THE GOVERNMENT SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

No.: 13/2023/NĐ-CP *Hanoi, 17 April 2023*

DECREE
On personal data protection

Pursuant to the Law on Organization of the Government dated 19 June 2015;and the Law amending and supplementing a number of 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 03 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. Governing scope and applicable subjects

1. This Decree provides the personal data protection and responsibilities of relevant agencies, organizations and individuals for personal data protection. 2. This Decree applies to:

a) Vietnamese agencies, organizations and individuals;

b) Foreign agencies, organizations and individuals being based in Vietnam; c) Vietnamese agencies, organizations and individuals operating overseas; d) Foreign agencies, organizations and individuals directly participating in or involved in the personal data processing in Vietnam.

Article 2. Interpretation of terms

In this Decree, the terms below shall be construed as follows:

1. Personal data means any information that is expressed in the form of symbol,

text, digit, image, sound or in similar forms in electronic environment that is associated with a particular natural person or helps identify a particular natural person. Personal data includes basic personal data and sensitive personal data.

2. Personally identifiable information means any information that is formed from the activities of an individual and, when used with other maintained data and information, can identify such particular natural person.

3. Basic personal data includes:

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

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

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;

g) Phone number, people's identity card number, personal identification number, passport number, driver's license number, license plate number, personal tax identification number, social insurance number, health insurance card number; h) Marital status;

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

k) Information on personal digital accounts; personal data that reflects activities or history of activities in cyberspace;

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

4. Sensitive personal data means personal data associated with an individual's privacy that, when being infringed upon, shall cause a direct effect on the legitimate rights and interests of such individual, including:

a) Political and religious views;

b) Information on health condition and private life that is documented in medical records, excluding information on blood type;

c) Information relating to racial origin and ethnic origin;

d) Information on inherited or acquired genetic characteristics of such individual;

dd) Information on distinctive physical attributes and biological characteristics of such individual;

e) Information on sex life and sexual orientation of such individual; g) Data about crimes and criminal acts that are obtained and kept by law enforcement agencies;

h) Customer information held by credit institutions, foreign bank branches, intermediary payment service providers and other authorized organizations, including: customer identification information as stipulated by law, information on accounts, information on deposits, information on deposited properties, information on transactions, information on organizations or individuals being the securing parties at credit institutions, bank branches and intermediary payment service providers;

i) Personal location data that are identified through positioning services; k) Other personal data that are regarded by law as specific and requires necessary security measures.

5. Personal data protection means any act of prevention, detection, suppression and handling of violations regarding personal data in accordance with the law. 6. Data subject means an individual identified by personal data.

7. Personal data processing means one or more operations that affect personal data, such as: obtaining, recording, analysis, confirmation, storage, alteration, publicity, combination, access, retrieval, recovery, encryption, decryption, duplication, sharing, transmission, provision, transfer, deletion, destruction of personal data or other relevant operations.

8. Consent of the data subject means an explicit, voluntary and affirmative expression of the permission of a data subject for the data processing of their personal data.

9. Personal Data Controller means an organization or individual that decides on the purpose and means of personal data processing.

10.Personal Data Processor means an organization or individual that performs

the processing of the data on behalf of a Personal Data Controller under a contract or

agreement with such Personal Data Controller.

11.Personal Data Controller and Processor means an organization or individual that decides on the purpose and means of processing and simultaneously and directly performs the personal data processing.

12.Third Party means an organization or individual other than the Data Subject, Personal Data Controller, Personal Data Processor and Personal Data Controller and Processor that is authorized to process personal data.

13.Automated personal data processing means a form of personal data processing performed by use of electronic means in order to evaluate, analyze and predict the activities of a particular natural person, such as: habits, preferences, level of reliability, behaviors, locations, tendencies, capacities and others.

14.Cross-border transfer of personal data means any activity involving the use of cyberspace, electronic equipment, electronic 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 of a location outside the territory of the Socialist Republic of Vietnam to process a Vietnamese citizen's personal data of, including:

a) Organizations, enterprises or individuals transferring personal data of Vietnamese citizens to organizations, enterprises or management bodies located overseas for processing in accordance with the purposes consented by the data subjects;

b) Processing of personal data of Vietnamese citizens by use of automated systems located outside the territory of the Socialist Republic of Vietnam by the Personal Data Controller, Personal Data Controller and Processor or Personal Data Processor in accordance with the purposes consented by the data subjects.

Article 3. Principles of personal data protection

1. Personal data shall be processed in accordance with applicable regulations of the law.

2. Data subjects shall be made aware of any operation relating to the processing of their personal data, unless otherwise provided by law.

3. Personal data shall be processed only for the purposes registered and announced by the Personal Data Controller, Personal Data Processor, Personal Data Controller and Processor or Third Party in relation to the personal data processing.

4. Personal data that are obtained must be appropriate and limited to 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 shall be updated and supplemented in accordance with the purposes of processing.

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

7. Personal data shall be kept only for a term appropriate with the purposes of data processing, unless otherwise provided by law.

8. The Personal Data Controller and Personal Data Controller and Processor shall be responsible for complying with the principles of data processing stipulated in clauses 1 to 7 of this Article and demonstrate their compliance with such principles of data processing.

Article 4. Handling of violations of regulations on personal data protection

Agencies, organizations and individuals that commit violation of the regulations on personal data protection, depending on the severity, may be subject to disciplinary, administrative or criminal penalty in accordance with applicable regulations. **Article 5. State management over personal data protection**

The Government shall unify the State management over personal data protection. The contents of State management over personal data protection include: 1. To submit to the State agencies with the authority to promulgate or promulgate intra vires legal normative documents and direct and organize the implementation of legal normative documents on personal data protection. 2. To develop and organize the implementation of strategies, policies, projects, schemes, programs and plans on personal data protection.

3. To provide guidelines for agencies, organizations and individuals on measures, processes and standards for personal data protection in accordance with the law.

