office address of organization, enterprise:.....

5. Telephone number[2] .....; Fax .....; Email: .....

6. Personal data being requested:.....

7. Purpose(s) of the request:.....

8. Request for provision of personal data for the:

a) first time ..... b) other: …. (specify the number of times that the request with the above contents has been submitted)

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

10. Method of receiving personal data:

□ Receiving at the place of request

□ Receiving via post office (please specify the receipt address):.....

□ Fax (please specify the facsimile number):.....

□ Receiving via electronic network (please specify the receiving [electronic] address):

□ Other (please specify):.....

11. Attached documents (in case of provision [of personal data] with conditions):....

REQUESTOR [4]

(sign, specify full name)

[1] In accordance with the provisions set out in the Civil Code on representatives of organizations and enterprises

[2] Write telephone number, facsimile number, email of representative of the requestor requesting provision of information.

[3] Printed copy, photocopy, duplicate or file of data.

[4] Representative signs, specifies full name and affixes seal of the organization or enterprise.

Form No. 03

NAME OF ORGANIZATION	**SOCIALIST REPUBLIC OF VIETNAM**
_____	**Independence – Freedom – Happiness**
	_____
No.: …	
	...., date .....

NOTICE
ON VIOLATION OF REGULATIONS ON PERSONAL DATA PROTECTION

To: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention under the Ministry of Public Security)

In compliance with regulations on personal data protection, ...[1] submits to the Ministry of Public Security a Personal Data Processing Impact Assessment Record as follows:

1. Information on organization or enterprise

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

- Head office address: .....

- Address of the transaction office: .....

- Establishment Decision / Enterprise Registration Certificate / Business Registration Certificate / Investment Certificate No.: ..... issued by .... on ..... in .....

- Telephone: .....Website .....

- Person in charge of personal data protection:

Full name: .....

Position: .....

Contact telephone (landline and mobile): .....

Email: .....

2. Description of acts of violation of personal data protection regulations

- Time: .....

- Place: .....

- Acts of violation: .....

- Organization, individual, types of personal data and the amount/ size of data involved;

- Person in charge of personal data protection: .....

Full name: .....

Position: .....

Contact telephone (landline and mobile): .....

Email: .....

- Consequences that occurred: .....

- Applicable measures:.....

3. Attached documents

1. ……

2. ……

4. Undertakings

(Name of agency, organization, enterprise) hereby undertakes to assume responsibility before the laws for the accuracy and legality of the provided information and the attached documents.

Recipients:	**FOR THE ORGANIZATION OR ENTERPRISE**
- As above;	*(sign, specify full name, seal)*
....	

[1] Name of organization or enterprise

Form No. 04

NAME OF ORGANIZATION	**SOCIALIST REPUBLIC OF VIETNAM**
	Independence – Freedom – Happiness
No.: …	*…., date .....*

NOTICE
ON SUBMISSION OF
PERSONAL DATA PROCESSING
IMPACT ASSESSMENT RECORD

To: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention under the Ministry of Public Security)

In compliance with regulations on personal data protection, ...[1] submits to the Ministry of Public Security a Personal Data Processing Impact Assessment Record as follows:

1. Information on organization or enterprise

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

- Head office address: .....

- Address of the transaction office: .....

- Establishment Decision / Enterprise Registration Certificate / Business Registration Certificate / Investment Certificate No.: ..... issued by .... on ..... in .....

- Telephone: .....Website .....

- Person in charge of personal data protection:

Full name: .....

Position: .....

Contact telephone (landline and mobile): .....

Email: .....

2. Personal Data Processing Impact Assessment Record

1. ……

2. ……

3. Undertakings

(Name of agency, organization, enterprise) hereby undertakes to assume responsibility before the laws for the accuracy and legality of the Dossier of Impact Evaluation of Personal Data Processing and the attached documents.

Recipients:	**FOR THE ORGANIZATION OR ENTERPRISE**
- As above;	*(sign, specify full name, seal)*
....	

[1] Name of organization or enterprise

Form No. 05

NAME OF ORGANIZATION	**SOCIALIST REPUBLIC OF VIETNAM**
	Independence – Freedom – Happiness
_____	_____
No.: …	*…., date .....*

NOTICE
ON CHANGE OF CONTENTS OF RECORD ……[1]

To: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention under the Ministry of Public Security)

In compliance with regulations on personal data protection, ...[2] submits to the Ministry of Public Security a Personal Data Processing Impact Assessment Record as follows:

1. Information on organization or enterprise

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

- Head office address: .....

- Address of the transaction office: .....

- Establishment Decision / Enterprise Registration Certificate / Business Registration Certificate / Investment Certificate No.: ..... issued by .... on ..... in .....

- Telephone: .....Website .....

- Person in charge of personal data protection:

Full name: .....

Position: .....

Contact telephone (landline and mobile): .....

Email: .....

2. Brief description of changes to contents of the Record

- Content(s) of change:.....

- Reason(s) for change: .....

3. Attached documents:

1. ……

2. ……

4. Undertaking

(Name of agency, organization, enterprise) hereby undertakes to assume responsibility before the laws for the accuracy and legality of the contents of change and the attached documents.

Recipients:
- As above;
....

FOR THE ORGANIZATION OR ENTERPRISE
(sign, specify full name, seal)

---

[1] Record name: Record of Personal Data Processing Impact Assessment or Record of Impact Assessment of Cross-border Transfer of Personal Data.

[2] Name of organization or enterprise.

Form No. 06

NAME OF ORGANIZATION	**SOCIALIST REPUBLIC OF VIETNAM**
_____	**Independence – Freedom – Happiness**
No.: …	_____
	...., date .....

RECORD OF IMPACT ASSESSMENT OF CROSS-BORDER TRANSFER OF PERSONAL DATA

To: Ministry of Public Security

(Department of Cybersecurity and Hi-Tech Crime Prevention under the Ministry of Public Security)

In compliance with regulations on personal data protection, ...[1] submits to the Ministry of Public Security a Record of Impact Assessment of Cross-border Transfer of Personal Data as follows:

1. Information on organization or enterprise

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

- Head office address: .....

- Address of the transaction office: .....

- Establishment Decision / Enterprise Registration Certificate / Business Registration Certificate / Investment Certificate No.: ..... issued by .... on ..... in .....

- Telephone: ..... Website .....

- Person in charge of personal data protection:

Full name: .....

Position: .....

Contact telephone (landline and mobile): .....

Email: .....

2. Record of Impact Assessment of Cross-border Transfer of Personal Data

1. ……

2. ……

3. Undertakings

(Name of agency, organization, enterprise) hereby undertakes to assume responsibility before the laws for the accuracy and legality of the Record of Impact Assessment of Cross-border Transfer of Personal Data and the attached documents.

Recipients:
- As above;
....

FOR THE ORGANIZATION OR ENTERPRISE
(sign, specify full name, seal)

[1] Name of organization or enterprise