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

DECREE

On personal data protection[1]

Pursuant to the June 19, 2015 Law on Organization of the Government; and the November 22, 2019 Law Amending and Supplementing a Number of Articles of the Law on Organization of the Government and the Law on Organization of Local Administration;

Pursuant to the November 24, 2015 Civil Code;

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

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

At the proposal of the Minister of Public Security;

The Government promulgates the Decree on personal data protection.

Chapter I

GENERAL PROVISIONS

Article 1. Scope of regulation and subjects of application

1. This Decree provides for personal data protection and personal data protection responsibility of related agencies, organizations and individuals.

2. This Decree applies to:

a/ Vietnamese agencies, organizations and individuals;

b/ Vietnam-based foreign agencies, organizations and individuals;

c/ Vietnamese agencies, organizations and individuals operating in foreign countries;

d/ Foreign agencies, organizations and individuals directly engaged or involved in personal data processing activities in Vietnam.

---

[1] Công Báo Nos 685-686 (30/4/2023)

Article 2. Interpretation of terms

In this Decree, the terms below are construed as follows:

1. Personal data means information in the form of symbol, script, digit, image or sound or in a similar form in the electronic environment which is affiliated to a specific person or helps identify a specific person. Personal data include basic personal data and sensitive personal data.

2. Information helping identify a specific person means information formed from activities of an individual that, when combined with other stored data and information, can help identify such person.

3. Basic personal data of an individual include:

a/ Family name, middle name and first name shown in birth registration certificate, and other names (if any);

b/ Day, month and year of birth; day, month, year of death or missing;

c/ Gender;

d/ Place of birth, place of birth registration, place of permanent residence, place of temporary residence, current place of residence, native place, and contact address;

dd/ Citizenship;

e/ Image;

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, and health insurance card number;

h/ Marital status;

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

k/ Information on digital account of the individual; personal data reflecting activities and history of activities of the individual in the cyberspace;

l/ Other information affiliated to a specific person or helping identify a specific person which is not mentioned in Clause 4 of this Article.

4. Sensitive personal data means personal data associated with the privacy of an individual that, once infringed upon, will directly affect lawful rights and interests of such individual, including:

a/ Political views and religious views;

b/ Information on health status and privacy as stated 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 the individual;

dd/ Information on physical attributes and biological characteristics of the individual;

e/ Information on sex life and sexual orientation of the individual;

g/ Data on crimes and criminal acts that are collected and stored by law enforcement agencies;

h/ Client information of credit institutions, foreign bank branches, intermediary payment service providers and other licensed organizations, including: know-your-customer information as specified by law, information on accounts, information on deposits, information on deposited assets, information on transactions, and information on securing parties at credit institutions, foreign bank branches and intermediary payment service providers;

i/ Data on the individual's position determined through positioning services;

k/ Other personal data that are defined by law as specific data and need application of necessary confidentiality measures.

5. Personal data protection means prevention, detection, stoppage and handling of violations related to personal data in accordance with law.

6. Data subject means an individual whose information is reflected by personal data.

7. Personal data processing means activity or activities that affect(s) personal data, such as collecting, recording, analyzing, certifying, storing, modifying, publicizing, combining, retrieving, revoking, encrypting, decoding, copying, sharing, transmitting, providing, transferring, deleting and destroying personal data or other relevant activities.

8. Data subject's consent means an explicit and willing expression confirming the data subject's permission for the processing of his/her personal data.

9. Personal data controller means an organization or individual that decides on the purposes and means of personal data processing.

10. Personal data processor means an organization or individual that carries out data processing on behalf of a data controller under a contract or an agreement with the data controller.

11. Personal data controlling and processing party means an organization or individual that simultaneously decides on personal data processing purposes and means and directly carries out personal data processing.

12. Third party means an organization or individual other than the data subject, personal data controller, personal data processor or personal data controlling and processing party that is permitted to process personal data.

13. Automatic personal-data processing means a form of personal data processing performed by electronic means in order to evaluate, analyze and predict activities of a specific person, such as his/her habits, likes, level of reliability, behaviors, location, trends and capacity, and other cases.

14. Transfer of personal data abroad means the use of cyberspace, devices, 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 the use of a location outside the territory of the Socialist Republic of Vietnam to process personal data of Vietnamese citizens, covering:

a/ Organizations, enterprises and individuals transferring personal data of Vietnamese citizens to overseas organizations, enterprises and management divisions for processing in conformity with purposes consented to by data subjects;

b/ Personal data controllers, personal data controlling and processing parties or personal data processors processing personal data of Vietnamese citizens by automated systems located outside the territory of the Socialist Republic of Vietnam in conformity with purposes consented to by data subjects.