4. To implement propagation and education of the law on personal data

protection; communication and dissemination of knowledge and skills on personal data protection.

5. To build, train and foster the officials, public employees and persons assigned to be in charge of personal data protection.

6. To inspect and examine the implementation of the law on personal data protection; settle claims and denunciations and handle violations of the law on personal data protection as prescribed by law.

7. To submit statistics, communication and report on the situation of personal data protection and the implementation of the law on personal data protection to competent State agencies.

8. To engage in the international cooperation on personal data protection.

Article 6. Application of the Decree on personal data protection, relevant laws and International treaties

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

Article 7. International cooperation on personal data protection 1. To develop a mechanism for international cooperation to facilitate the effective enforcement of the law on personal data protection.

2. To engage in mutual legal assistance in the protection of personal data protection of other countries, including notification, requests, claims, investigation assistance and information exchange, with appropriate measures for personal data protection.

3. To organize conferences, seminars, scientific research and activities for promotion of international cooperation in law enforcement for the personal data protection.

4. To organize bilateral and multilateral meetings, and exchange experience on law-making and practice of personal data protection.

5. To perform technology transfer for the personal data protection.

Article 8. Prohibited acts

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

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

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

4. Obstructing the personal data protection by competent agencies. 5. Taking advantage of the personal data protection activities to violate the law.

Chapter II
PERSONAL DATA PROTECTION

Section 1
RIGHTS AND OBLIGATIONS OF DATA SUBJECTS

Article 9. Rights of data subjects

1. Right to be informed

Data subjects shall be made aware of any operation of processing of their personal data unless otherwise provided by law.

2. Right to consent

Data subjects may or may not consent to the processing of their personal data, unless otherwise provided by Article 17 hereof.

3. Right to access [to information]

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

4. Right to withdraw consent

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

5. Right to delete data

Data subjects may delete or request for deletion of their personal data, unless otherwise provided by law.

6. Right to restrict data processing

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

b) The restriction of data processing shall be effected within 72 hours after the request of the data subjects for all the personal data requested for restriction of data processing by the data subjects, unless otherwise provided by law.

7. Right to provision of data

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

8. Right to object to data processing

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

b) The Personal Data Controller and Personal Data Controller and Processor shall implement the request of the Data Subject within 72 hours after receiving such, unless otherwise provided by law.

9. Right to complain, denounce and/or initiate lawsuits

Data subjects may complain, denounce or initiate lawsuits in accordance with the law.

10.Right to claim damages

Data subjects are entitled to claim damages in accordance with the law upon violation of the regulations on personal data protection, unless otherwise agreed by the parties or prescribed by law.

11.Right to self-defense

Data subjects are entitled to self-defense in accordance with the Civil Code,

other relevant laws, and this Decree, or may request competent agencies or organizations to implement the measures for protection of civil rights as prescribed in Article 11 of the Civil Code.

Article 10. Obligations of data subjects

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

2. To respect and protect others' personal data.

3. To fully and accurately provide personal data upon giving consent to the personal data processing.

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

5. To comply with the law on personal data protection and participate in the prevention of and fight against violations of the regulations on personal data protection.

Section 2
PERSONAL DATA PROTECTION
IN PERSONAL DATA PROCESSING

Article 11. Consent of the data subject

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

2. The consent of the data subject shall only be valid when the data subject volunteers and fully knows the following:

a) Type of personal data to be processed;

b) Purpose(s) of the personal data processing;

c) Organizations and/or individuals entitled to the personal data processing;

d) Rights and obligations of data subjects

3. The consent of the data subject shall be clearly and specifically expressed by written instrument, by voice, by ticking the consent box, by text message, by selecting technical settings, or by another action that demonstrates the same.

4. The consent shall be made for a single purpose. Upon multiple purposes, the

Personal Data Controller and Personal Data Controller and Processor shall list the purposes for the data subjects to give consent to one or more of the stated purposes.

5. The consent of the data subject shall be expressed in a format that can be printed and/or reproduced in writing, including in electronic or verifiable formats. 6. The data subjects' silence or non-response shall not be regarded as their consent.

7. The data subjects may give a partial or conditional consent.

8. With regards to the processing of sensitive personal data, the data subjects

shall be informed that the data to be processed is sensitive personal data. 9. The consent of the data subject shall be valid until otherwise decided by the data subjects or as requested in writing by a competent state authority. 10.In the event of a dispute, the Personal Data Controller and/or the Personal Data Controller and Processor shall be responsible for demonstrating the consent of the data subject.

11.By means of authorization under the Civil Code, an organization and/or individual may act on behalf of a data subject to carry out procedures in relation to processing of the personal data of the data subject with the Personal Data Controller or the Personal Data Controller and Processor in case the data subject has acknowledged and given consent thereto as prescribed in clause 3 of this Article, unless otherwise provided by law.

Article 12. Withdrawal of consent

1. The withdrawal of consent does not affect the legality of the data processing to which the consent was given prior to the withdrawal.

2. The withdrawal of consent shall be expressed in a format that can be printed and/or reproduced in writing, including in electronic or verifiable formats. 3. Upon receipt of the data subject's request for withdrawal of consent, the Personal Data Controller and/or the Personal Data Controller and Processor shall notify the data subject of possible consequences and damage upon withdrawal of consent. 4. Following the implementation of clause 2 of this Article, the Data controller, Data processor, Data controller and processor, and the Third Party must cease and request relevant organizations and/or individuals to cease the processing of the data to which the consent has been withdrawn by the data subject.

Article 13. Notification of the personal data processing

1. One notification shall be given before the personal data processing. 2. The notification to be given to a data subject on the processing of his/her personal data shall cover the following:

a) Purpose(s) of the processing;

b) Type of personal data to be processed according to the purpose(s) specified in point a of clause 2 of this Article;

c) Method of processing;

d) Information on other organizations and/or individuals who are relevant to the processing purpose(s) specified in Point a, clause 2 of this Article; dd)Potential and unwanted consequences and/or damage;

e) Starting time and ending time of the data processing.

3. The notification to be given to the data subject shall be made in a format that can be printed and/or reproduced in writing, including in electronic or verifiable formats.

4. The Personal Data Controller and Personal Data Controller and Processor shall not be required to comply with clause 1 of this Article in the following cases: a) The data subject has acknowledged and given consent to all of the contents specified in clauses 1 and 2 of this Article before authorizing the Personal Data Controller and Personal Data Controller and Processor to collect his/her personal data in accordance with Article 9 hereof;

b) The personal data is subject to the processing by a competent state agency for the operation of the state agency in accordance with the law;

Article 14. Provision of personal data

1. Data subjects are entitled to request the Personal Data Controller and Personal Data Controller and Processor to provide them with their own personal data. 2. The Personal Data Controller and Personal Data Controller and Processor are entitled to:

a) Provide the data subjects' personal data to other organizations and/or individuals with the consent of the data subjects, unless otherwise provided by law; b) Provide, on behalf of the data subjects, the data subjects' personal data to other

organizations and/or individuals under the consent of the data subjects to such representation and authorization, unless otherwise provided by law. 3. The data subjects' personal data shall be provided by the Personal Data Controller or Personal Data Controller and Processor within 72 hours upon request by the data subjects, unless otherwise provided by law.

4. The Personal Data Controller and Personal Data Controller and Processor shall not provide personal data in the case that:

a) The national defense, security, and/or social order and safety may be compromised.

b) The provision of 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 or give consent for representation or authorization to receive his/her personal data.

5. Form of request for provision of personal data

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

The person receiving the request is responsible for guiding the requesting organization or individual to complete the Request for provision of personal data. In case the requesting organization or individual is illiterate or disabled and cannot complete the request, the person receiving the Request for provision of personal data shall be responsible for assisting him/her to complete the Request for provision of personal data;

b) Send the Request for provision of personal data in Form No. 01 and 02 set out in the Appendices hereof via electronic network, by post, by facsimile to the Personal Data Controller, the Personal Data Controller and Processor.

6. The Request for provision of personal data must be presented in Vietnamese, including the following main details:

a) Full name; place of residence, address; identity card number, citizen identification card or passport number of the person who requests the personal data;

fax number, telephone, email address (if any);

b) The requested personal data, specifying the name of documents, records, documents;

c) Form of provision of personal data;

d) The reason and purpose of requesting the provision of personal data. 7. In case of request for provision of personal data specified in clause 2 of this Article, the request must be accompanied with a written consent of the concerned individual or organization.

8. Receipt of requests for provision of personal data

a) The Personal Data Controller, the Personal Data Controller and Processor are responsible for receiving requests for provision of personal data and monitoring of the process and the list of provision of personal data per request.

b) In case the requested personal data are not under its authority, the Personal Data Controller, the Personal Data Controller and Processor receiving the request must notify and guide the requesting organization or individual to make request to the competent authority or expressly notify its inability to provide such personal data.

9. Handling of requests for provision of personal data

Upon receipt of a valid request for provision of personal data, the Personal Data Controller, the Personal Data Controller and Processor is responsible for providing the personal data, notifying the time limit, location, form of provision of the personal data; actual expenses for printing, photocopying, sending information via postal and facsimile services (if any) and payment methods and terms; provide the personal data according to the order and procedures specified in this Article.

Article 15. Correction of personal data

1. Data subjects shall be entitled to:

a) Have access to view and correct their personal data collected by the Personal Data Controller or the Personal Data Controller and Processor under their consent, unless otherwise provided by law;

b) Request the Personal Data Controller or the Personal Data Controller and Processor to correct their personal data where the personal data cannot be corrected

directly [by the data subjects] for technical reasons or for other reasons.

2. The Personal Data Controller or the Personal Data Controller and Processor shall make correction of the data subjects' personal data as soon as possible after the data subjects have given consent thereto or in accordance with specialized laws. In the case that such practice is impracticable, there shall be a notification thereof to the data subjects after 72 hours of receiving the data subjects' request for correction of their personal data;

3. The Personal Data Processor and the Third Party may correct the data subjects' personal data after obtaining the written consent of the Personal Data

Controller or Personal Data Controller and Processor with the awareness that the data subjects have given the same;

Article 16. Storage, deletion, and destruction of personal data

1. Data subjects shall be entitled to request the Personal Data Controller or the Personal Data Controller and Processor to delete their personal data in the following cases:

a) The data subjects have found it no longer necessary for their personal data to be collected for the purpose(s) consented by the data subjects and accept possible damage upon requesting for data deletion;

b) Withdrawal of consent;

c) There is objection to the data processing and the Personal Data Controller or the Personal Data Controller and Processor has no legitimate reason to continue the processing;

d) The personal data processing is not for the consented purpose(s) or is in violation of the law;

dd) The personal data shall be deleted in accordance with the law; 2. The deletion of personal data shall not come into effect once requested by the data subjects in the following cases:

a) The deletion of data is not permitted by law;

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

c) The personal data has been made public in accordance with the law; d) The personal data is processed to serve legal requirements, scientific research and statistics in accordance with the law;

dd) A state of emergency has been proclaimed on the national defense, national security, social order and safety, major disasters, dangerous epidemics; there are dangers threatening the national security and defense but not to the extent of proclaiming the state of emergency; in order to prevent and fight against riots and terrorism, to prevent and fight against crimes and law violations;

e) It is required to respond to an emergency threatening the life, health or safety of the data subject or other individual(s).