Article 3. Principles of personal data protection

1. Personal data shall be processed in accordance with law.

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

3. Personal data shall be processed only for purposes registered or declared by personal data controllers, personal data processors, personal data controlling and processing parties or third parties concerning personal data processing.

4. Collected personal data must be appropriate and limited to the data processing scope and purposes. Personal data may not be purchased or sold in any form, unless otherwise provided for by law.

5. Personal data shall be updated and added in conformity with data processing purposes.

6. Personal data are eligible for the application of protection and confidentiality measures during data processing, including also protection against violations of regulations on personal data protection and prevention and combat of data loss, destruction or damage caused by incidents or use of technical measures.

7. Personal data may only be stored for a period of time suitable to data processing purposes, unless otherwise provided for by law.

8. Personal data controllers or personal data controlling and processing parties shall adhere to the data processing principles specified in Clauses 1 thru 7 of this Article and prove their adherence to such principles.

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

Agencies, organizations and individuals that violate regulations on personal data protection shall, depending on severity of their violations, be disciplined, administratively sanctioned or criminally handled under regulations.

Article 5. State management of personal data protection

The Government shall perform the unified state management of personal data protection.

Contents of the state management of personal data protection:

1. Submitting to competent state agencies for promulgation or promulgating according to competence legal documents on personal data protection and directing and organizing the implementation of such legal documents.

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

3. Providing agencies, organizations and individuals with guidance on personal data protection measures, processes and standards in accordance with law.

4. Disseminating and educating about the law on personal data protection; carrying out public communications and disseminating knowledge and skills about personal data protection.

5. Developing, training and further training cadres, civil servants, public employees and persons assigned to perform personal data protection.

6. Inspecting and examining the implementation of the law on personal data protection; settling complaints and denunciations and handling violations of the law on personal data protection in accordance with law.

7. Compiling statistics, providing information and making reports on the situation of personal data protection and implementation of the law on personal data protection to competent state agencies.

8. Carrying out international cooperation on personal data protection.

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

The protection of personal data must comply with the treaties to which the Socialist Republic of Vietnam is a contracting party, provisions of relevant laws and this Decree.

Article 7. International cooperation on personal data protection

1. Formulating international cooperation mechanisms to facilitate the effective implementation of the law on personal data protection.

2. Participating in mutual legal assistance on personal data protection with other countries, including notification, complaint proposal, investigation assistance and information exchange, with the application of appropriate safeguards for personal data protection.

3. Organizing conferences, seminars and scientific researches and promoting international cooperation in the law enforcement for personal data protection.

4. Organizing bilateral and multilateral meetings, and exchanging experience in lawmaking activities and personal data protection practices.

5. Carrying out technology transfer to serve personal data protection.

Article 8. Prohibited acts

1. Processing personal data in contravention of the law on personal data protection.

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

3. Processing personal data to create information and data affecting national security, social order and safety, or lawful rights and interests of other organizations and individuals.

4. Obstructing personal data protection activities of competent agencies.

5. Abusing personal data protection activities to violate law.

Chapter II

PERSONAL DATA PROTECTION ACTIVITIES

Section 1

RIGHTS AND OBLIGATIONS OF DATA SUBJECTS

Article 9. Rights of data subjects

1. The right to know

Data subjects are entitled to know information on the processing of their personal data, unless otherwise provided for by law.

2. The right to consent

Data subjects are entitled to consent or refuse to consent to the processing of their personal data, except the case specified in Article 17 of this Decree.

3. The right to access

Data subjects are entitled to access for viewing, modifying or requesting modification of their personal data, unless otherwise provided for by law.

4. The right to withdraw consent

Data subjects are entitled to withdraw their consent, unless otherwise provided for by law.

5. The right to data deletion

Data subjects are entitled to delete or request the deletion of their personal data, unless otherwise provided for by law.

6. The right to restriction of data processing

a/ Data subjects are entitled to request restriction of the processing of their personal data, unless otherwise provided for by law;

b/ The restriction of data processing shall be imposed within 72 hours after it is requested by a data subject, for all personal data for which the data subject requests processing restriction, unless otherwise provided for by law.

7. The right to data provision

Data subjects are entitled to request personal data controllers or personal data controlling and processing parties to provide the former with their personal data, unless otherwise provided for by law.

8. The right to object to data processing

a/ Data subjects are entitled to object to the processing of their personal data by personal data controllers or personal data controlling and processing parties in order to stop or restrict disclosure of personal data or use of personal data for advertising or marketing purposes, unless otherwise provided for by law;

b/ Personal data controllers or personal data controlling and processing parties shall comply with a request of data subjects within 72 hours after receiving such request, unless otherwise provided for by law.