3. Upon partial or complete division, merger, consolidation, dissolution of an enterprise, the personal data shall be transferred in accordance with the law. 4. Upon partial or complete division, merger of an agency, organization, administrative unit and re-organization or transformation of form of ownership of a state enterprise, the personal data shall be transferred in accordance with the law. 5. The deletion of data shall be implemented within 72 hours after the request of the data subjects for all the personal data collected by the Personal Data Controller or the Personal Data Controller and Processor, unless otherwise provided by law. 6. The Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, and Third Party shall store personal data in a form appropriate for their operations and take measures to protect personal data in accordance with the law.

7. The Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, and Third Party shall make permanent deletion [of personal data] in the following cases:

a) The data has been processed for improper purposes or the purpose(s) consented by the data subjects for the data processing has been fulfilled; b) The storage of personal data is no longer necessary for the operation of the Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, and Third Party;

c) The Personal Data Controller, Personal Data Controller and Processor,

Personal Data Processor, or Third Party is dissolved or no longer operates or declares bankruptcy or has its business operations terminated in accordance with the law.

Article 17. Personal data processing without requiring the consent of the data subject

1. In case of emergency, the relevant personal data may be processed immediately to protect the life and health of the data subject or others. The Personal Data Controller, Personal Data Processor, Personal Data Controller and Processor, and Third Party shall be responsible for demonstrating such situation.

2. To conduct disclosure of personal data in accordance with the law.

3. To serve the processing by a state competent authority in a state of emergency

on the national defense, national security, social order and safety, major disasters, dangerous epidemics; where there are dangers threatening the national security and defense but not to the extent of proclaiming the state of emergency; or to prevent and fight against riots and terrorism, to prevent and fight against crimes and violations of the law in accordance with the law.

4. To fulfill the contractual obligations of the data subject with relevant agencies, organizations and/or individuals in accordance with the law.

5. To serve the operations of state agencies as prescribed by specialized laws.

Article 18. Personal data processing obtained from audio and video recording in public locations

Competent agencies and organizations may record audio and/or video and process personal data obtained from audio and video recording activities in public locations for the protection of the national security, social order and safety, and their legitimate rights and interests in accordance with the law without the consent of the data subject. Upon performance of such audio and/video recording, the competent agencies and organizations shall be responsible for notifying the data subjects to understand that they are being recorded, unless otherwise provided by law.

Article 19. Personal data processing of persons declared missing or dead 1. The personal data processing relating to the personal data of a person declared missing or dead shall be subject to the consent of his/her spouse or adult children, or his/her

parents if he/she has no spouse or child, except for the cases specified in Articles 17 and 18 hereof.

2. In the absence of all the persons mentioned in clause l of this Article, it is regarded as to have no consent.

Article 20. Processing of children's personal data

1. The processing of children's personal data shall always follow the principle of protection of the rights and for the best interests of children;

2. The processing of children's personal data shall be subject to the consent of the children in the case where they are full 7 years old or the consent of their parent or guardian as prescribed, except in the case specified in Clause 1, Article 17 hereof. The Personal Data Controller, Personal Data Processor, Personal Data Controller and

Processor, and Third Party shall verify the age of the children before proceeding with the personal data processing of children.

3. The personal data of children shall be subject to suspension of processing, permanent deletion, or destruction in the following cases:

a) The data has been processed for improper purposes or has fulfilled the purpose(s) consented by the data subjects, unless otherwise provided by law; b) The consent for the personal data processing of the children has been withdrawal by their parents or guardians, unless otherwise provided by law; c) It is requested by a competent authority where there are sufficient grounds to prove that the personal data processing affects children's legitimate rights and interests, unless otherwise provided by law.

Article 21. Personal data Protection in the marketing and advertisement business

1. Organizations and/or individuals conducting the marketing and advertisement business may only use the personal data of their customers collected during their operations to conduct marketing and advertisement business upon having the consent of the data subject.

2. The processing of customers' personal data for the marketing and advertisement business shall be subject to the consent of the customers, on the ground

that the customers are aware of the content, method, form and frequency of product introduction.

3. Organizations and/or individuals providing services of product marketing and advertisement shall be responsible for proving the use of personal data of the customers to whom a product is introduced in accordance with clauses 1 and 2 of this Article.

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

1. Organizations and/or individuals involved in the personal data processing shall apply measures for personal data protection to prevent unauthorized collection of personal data from their system, equipment and services.

2. It is violation of law to set up software systems, technical measures or

organize the collection, transfer, purchase and sale of personal data without the consent of the data subject.

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

1. Upon detection of a violation of the regulations on personal data protection, the Personal Data Controller or the Personal Data Controller and Processor shall notify the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) within 72 hours of the occurrence of the violation in Form No. 03 set out in the Appendix hereof. In case of notifying after 72 hours, the reason for delay or late notification must be included.

2. The Personal Data Processor shall notify the Personal Data Controller as soon as possible upon becoming aware of a violation of the regulations on personal data protection.

3. The notification of violation of the regulations on personal data protection shall include the following:

a) Descriptions of the nature of the violation of the regulations on personal data protection, including: time, location, acts, organization, individual, types of personal data and the amount of related data;

b) Contact details of the staff assigned to data protection or organizations or individuals responsible for personal data protection;

c) Descriptions of the possible consequences and damage caused by the violation of the regulations on personal data protection

d) Descriptions the measures put in place to handle and minimize the harm of the violation of the regulations on personal data protection

4. In case the contents specified in clause 3 of this Article cannot be fully notified, the notification may be made in multiple installments and stages. 5. The Personal Data Controller and/or Personal Data Controller and Processor shall prepare a written minutes confirming the occurrence of the violation of the regulations on personal data protection, and coordinate with the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) to handle the violation.

6. Organizations and/or individuals shall notify the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) upon detection of the following cases:

a) There are violations of the law with respect to personal data;

b) The personal data is processed for improper purposes or not in accordance with the original agreement between the Data Subject and the Personal Data Controller and/or the Personal Data Controller and Processor or in violation of the law;

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

d) Other cases as prescribed by law.