9. The right to file complaints or denunciations and initiate lawsuits

Data subjects are entitled to file complaints or denunciations or initiate lawsuits in accordance with law.

10. The right to claim compensation for damage

Data subjects are entitled to claim compensation for damage in accordance with law upon occurrence of a violation of regulations on protection of their personal data, unless otherwise agreed upon by the parties or otherwise provided for by law.

11. The right to self-protection

Data subjects are entitled to self-protection in accordance with the Civil Code, other relevant laws and this Decree, or request competent agencies or organizations to take measures to protect their civil rights in accordance with Article 11 of the Civil Code.

Article 10. Obligations of data subjects

1. To protect their own personal data by themselves; to request related organizations and individuals to protect their personal data.

2. To respect and protect personal data of others.

3. To provide adequate and accurate personal data when permitting the processing of their personal data.

4. To participate in disseminating and popularizing personal data protection skills.

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

Section 2

PROTECTION OF PERSONAL DATA DURING THE PERSONAL DATA PROCESSING

Article 11. Consent of data subjects

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

2. The consent of a data subject takes effect only when the data subject shows his/her willingness and is explicitly aware of:

a/ Type of personal data to be processed;

b/ Purpose of personal data processing;

c/ Organizations and individuals licensed to process personal data;

d/ Rights and obligations of data subjects.

3. The consent of a data subject must be explicitly and specifically expressed in written form, by voice, by ticking the "yes" box, typing "yes" syntax in text message, selecting "yes" technical settings or through another action.

4. Consent must be given for the same purpose. In case of multiple purposes, the personal data controller or personal data controlling and processing party shall list such purposes for the data subject to give his/her consent 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 copied in written form, including also in electronic form or verifiable format.

6. Silence or non-response of a data subject is not regarded as a consent.

7. Data subjects may give their consent in part or with accompanying conditions.

8. In case of processing sensitive personal data, a data subject shall be informed that to-be-processed data are sensitive data.

9. The consent of a data subject shall be valid until the data subject otherwise decides or when a competent state agency makes a written request.

10. In case of a dispute, the responsibility to prove the data subject's consent rests with the personal data controller or personal data controlling and processing party.

11. By authorization in accordance with the Civil Code, an organization or individual may, on behalf of the data subject, carry out procedures related to the processing of the data subject's personal data with the personal data controller or personal data controlling and processing party in case the data subject is explicitly aware of and gives consent to such in accordance with Clause 3 of this Article, unless otherwise provided for by law.

Article 12. Withdrawal of consent

1. The withdrawal of consent does not affect the lawfulness of the data processing already consented to prior to the withdrawal of consent.

2. The withdrawal of consent must be expressed in a format that can be printed or copied in written form, including also in electronic form or verifiable format.

3. Upon receiving a consent withdrawal request from a data subject, the personal data controller or personal data controlling and processing party shall notify the data subject of consequences and damage that are likely to occur when the consent is withdrawn.

4. After implementing Clause 2 of this Article, the personal data controller, personal data processor, personal data controlling and processing party or the third party shall stop and request related organizations and individuals to stop processing data of the data subject that has withdrawn his/her consent.

Article 13. Notification of personal data processing

1. The notification of personal data processing shall be made once before personal data processing activities are carried out.

2. Contents of the notification of personal data processing to a data subject:

a/ Purpose of data processing;

b/ Type of used personal data that are related to the data processing purpose specified at Point a, Clause 2 of this Article;

c/ Method of data processing;

d/ Information on other organizations and individuals related to the data processing purpose specified at Point a, Clause 2 of this Article;

dd/ Possible undesirable consequences and damage;

e/ Times of data processing commencement and completion.

3. The notification of personal data processing to data subjects shall be made in a format that can be printed or copied in written form, including also in electronic form or verifiable format.

4. The personal data controller or personal data controlling and processing party is not required to comply with Clause 1 of this Article in the following cases:

a/ The data subject is explicitly aware of and gives a full consent to the contents specified in Clauses 1 and 2 of this Article before permitting the personal data controller or personal data controlling and processing party to collect personal data in accordance with Article 9 of this Decree;

b/ Personal data are processed by competent state agencies for the purpose of serving the operation of state agencies in accordance with law.

Article 14. Provision of personal data

1. Data subjects may request personal data controllers or personal data controlling and processing parties to provide the former with their personal data.

2. A personal data controller or personal data controlling and processing party:

a/ May provide personal data of a data subject to another organization or individual after obtaining the consent of the data subject, unless otherwise provided for by law;

b/ May, on behalf of a data subject, provide such data subject's personal data to another organization or individual when such data subject permits representation and authorization, unless otherwise provided for by law.

3. A personal data controller or personal data controlling and processing party shall provide personal data of a data subject within 72 hours after receiving the request of such data subject, unless otherwise provided for by law.

4. A personal data controller or personal data controlling and processing party may not provide personal data of a data subject in the following cases:

a/ The provision of personal data causes harm to national defense and security or social order and safety;

b/ The provision of personal data is likely to affect the safety or physical or mental health of others;

c/ The data subject refuses to give consent to the provision, or representation or authorization for the receipt, of personal data.

5. Forms of request for personal data provision:

a/ A data subject may directly come or authorize another person to come to the head office of the personal data controller or personal data controlling and processing party to request personal data provision.

The request recipient shall instruct the requester to fill in the form of request for personal data provision.

In case the requester is illiterate or is a person with disabilities which render him/her unable to fill in the form of request for personal data provision, the request recipient shall help fill in the form of request;

b/ A form of request for personal data provision, made according to Form No. 01 or No. 02 provided in the Appendix to this Decree, may be sent via the electronic network, by post or by fax to the personal data controller or personal data controlling and processing party.

6. A form of request for personal data provision must be presented in Vietnamese and have the following principal contents:

a/ Full name; place of residence, address; people's identity card number, citizen identity card number or passport number of the requester; fax number, telephone number, email address (if any);

b/ Personal data requested to be provided, clearly stating title(s) of document(s), dossier(s) or material(s);

c/ Form of personal data provision;

d/ Reason for and purpose of request for personal data provision.

7. In case of request for personal data provision under Clause 2 of this Article, a written consent of related individuals and organizations is required.

8. Receipt of requests for personal data provision

a/ A personal data controller or personal data controlling and processing party shall receive requests for personal data provision and monitor the process of personal data provision and list of personal data to be provided as requested;

b/ In case personal data requested to be provided fall beyond its/his/her competence, the personal data controller or personal data controlling and processing party shall notify such to and refer the requester to a competent authority or clearly notify that it/he/she cannot provide personal data.

9. Settlement of requests for personal data provision

Upon receiving a valid request for personal data provision, a personal data controller or personal data controlling and processing party that is responsible for personal data provision shall notify the duration, place and form of personal data provision; actual expenses for printing, photocopying and sending information via post and fax (if any) and payment mode and term; and provide personal data according to the order and procedures specified in this Article.

Article 15. Modification of personal data

1. For data subjects:

a/ To be entitled to access data for viewing and modifying their personal data after such data are collected by the personal data controller or personal data controlling and processing party with their consent, unless otherwise provided for by law;

b/ In case it is impossible to make direct modification for technical reasons or other reasons, to request the personal data controller or personal data controlling and processing party to modify their personal data.

2. A personal data controller or personal data controlling and processing party may modify personal data of a data subject after obtaining the latter's consent as soon as possible or in accordance with specialized laws. If unable to modify data, it/he/she shall notify such to the data subject within 72 hours after receiving the latter's request for data modification.

3. A personal data processor or a third party may modify personal data of a data subject after obtaining the written consent of the personal data controller or personal data controlling and processing party and being explicitly aware that the data subject's consent has been obtained.

Article 16. Storage, deletion and destruction of personal data

1. A data subject may request a personal data controller or personal data controlling and processing party to delete the former's personal data in the following cases:

a/ He/she finds that such personal data are no longer necessary for the consented purpose of data collection and accepts damage that is likely to occur upon request for data deletion;

b/ He/she withdrawals his/her consent;

c/ He/she objects to data processing and the personal data controller or personal data controlling and processing party has no plausible reason for continued data processing;

d/ Personal data are processed in contravention of the consented purpose or the data processing violates law;

dd/ Personal data are subject to deletion in accordance with law.

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

a/ Data deletion is not allowed under law;

b/ Personal data are processed by competent state agencies for the purpose of serving the operation of state agencies in accordance with law;

c/ Personal data have been made public in accordance with law;

d/ Personal data are processed for legal, scientific research and statistical purposes in accordance with law;

dd/ In emergency cases of national defense and security, social order and safety, catastrophes or dangerous epidemics; in case of a threat to security or national defense which is not serious to the extent requiring the declaration of a state of emergency; or for preventing and combating riots, terrorism, crime and violations;

e/ For responding to emergency circumstances that threaten the life, health or safety of the data subject or other individuals.

3. In case an enterprise is divided, split, merged, consolidated or dissolved, personal data shall be transferred in accordance with law.

4. In case of division, splitting or merger of agencies, organizations or administrative units or reorganization or transformation of state enterprises, personal data shall be transferred in accordance with law.