Section 3

IMPACT ASSESSMENT AND CROSS-BORDER TRANSFER OF PERSONAL DATA

Article 24. Assessment of the impact of personal data processing 1. The Personal Data Controller and Personal Data Controller and Processor shall prepare and maintain a Dossier for assessment of the impact of personal data processing from the commencement of the personal data processing. The Dossier for assessment of the

impact of personal data processing of the Personal Data Controller and Personal Data Controller and Processor shall include: a) Information and contact details of the Personal Data Controller and Personal Data Controller and Processor;

b) Full name and contact details of the organization tasked with the personal data protection and the staff responsible for the personal data protection of the Personal Data Controller and Personal Data Controller and Processor;

c) Purpose(s) of the personal data processing;

d) Types of personal data to be processed;

dd) Organizations and/or individuals receiving personal data, including organizations and/or individuals outside the Vietnamese territory;

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

g) Time for personal data processing; estimated time for removal, destruction

of personal data (if any);

h) Descriptions of the applied measures for personal data protection; i) Assessment of the impact of personal data processing; potential and unwanted consequences and/or damage, and measures for minimization or elimination thereof.

2. The Personal Data Processor shall prepare and maintain a Dossier for assessment of the impact of the personal data processing under an agreement with the Personal Data Controller. The Dossier for assessment of the impact of personal data processing of the Personal Data Processor shall include:

a) Information and contact details of the Personal Data Processor; b) Full name and contact details of the organization assigned to proceed the personal data processing and the Personal Data Processor' staff processing the personal data;

c) Descriptions of the processing activities and types of personal data to be processed under an agreement with the Personal Data Controller;

d) Time for personal data processing; estimated time for removal, destruction of personal data (if any);

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

e) General descriptions of the applied measures for personal data protection; f) Potential and unwanted consequences and/or damage, and measures for minimization

or elimination thereof.

3. The Dossier for assessment of the impact of personal data processing specified in clauses 1 and 2 of this Article shall be prepared in a legally valid document of the Personal Data Controller, Personal Data Controller and Processor, or Personal Data Processor.

4. The dossier for assessment of the impact of personal data processing shall be made available at all times for the inspection and evaluation by the Ministry of Public Security and 01 original copy thereof in Form No. 04 set out in the Appendix hereof shall be submitted to the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) within 60 days from the date of processing of personal data.

5. The Ministry of Public Security (Department of Cybersecurity and Hi-tech

Crime Prevention) shall perform the evaluation and may request the Personal Data Controller, Personal Data Controller and Processor, and/or Personal Data Processor to complete the Dossier for assessment of the impact of personal data processing in case the Dossier is incomplete and not correct to the provisions.

6. The Personal Data Controller, Personal Data Controller and Processor, and/or Personal Data Processor shall update and supplement the Dossier for assessment of the impact of personal data processing upon having changes to the content of the Dossier submitted to the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) in Form No. 05 set out in the Appendix hereof.

Article 25. Cross-border transfer of personal data

1. The personal data of Vietnamese citizens may be transferred abroad in case the Cross-border data transferrer has prepared a Dossier for assessment of the impact of cross-border transfer of personal data and conducted the procedures specified in clauses 3, 4 and 5 of this Article. The cross-border data transferrer includes the Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, and Third Party.

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

a) Information and contact details of the Cross-border data transferrer as well as the Receiver of the personal data of Vietnamese citizens;

b) Full name and contact details of the organization and/or individual in charge of the Data transferrer in relation to transfer and receipt of the personal data of Vietnamese citizens;

c) Descriptions and explanations of the objectives of the personal data processing of Vietnamese Citizens following the cross-border transfer; d) Descriptions and clarification of the type of personal data to be subject to the cross-border transfer;

dd) Descriptions and express statement of compliance with the regulations on personal data protection specified herein, detailing the applied measures for personal data protection.

e) Assessment of the impact of personal data processing; potential and

unwanted consequences and/or damage, and measures for minimization or elimination thereof.

g) The consent of the data subject as prescribed in Article 11 hereof, which is given based on a full awareness of the mechanism for feedback and claim upon occurrence of issues or requests;

h) A document showing the binding and responsibility for the personal data processing between the organizations and/or individuals transferring and receiving the personal data of Vietnamese citizens.

3. The dossier for assessment of the impact of cross-border transfer of personal data shall be made available at all times for the inspection and evaluation by the Ministry of Public Security.

The cross-border data transferrer shall submit 01 original copy thereof to the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) in Form No. 06 set out in the Appendix hereof within 60 days from the date of processing of personal data.

4. The data transferrer shall notify and submit the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) the information on the data transfer and the contact details of the responsible organization and/or individual in writing upon the successful completion of the data transfer.

5. The Ministry of Public Security (Department of Cybersecurity and Hi-tech

Crime Prevention) shall perform the evaluation and may request the cross-border data transferrer to complete the Dossier for assessment of the impact of cross-border transfer of personal data in case the Dossier is incomplete and not correct to the provisions.

6. The cross-border data transferrer shall update and supplement the Dossier for assessment of the impact of cross-border transfer of personal data upon having changes to the content of the Dossier submitted to the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) in Form No. 05 set out in the Appendix hereof. The time limit for completion of the dossier for the cross-border data transferrer
is 10 days from the date of such request.

7. Depending on the specific situation, the Ministry of Public Security shall decide to inspect the cross-border transfer of personal data once a year, unless a

violation of the regulations on personal data protection prescribed herein is detected or there is an incident of disclosure and loss of personal data of Vietnamese citizens. 8. The Ministry of Public Security shall decide to request the cross-border data transferrer to cease the cross-border transfer of personal data in cases where: a) It is detected that the transferred personal data is used for activities that violate the interests and national security of the Socialist Republic of Vietnam; b) The cross-border data transferrer fails to comply with the provisions of Clauses 5 and 6 of this Article;

c) The personal data of a Vietnamese citizen is disclosed or lost.