5. Data deletion shall be carried out within 72 hours after the receipt of the request of a data subject for all personal data collected by the personal data controller or personal data controlling and processing party, unless otherwise provided for by law.

6. Personal data controllers, personal data controlling and processing parties, personal data processors and third parties shall store personal data in forms suitable to their operation and take measures to protect personal data in accordance with law.

7. A personal data controller, personal data controlling and processing party, personal data processor or third party shall permanently delete data in the following cases:

a/ Data are processed for improper purposes or the purpose of data processing has been accomplished as consented to by the data subject;

b/ The storage of personal data is no longer necessary for the operation of the data controller, personal data controlling and processing party, personal data processor or third party;

c/ The data controller, personal data controlling and processing party, personal data processor or third party is dissolved or no longer operates or is declared bankrupt or is subject to business operation termination in accordance with law.

Article 17. Processing of personal data without requiring consent of data subjects

1. In case of emergency in which relevant personal data should be immediately processed to protect the life and health of data subjects or others. Personal data controllers, personal data processors, personal data controlling and processing parties and third parties shall prove this case.

2. Disclosure of personal data as prescribed by law.

3. Data processing by competent state agencies in the state of emergency of national defense and security, social order and safety, catastrophes or dangerous epidemics; occurrence of a threat to security or national defense which is not serious to the extent of requiring the declaration of a state of emergency, or for preventing and combating riots, terrorism, crimes and violations in accordance with law.

4. For performance of contractual obligations of data subjects toward related agencies, organizations and individuals in accordance with law.

5. To serve the operation of state agencies in accordance with specialized laws.

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

Competent agencies and organizations may audio-record, video-record and process personal data collected from audio and video recording activities in public places for purposes of protecting national security, social order and safety and lawful rights and interests of organizations and individuals in accordance with law

without having to obtain the consent of data subjects. When making audio or video recording, competent agencies and organizations shall notify such to data subjects for the latter to understand that they are being audio- or video-recorded, unless otherwise provided for by law.

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

1. The processing of personal data of a person declared missing or dead must be consented to by his/her spouse or adult child; in the absence of the spouse or adult child of such person, the consent of such person's parent is required, except 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 shall be regarded as no consent being given.

Article 20. Processing of personal data of children

1. The processing of personal data of children must always adhere to the principle of protecting rights and the best interests of children.

2. For the processing of personal data of a child, it is required to obtain the consent of such child, in case the child is full 7 years old or older, and the consent of the child's parent or guardian under regulations, except the cases specified in Article 17 of this Decree. The personal data controller, personal data processor, personal data controlling and processing party or third party shall verify the age of children before processing their personal data.

3. The processing, permanent deletion or destruction of personal data of a child shall be stopped in the following cases:

a/ Data are processed for improper purposes or the purpose of processing personal data has been accomplished as consented to by the data subject, unless otherwise provided for by law;

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

c/ The stoppage is requested by a competent authority when there are sufficient grounds to prove that the processing of the child's personal data affects his/her lawful rights and interests, unless otherwise provided for by law.

Article 21. Protection of personal data in marketing and introduction of promotional products

1. Organizations or individuals providing services of marketing and introducing promotional products may use customers' personal data collected

through the former's business activities to provide such services only after obtaining the consent of data subjects.

2. The processing of personal data of customers for provision of services of marketing and introducing promotional products must be consented to by customers, provided that such customers clearly know contents, methods, forms and frequency of product introduction.

3. Organizations or individuals providing services of marketing and introducing promotional products shall prove that the use of personal data of customers to whom products are introduced complies with Clauses 1 and 2 of this Article.

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

1. Organizations and individuals involved in personal data processing shall apply personal data protection measures in order to stop the unauthorized collection of personal data from the former's service systems and equipment.

2. The establishment of software systems or technical measures or the organization of activities of collecting, transferring, purchasing and selling personal data without the consent of data subjects is a violation of law.

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

1. In case of detecting a violation of regulations on personal data protection, the personal data controller or personal data controlling and processing party shall send a notice of the violation of regulations on personal data protection, made according to Form No. 03 provided in the Appendix to this Decree, to the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) within 72 hours after the violation occurs. In case the notice is sent beyond the 72-hour time limit, it must be accompanied by the reason for late sending.

2. The personal data processor shall notify the personal data controller as promptly as possible after detecting a violation of regulations on personal data protection.

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

a/ Describing the nature of the violation of regulations on personal data protection, including: time, place, act of violation, violator, type of personal data, and quantity of relevant data;

b/ Contact details of the staff member assigned to perform data protection or of the organization or individual responsible for personal data protection;

c/ Describing possible consequences and damage caused by the violation;

d/ Describing measures put in place to address and mitigate harms caused by the violation.