Section 4

MEASURES AND CONDITIONS FOR ENSURING THE PERSONAL DATA PROTECTION

Article 26. Measures for the personal data protection

1. Measures for the personal data protection shall be implemented from the commencement and throughout the personal data processing.

2. Measures for the personal data protection shall include:

a) Management measures taken by organizations and/or individuals in relation

to the personal data processing;

b) Technical measures taken by organizations and/or individuals in relation to the personal data processing;

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. Protection of basic personal data

1. To apply the measures specified in clause 2, Article 26 hereof.

2. To develop and promulgate the regulations on personal data protection, specifying the tasks to be completed in accordance with this Decree. 3. To encourage the application of standards for personal data protection appropriate to the fields, industries and activities in relation to the personal data

processing.

4. To check the systems, facilities and equipment serving the personal data processing for network security before the processing, permanent deletion or destruction of devices containing personal data.

Article 28. Protection of sensitive personal data

1. To apply the measures specified in clause 2, Articles 26 and 27 hereof. 2. To designate a department functioned with personal data protection, to appoint personnel in charge of personal data protection and communicate the information on such department and individual in charge of personal data protection with the Specialized Agency for the Personal Data Protection. In the case that the Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, and Third Party are individuals, to communicate the information of such individual.

3. To notify the data subjects that their sensitive personal data shall be processed, except for the cases specified in clause 4 Article 13, Article 17 and Article 18 hereof.

Article 29. Specialized Agency for the Personal Data Protection and the National Personal Data Protection Portal

1. The Specialized Agency for the Personal Data Protection is the Department of Cybersecurity and Hi-tech Crime Prevention, Ministry of Public Security, which shall be responsible for assisting the Ministry of Public Security in performing the state management of personal data protection.

2. The National Personal Data Protection Portal:

a) To provide information on the guidelines, directions and policies of the Party and the State's laws on personal data protection;

b) To propagate, disseminate the policies and laws on personal data protection; c) To update the information and status of personal data protection; d) To receive information, dossiers and data on the personal data protection on cyberspace;

dd) To provide information on the results of assessment of the personal data protection by relevant agencies, organizations and individuals;

e) To receive notifications of violations of the regulations on personal data protection;

g) To give warnings and coordinate in warning about risks and acts of infringement of personal data in accordance with the law;

h) To handle violations in relation to personal data protection in accordance with the law;

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

Article 30. Conditions for ensuring the personal data protection

1. Personal data protection force:

a) The personal data protection task force is located at the Specialized Agency for the Personal Data Protection.

b) A department and/or personnel in charge of personal data protection shall be appointed in agencies, organizations and enterprises to ensure compliance with the regulations on personal data protection.

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

d) The Ministry of Public Security shall develop specific programs and plans to

develop human resources for the personal data protection.

2. Agencies, organizations and individuals shall be responsible for propagating and disseminating knowledge and skills, and raising awareness of personal data protection for [the other] agencies, organizations and individuals.

3. The facilities and operating conditions for the Specialized Agency for the Personal Data Protection shall be ensured.

Article 31. Funds for ensuring the personal data protection

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

2. Funds for the personal data protection of State agencies shall be guaranteed by the State budget and arranged in the annual State budget estimate. The management

and use of State budget funds shall accord with the law on State budget. 3. Funds for the personal data protection of organizations and enterprises shall be arranged and implemented by the organizations and enterprises themselves in accordance with applicable regulations.

Chapter III
RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS, AND INDIVIDUALS

Article 32. Responsibilities of the Ministry of Public Security

1. To assist the Government to unify the state management of personal data protection.

2. To guide and implement the personal data protection, protect the rights of data subjects against violations of the law on personal data protection, and propose the promulgation of Standards for personal data protection and applicable recommendations.

3. To develop, manage and operate the National Personal Data Protection Portal;

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

5. To receive dossiers, forms and information on the personal data protection as prescribed herein.

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

7. To inspect, examine, settle claims and/or denunciations, and handle violations of the 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, presses, and organizations and enterprises operating in the field under its management to implement the personal data protection according to the provisions hereof.

2. To develop, guide and implement measures for personal data protection, and to ensure cyber information security for personal data in the operations of information and communication according to the assigned tasks and functions.

3. To cooperate 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, handle violations and apply the regulations on personal data protection to agencies, organizations and individuals under its management in accordance with the law and the assigned tasks and functions. **Article 35. Responsibilities of the Ministry of Science and Technology** 1. To coordinate with the Ministry of Public Security in developing the Standards for personal data protection and recommendations for the application of the Standards for personal data protection.

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 the state management of personal data protection for the sectors

and fields under their management in accordance with the law on personal data protection.

2. To develop and implement the contents and tasks of personal data protection prescribed herein.

3. To supplement the provisions on personal data protection in the development and implementation of tasks of ministries and branches.

4. To allocate funds for the personal data protection according to the current delegation of budget management.

5. To issue a National Open Data Directory in accordance with applicable regulations on personal data protection.

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

1. To perform the state management of personal data protection for the sectors

and fields under their management in accordance with the law on personal data protection.

2. To implement the regulations on personal data protection herein. 3. To allocate funds for the personal data protection according to the current delegation of budget management.

4. To issue a National Open Data Directory in accordance with applicable regulations on personal data protection.

Article 38. Responsibilities of the Personal Data Controller

1. To implement organizational and technical measures as well as appropriate safety and security measures to demonstrate the compliance of the data processing with the law on personal data protection, and to review and update these measures, as necessary.

2. To record and store the system log of personal data processing. 3. To notify the violations of regulations on personal data protection as prescribed in Article 23 of this Decree.

4. To make proper selection of Personal Data Processor with express task assignments and work only with a Personal Data Processor having in place appropriate

security measures.

5. To guarantee the rights of data subjects as prescribed in Article 9 hereof. 6. To be responsible to the data subjects for damage caused by the personal data processing.

7. To coordinate with the Ministry of Public Security and competent state agencies in the personal data protection, and 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. To receive personal data only after having signed a contract or agreement on data processing with the Personal Data Controller.

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

3. To fully implement measures for personal data protection as prescribed herein and other relevant legal documents.

4. To be responsible to the data subjects for damage caused by the personal data processing.

5. To delete and/or return all personal data to the Personal Data Controller after completion of the data processing.

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

Article 40. Responsibilities of the Personal Data Controller and Processor

To fully comply with the regulations on responsibilities for personal data processing as prescribed herein.

Article 41. Responsibilities of Third Parties

To fully comply with the regulations on responsibilities for personal data processing as prescribed herein.

Article 42. Responsibilities of relevant organizations and individuals 1. To take measures for protection of their own personal data, and take responsibility for the accuracy of the personal data provided.

2. To comply with the regulations on personal data protection herein. 3. To timely notify the Ministry of Public Security of violations in relation to personal data protection.

4. To cooperate with the Ministry of Public Security in handling violations in relation to personal data protection.

Chapter IV
IMPLEMENTATION

Article 43. Effectiveness

1. This Decree shall take effect as of 01 July 2023.

2. Micro-enterprises, small enterprises, medium-sized enterprises, and start-up enterprises shall be entitled to choose to be exempt from the provisions on assignment of the persons and department to be in charge of personal data protection for the first 02 years from the date of establishment.

3. Micro-enterprises, small enterprises, medium-sized enterprises, and start-up enterprises directly engaged in the personal data processing shall not apply clause 2 of

this Article.

Article 44. Implementation responsibilities

1. The Minister of Public Security shall urge, inspect and guide the implementation hereof.

2. The Ministers, Heads of ministerial-level agencies, Heads of Government agencies, Chairpersons of People's Committees of provinces and centrally-run cities shall be responsible for the implementation hereof./.

ipients:
- Secretariat of the Communist Party of Vietnam;
- The Prime Minister and Deputy Prime Ministers;
- Ministries, ministerial-level agencies and Government agencies; - People's Councils, People's Committees of provinces and centrally-run cities;
- Office of the Central Committee and Boards of the Communist Party of Vietnam;
- Office of the General Secretary;
- Office of the President;
- Ethnic Council and Committees of the National Assembly; - Office of the National Assembly;
- Supreme People's Procuracy;
- Supreme People's Court;
- The State Audit Office of Vietnam;
- National Financial Supervisory Commission;
- Vietnam Bank for Social Policies;
- Vietnam Development Bank;
- The Central Committee of the Vietnam Fatherland Front; - Central agencies of unions;
- The Government Office: The Minister-Chairman, Vice Chairmen, PM's Assistant, General Director of the Portal, Departments, Authorities, subordinated units, and the Official Gazette;
- For filing: Archives, Compliance Control (2 copies)$_{TM}$.

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

MINISTER

Tran Luu Quang

[signed and sealed]

Appendix

(Promulgated together with Decree No. 13/2023/ND-CP dated 17 April 2023 of the Government)

Form No. 01	Request for Provision of Personal Data (For Individuals)
Form No. 02	Request for Provision of Personal Data (For Organizations and Enterprises)
Form No. 03	Notice of Violation of Regulations on Personal Data Protection
Form No. 04	Notice of Submission of Dossier for Assessment of the Impact of Personal Data Processing
Form No. 05	Notice of Changes to a Dossier
Form No. 06	Dossier for Assessment of the Impact of Cross-Border Transfer of Personal Data

Form No. 01

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

.. …., [insert date]

REQUEST FOR PROVISION OF PERSONAL DATA

(*For Individuals*)

Respectfully 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 …./…./…….. at ..... 4. Residence[2]: ..... 5. Telephone[3]

..... ; Fax..... ; E-mail: ..... 6. Personal data requested for provision[4]: ..... 7. Purpose of provision:..... 8. Provision of personal data requested for:

a) The first time b) Other: the … time (specify an ordinal number indicating the number of times that the above mentioned provision of data has been requested)

9. Number of copies[5]:

..... 10. Methods of receipt of personal data:

Receipt at the place requested for provision of data

Receipt by post (specify recipient's address: ..... Fax (specify fax number..... Receipt via electronic networks (specify recipient's address): ..... Other (specify): ..... 11. Enclosures (if required):.....

REQUESTER
(Signature and full name)

[1] In accordance with the provisions set out in the Civil Code on representatives and guardians of individuals requesting information being minors, persons having limited civil act capacity, persons having lost their civil act capacity, persons having cognitive and behavioral difficulties, etc.
[2] Specify residence of the representative/guardian.
[3] Specify telephone number, fax number and email address of the representative/guardian. [4] Specify name of the data subject and relevant information to be provided.
[5] Printed, copied or photographed version or data file.

Form No. 02

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

.. …., [insert date]

REQUEST FOR PROVISION OF PERSONAL DATA
(For Organizations and Enterprises)

Respectfully to: .....

1. Name of organization/enterprise:

..... 2. Representative[1]:..... 3. ID Card/Citizen Identity Card/Passport No.:..... issued on …./…./…….. at ..... 4. Head office address: ..... 5. Telephone[2] ..... ; Fax..... ; E-mail: ..... 6. Personal data requested for provision:..... 7. Purpose of provision:..... 8. Provision of personal data requested for:

a) The first time b) Other: the … time (specify an ordinal number indicating the number of times that the above-mentioned provision of data has been requested)

9. Number of copies[3]:

..... 10. Method of receipt of documents, records and documents:

Receipt at the place requested for provision of data

Receipt by post (specify recipient's address:

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

..... Receipt via electronic networks (specify recipient's address): ..... Other (specify):

..... 11. Enclosures (if required):.....

REQUESTER[4]

(Signature and full name)

[1] In accordance with the provisions set out in the Civil Code on representatives of organizations and enterprises. [2] Specify telephone number, fax number and email address of the representative.