4. In case it is impossible to fully notify the contents specified in Clause 3 of this Article, the notification may be made in phases.

5. The personal data controller or personal data controlling and processing party shall make a written confirmation of the occurrence of a violation of regulations on personal data protection, and coordinate with the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) in handling the violation.

6. Organizations and individuals shall send a notice to the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) in the following cases:

a/ Detecting violations with respect to personal data;

b/ Detecting that personal data are processed for improper purposes and in contravention of the initial agreement reached between the data subject and the personal data controller or personal data controlling and processing party or in violation of law;

c/ Detecting that rights of the data subject are not guaranteed or are improperly exercised;

d/ Other cases specified by law.

Section 3

IMPACT ASSESSMENT OF PERSONAL DATA PROCESSING AND TRANSFER OF PERSONAL DATA ABROAD

Article 24. Impact assessment of personal data processing

1. Personal data controllers or personal data controlling and processing parties shall compile and keep their dossiers of impact assessment of personal data processing from the time of commencement of personal data processing.

A dossier of impact assessment of personal data processing by a personal data controller or personal data controlling and processing party must have:

a/ Information and contact details of the personal data controller or personal data controlling and processing party;

b/ Full names and contact details of the organization assigned to protect personal data and of the personal data protection staff of the personal data controller or personal data controlling and processing party;

c/ Purpose of data processing;

d/ Types of personal data processed;

dd/ Organizations and individuals receiving personal data, including those outside the territory of Vietnam;

e/ Cases of transfer of personal data abroad;

g/ Period of personal data processing; projected time for deletion or destruction of personal data (if any);

h/ Description of personal data protection measures applied;

i/ Evaluation of impacts of personal data processing; possible undesirable consequences and risks/harms, and measures to mitigate or eliminate such risks/harms.

2. A personal data processor shall prepare and keep a dossier of impact assessment of personal data processing in case of performance of a contract with a personal data controller. Such a dossier must have:

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 of the personal data processing staff of the personal data processor;

c/ Description of personal data processing activities and types of personal data processed under the contract signed with the personal data controller;

d/ Period of personal data processing; projected time for deletion or destruction of personal data (if any);

dd/ Cases of transfer of personal data abroad;

e/ General description of personal data protection measures applied;

g/ Possible undesirable consequences and risks/harms, and measures to mitigate or eliminate such risks/harms.

3. A dossier of impact assessment of personal data processing specified in Clause 1 or 2 of this Article shall be made in writing with legal validity of the personal data controller or personal data controlling and processing party or personal data processor.

4. Dossiers of impact assessment of personal data processing must always be available to serve inspection and evaluation activities of the Ministry of Public Security, and it is required to send 1 original of a notice of sending a dossier of impact assessment of personal data processing, made according to Form No. 04 provided in the Appendix to this Decree, to the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) within 60 days from the date of commencement of personal data processing.

5. The Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) shall check the dossier of impact assessment of personal data processing and request the personal data controller or personal data controlling and processing party or personal data processor to complete the dossier in case the dossier is incomplete or invalid.

6. Personal data controllers, personal data controlling and processing parties or personal data processors shall update changes and send a notice of changes in dossiers of impact assessment of personal data processing, made according to Form No. 05 provided in the Appendix to this Decree, when there is a change in contents of dossiers sent to the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control).

Article 25. Transfer of personal data abroad

1. Personal data of Vietnamese citizens shall be transferred abroad in cases in which transferors of personal data abroad make a dossier of assessment of impacts of the transfer of personal data abroad and carry out the procedures specified in Clauses 3, 4 and 5 of this Article. Transferors of personal data abroad include personal data controllers, personal data controlling and processing parties, personal data processors and third parties.

2. A dossier of assessment of impacts of the transfer of personal data abroad must have:

a/ Information and contact details of the transferor and the recipient of personal data of Vietnamese citizens;

b/ Full name and contact details of the in-charge organization or individual of the data transferor involved in the transfer and receipt of personal data of Vietnamese citizens;

c/ Description of and explanation about objectives of the processing of personal data of Vietnamese citizens after the data are transferred abroad;

d/ Description and clarification of the type of personal data to be transferred abroad;

dd/ Description and statement of the compliance with this Decree's provisions on personal data protection, and detailed description of personal data protection measures applied;

e/ Assessment of impacts of personal data processing; possible undesirable consequences and risks/harms, and measures to mitigate or eliminate such risks/harms;

g/ Consent of data subjects as mentioned in Article 11 of this Decree on the basis of being fully aware of the mechanism for response and filing complaints in case of incidents or upon request;

h/ Documents showing the binding and responsibility between transferors and recipients of personal data of Vietnamese citizens concerning personal data processing.