[3] Printed, copied or photographed version or data file.

[4] Representative is to sign, write full name and affix seal of the organization/enterprise.

NAME OF ORGANIZATION No.:

Form No. 03
SOCIALIST REPUBLIC OF VIETNAM Independence - Freedom - Happiness

NOTICE

...., [insert date]

OF VIOLATION OF REGULATIONS ON PERSONAL DATA PROTECTION

Respectfully to: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention,
Ministry of Public Security)

Pursuant to the regulations on personal data protection, …….[1] would like to submit to the Ministry of Public Security a Dossier for Assessment of the Impact of Personal Data Processing, as follows:

1. Details of organization/enterprise

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

Head office address:..... -

Transaction office address:..... -

Decision on Establishment/Certificate of Enterprise Registration/Certificate of Business Registration/Certificate of Investment No.: ……. issued by .... on [*insert date*] at ...

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

- Staff in charge of personal data protection:

Full name:.....

Position:.....

Contact telephone numbers (landline & mobile):.....

Email:.....

2. Description of violation of regulations on personal data protection

- Time: .....

- Location:.....

- Violation:.....

- Related organizations, individuals and amount of data;

[1] Name of organization/enterprise

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

Full name:.....

Position:.....

Contact telephone numbers (landline & mobile):.....

Email:.....

- Consequences:.....

- Measures taken:.....

3. Enclosures

1. .

..... 2.

. .....

4. Undertakings

(Name of agency/organization/enterprise) undertakes: To take responsibility before the law for the accuracy and legality of the information provided and the enclosures.

Recipients:
- As mentioned above; ....

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

SOCIALIST REPUBLIC OF VIETNAM Independence - Freedom - Happiness

...., [insert date]

NOTICE

NAME OF ORGANIZATION No.: …

36

Form No. 04

OF SUBMISSION OF THE DOSSIER FOR ASSESSMENT OF THE IMPACT OF PERSONAL DATA PROCESSING

Respectfully to: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention, Ministry of Public Security)

Pursuant to the regulations on personal data protection, ……..[1] would like to

submit to the Ministry of Public Security a Dossier for Assessment of the Impact of Personal Data Processing, as follows:

1. Details of organization/enterprise

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

- Head office address:.....

- Transaction office address:.....

- Decision on Establishment/Certificate of Enterprise Registration/Certificate of Business Registration/Certificate of Investment No.: ……. issued by .... on [*insert date*] at ...

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

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

Full name:.....

Position:.....

Contact telephone numbers (landline & mobile):.....

Email:.....

2. Dossier for Assessment of the Impact of Personal Data Processing

1. .....

2. .....

[1] Name of organization/enterprise:

3. Undertakings

(Name of agency/organization/ enterprise) undertakes: To take responsibility before the law for the accuracy and legality of the Dossier for Assessment of the Impact of Personal Data Processing and the enclosures.

Recipients:
- As mentioned above; ....
ON BEHALF OF THE ORGANIZATION/ENTERPRISE
(Signature, full name, seal)

NAME OF ORGANIZATION No.: …

Form No. 05

SOCIALIST REPUBLIC OF VIETNAM Independence - Freedom - Happiness

NOTICE

...., [insert date]

OF CHANGES TO A DOSSIER …… [1]

Respectfully to: Ministry of Public Security

(Via the Department of Cybersecurity and Hi-Tech Crime Prevention)

Pursuant to the regulations on personal data protection, …….[2] would like to submit to the Ministry of Public Security a Dossier for Assessment of the Impact of Personal Data Processing, as follows:

1. Details of organization/enterprise

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

- Head office address:.....

- Transaction office address: .....

- Decision on Establishment/Certificate of Enterprise Registration/Certificate of Business Registration/Certificate of Investment No.: ……. issued by .... on [*insert date*] at ...

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

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

Full name:.....

Position:.....

Contact telephone numbers (landline & mobile):.....

Email:.....

. **2. Brief description of changes to the dossier**

- Changed items:.....

- Reasons for changes:.....

3. Attached documents

[1] Name of dossier: Dossier for Assessment of the Impact of Personal Data Processing or Dossier for Assessment of The Impact of Cross-Border Transfer of Personal Data.
[2] Name of organization/enterprise.

1. .....

2. .....

4. Undertakings

(Name of agency/organization/enterprise) undertakes: To take responsibility before the law for the accuracy and legality of the changed items and the enclosures.

Recipients:
- As mentioned above; ....
ON BEHALF OF THE ORGANIZATION/ ENTERPRISE
(Signature, full name and seal)

Form No. 06
SOCIALIST REPUBLIC OF VIETNAM Independence - Freedom - Happiness

NAME OF ORGANIZATION No.: …

...., [insert date]

DOSSIER FOR ASSESSMENT OF THE IMPACT OF CROSS-BORDER TRANSFER OF PERSONAL DATA

Respectfully to: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention,
Ministry of Public Security)

Pursuant to the regulations on personal data protection, ……..[1] would like to submit to the Ministry of Public Security a Dossier for Assessment of the Impact of Cross-border Transfer of Personal Data, as follows:

1. Details of organization/enterprise

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

- Head office address:.....

- Transaction office address:.....

- Decision on Establishment/Certificate of Enterprise Registration/Certificate of Business Registration/Certificate of Investment No.: ……. issued by .... on [*insert date*] at ...

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

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

Full name:.....

Position:.....

Contact telephone numbers (landline & mobile):.....

Email:.....

2. Dossier for Assessment of the Impact of Cross-border Transfer of Personal Data

1. .....

2. .....

[1] Name of organization/enterprise

3. Undertakings

(Name of agency/organization/enterprise) undertakes: To take responsibility before the law for the accuracy and legality of the Dossier for Assessment of the Impact of Cross-border Transfer of Personal Data and the enclosures.

Recipients:
- As mentioned above; ....

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