3. Dossiers of assessment of impacts of the transfer of personal data abroad must always be available to serve the inspection and assessment by the Ministry of Public Security.

The transferor of data abroad shall send 1 original dossier of assessment of impacts of the transfer of personal data abroad, made according to Form No. 06 provided in the Appendix of this Decree, to the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) within 60 days from the date of commencement of personal data processing.

4. The data transferor shall provide the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) with written information and contact details of the in-charge organization or individual after the data transfer is successfully completed.

5. The Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control) shall check the dossier of assessment of impacts of the transfer of personal data abroad and request the data transferor to complete the dossier in case the dossier is incomplete and or invalid.

6. The data transferor shall update changes and send a notice of changes in dossiers of assessment of impacts of the transfer of personal data abroad, made according to Form No. 05 provided in the Appendix to this Decree, when there is a change in contents of dossiers sent to the Ministry of Public Security (the Department of Cyber Security and Hi-Tech Crime Prevention and Control). The time limit for the data transferor to complete the dossier is 10 days from the date the request is made.

7. Based on the practical situation, the Ministry of Public Security shall decide on annual transfer of personal data abroad, except cases of detecting violations of this Decree's provisions on personal data protection or cases of leakage or loss of personal data of Vietnamese citizens.

8. The Ministry of Public Security shall decide to request the transferor of personal data abroad to stop the data transfer in the following cases:

a/ When detecting that the transferred personal data are used for activities that infringe upon the national interests and security of the Socialist Republic of Vietnam;

b/ The data transferor fails to comply with Clauses 5 and 6 of this Article;

c/ Upon occurrence of incidents of leakage or loss of personal data of Vietnamese citizens.

Section 4

MEASURES AND CONDITIONS FOR PERSONAL DATA PROTECTION

Article 26. Personal data protection measures

1. Personal data protection measures shall be applied right from the beginning of, and during, personal data processing.

2. Personal data protection measures include:

a/ Management measures performed by organizations and individuals involved in personal data processing;

b/ Technical measures performed by organizations and individuals involved in personal data processing;

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

d/ Investigation and procedural measures performed 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 of this Decree.

2. To formulate and promulgate regulations on personal data protection, clarifying to-be-performed tasks under this Decree.

3. To encourage the application of personal data protection standards suitable to the fields, business lines and activities related to personal data processing.

4. To inspect the cyber security of systems, means and equipment serving personal data processing before data processing or permanently deleting personal data or destroying personal data-containing devices.

Article 28. Protection of sensitive personal data

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

2. To designate functional divisions for personal data protection or designate staffs in charge of personal data protection, and exchange information about such divisions and staffs with the Specialized Agency for Personal Data Protection. In case the personal data controller, personal data controlling and processing party, personal data processor or third party is an individual, to exchange information about such individual.

3. To notify data subjects of the processing of their sensitive personal data, except the cases specified in Clause 4, Article 13, and Articles 17 and 18, of this Decree.

Article 29. The specialized agency for personal data protection and the National Portal on Personal Data Protection

1. The Specialized Agency for Personal Data Protection is the Department of Cyber Security and Hi-Tech Crime Prevention and Control of the Ministry of Public Security, which shall assist the Ministry of Public Security in performing the state management of personal data protection.

2. The National Portal on Personal Data Protection is functioned to:

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

b/ Carry out public communications about and disseminate policies and laws on personal data protection;

c/ Update information and situation on personal data protection;

d/ Receive information, dossiers and data on personal data protection activities via the cyberspace;

dd/ Provide information on the evaluation results of the personal data protection work of related agencies, organizations and individuals;

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

g/ Provide warnings, and coordinate in provision of warnings about the risks and acts of infringing upon personal data in accordance with law;

h/ Handle violations of regulations on personal data protection in accordance with law;

i/ Carry out other activities in accordance with the law on personal data protection.

Article 30. Conditions for ensuring personal data protection activities

1. Personal data protection forces:

a/ A specialized force for personal data protection shall be arranged in the Specialized Agency for Personal Data Protection;

b/ Divisions or staffs performing the function of personal data protection shall be designated in agencies, organizations and enterprises to ensure the implementation of regulations on personal data protection;

c/ Organizations and individuals shall be mobilized to participate in personal data protection;

d/ The Ministry of Public Security shall formulate specific programs and plans for development of human resources for personal data protection.

2. Agencies, organizations and individuals shall disseminate knowledge and skills on personal data protection for raising the awareness of personal data protection for other agencies, organizations and individuals.

3. Physical foundations and operational conditions must be ensured for the Specialized Agency for Personal Data Protection.

Article 31. Funds for personal data protection activities

1. Financial sources for personal data protection include state budget funds; contributions of agencies, organizations and individuals at home and abroad; revenues from provision of personal data protection services; international aid, and other lawful revenues.

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

3. Funds for personal data protection of organizations and enterprises shall be allocated by themselves under regulations.

Chapter III

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS

Article 32. Responsibilities of the Ministry of Public Security

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

2. To guide and organize activities of personal data protection, protection of the rights of data subjects against violations of the law on personal data protection, and propose the promulgation of personal data protection standards and standard application recommendations.

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

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

5. To receive dossiers and forms of, and information on, personal data protection under this Decree.

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

7. To carry out inspection and examination, settle complaints and denunciations in, and handle violations of regulations on, personal data protection in accordance with law.

Article 33. Responsibilities of the Ministry of Information and Communications

1. To direct media and press agencies, and organizations and enterprises operating in the fields under its management to perform personal data protection under this Decree.

2. To formulate, and guide and organize the implementation of, measures for personal data protection, ensuring cyberinformation security for personal data in information and communications activities according to its assigned functions and tasks.

3. To coordinate with the Ministry of Public Security in carrying out inspection and examination 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 in, and apply regulations on, personal data protection for agencies, organizations and

individuals under its management in accordance with law and within the ambit of its assigned functions and tasks.

Article 35. Responsibilities of the Ministry of Science and Technology

1. To coordinate with the Ministry of Public Security in formulating personal data protection standards and standard application recommendations.

2. To research, and exchange with the Ministry of Public Security about, personal data protection measures to keep pace with the science and technology development.

Article 36. Responsibilities of ministries, ministerial-level agencies and government-attached 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 formulate and implement the contents and tasks on personal data protection as specified in this Decree.

3. To include regulations on personal data protection in the formulation and implementation of their tasks.

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

5. To promulgate the lists of open data in compliance with regulations on personal data protection.

Article 37. Responsibilities of provincial-level People's Committees

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 this Decree's provisions on personal data protection.

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

4. To promulgate the lists of open data in compliance with regulations on personal data protection.

Article 38. Responsibilities of personal data controllers

1. To implement organizational and technical measures together with appropriate safety and confidentiality measures to prove that data processing

activities comply with the law on personal data protection and, when necessary, review and update such measures.

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

3. To notify acts of violating regulations on personal data protection under Article 23 of this Decree.

4. To select appropriate personal data processors with clear tasks and only work with personal data processors that apply appropriate data protection measures.

5. To guarantee the rights of data subjects as specified in Article 9 of this Decree.

6. To take responsibility before data subjects for damage caused in the course of personal data processing.

7. To coordinate with the Ministry of Public Security and competent state agencies in personal data protection and provision of information serving the investigation and handling of violations of the law on personal data protection.

Article 39. Responsibilities of personal data processors

1. To receive personal data only after entering into contracts or agreements on data processing with personal data controllers.

2. To carry out personal data processing according to the contracts or agreement signed with personal data controllers.

3. To fully perform personal data protection measures specified in this Decree and other relevant legal documents.

4. To take responsibility before data subjects for damage caused in the course of personal data processing.

5. To delete and return all personal data to personal data controllers after the completion of data processing.

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

Article 40. Responsibilities of personal data controlling and processing parties

To fully comply with regulations on responsibilities of personal data controllers and personal data processors.

Article 41. Responsibilities of third parties

To fully comply with regulations on responsibilities for personal data processing under this Decree.

Article 42. Responsibilities of related organizations and individuals

1. To take measures to protect their personal data and take responsibility for the accuracy of the personal data they provide.

2. To comply with this Decree's provisions on personal data protection.

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

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

Chapter IV

IMPLEMENTATION PROVISIONS

Article 43. Effect

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

2. Micro-, small- and medium-sized enterprises and startup enterprises may choose to be exempt from implementation of regulations on appointment of individuals and divisions in charge of personal data protection within the first 2 years from the date of their establishment.

3. Clause 2 of this Article shall not apply to micro-, small- and medium-sized enterprises and startup enterprises directly dealing in personal data processing.

Article 44. Implementation responsibility

1. The Minister of Public Security shall urge, examine and guide the implementation of this Decree.

2. Ministers, heads of ministerial-level agencies, heads of government-attached agencies, and chairpersons of provincial-level People's Committees shall implement this Decree.-

On behalf of the Government
For the Prime Minister
Deputy Prime Minister
TRAN LUU QUANG

* *The Appendix to this Decree is not translated.*