ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT

Presidential Decree No. 23169, Sep. 29, 2011
Amended by Presidential Decree No. 24425, Mar. 23, 2013
Presidential Decree No. 25531, Aug. 6, 2014
Presidential Decree No. 25751, Nov. 19, 2014
Presidential Decree No. 25840, Dec. 9, 2014
Presidential Decree No. 26140, Mar. 11, 2015
Presidential Decree No. 26728, Dec. 22, 2015
Presidential Decree No. 26776, Dec. 30, 2015
Presidential Decree No. 27370, Jul. 22, 2016
Presidential Decree No. 27522, Sep. 29, 2016
Presidential Decree No. 28074, May 29, 2017
Presidential Decree No. 28150, jun. 27, 2017
Presidential Decree No. 28211, Jul. 26, 2017
Presidential Decree No. 28355, Oct. 17, 2017
Presidential Decree No. 29421, Dec. 24, 2018
Presidential Decree No. 30509, Mar. 3, 2020
Presidential Decree No. 30833, Jul. 14, 2020
Presidential Decree No. 30892, Aug. 4, 2020
Presidential Decree No. 31429, Feb. 2, 2021
Presidential Decree No. 32528, Mar. 8, 2022
Presidential Decree No. 32813, Jul. 19, 2022
Presidential Decree No. 33723, Sep. 12, 2023

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose)

The purpose of this Decree is to prescribe matters mandated by the Personal Information Protection Act and matters necessary for the enforcement thereof.

Article 2 (Scope of Public Institutions)

"National agencies and public entities prescribed by Presidential Decree" in subparagraph 6 (b) of Article 2 of the Personal Information Protection Act (hereinafter referred to as the "Act") means: *<Amended on Jul.14, 2020>*

1. The National Human Rights Commission of Korea established under Article 3 of the National Human Rights Commission of Korea Act;

1-2. The Corruption Investigation Office for High-Ranking Officials under Article 3 (1) of the Act on the Establishment and Operation of the Corruption Investigation Office for High-Ranking Officials;

2. Public institutions provided for in Article 4 of the Act on the Management of Public Institutions;

3. Local government-invested public corporations and local government public corporations established under the Local Public Enterprises Act;

4. Special corporations incorporated under any special Act;

5. Schools of each level established under the Elementary and Secondary Education Act, the Higher Education Act, and under any other statutes.

Article 3 (Scope of Visual Data Processing Devices)

(1) "Devices prescribed by Presidential Decree" in subparagraph 7 of Article 2 of the Act means the following: *<Amended on Sep. 12, 2023>*

1. A closed-circuit television means either of the following devices:

(a) A device that takes pictures, etc. continuously or regularly through a camera installed at a certain place, or transmits such pictures, etc. to a specified place via transmission channel of wired or wireless closed circuits, etc.;

(b) A device that can videotape or record the visual data photographed or transmitted under item (a);

2. A network camera means a device with which a person who installs or manages such device can collect, store, or otherwise process visual data filmed continuously or regularly through a device installed at a certain place, via the wired or wireless Internet at any place.

(2) "Device prescribed by Presidential Decree" in subparagraph 7-2 of Article 2 of the Act means the following: *<Newly Inserted on Sep. 12, 2023>*

1. A wearable device: A device, such as eyeglasses or a watch, which is worn on the body or clothes of a person to take pictures, etc. or to collect, store, or transmit such pictures, etc.;

2. A portable device: A device, such as a mobile communications terminal or a digital camera, which a person carries to take pictures, etc. or to collect, store, or transmit such pictures, etc.;

3. An attachable or mountable device: A device that is attached to or mounted on a movable object, such as a vehicle or drone, to take pictures, etc. or to collect, store, or transmit such pictures, etc.

CHAPTER II PERSONAL INFORMATION PROTECTION COMMISSION

Article 4 Deleted. *<Aug. 4, 2020>*

Article 4-2 (Prohibition on Work for Profit)

The Commissioners of the Personal Information Protection Commission (hereinafter referred to as the "Protection Commission") provided for in Article 7 (1) of the Act shall not engage in any of the following work for the purpose of making profits in accordance with Article 7-6 (1) of the Act:

1. Work related to the matters to be deliberated and resolved by the Protection Commission in accordance with Article 7-9 (1) of the Act;
2. Work related to the matters to be mediated by the Personal Information Dispute Mediation Committee referred to in Article 40 (1) of the Act (hereinafter referred to as the "Dispute Mediation Committee").

Article 5 (Expert Committees)

(1) The Protection Commission shall establish an expert committee for each of the following sectors (hereinafter referred to as "expert committee") to professionally conduct a preliminary review on the matters to be deliberated and resolved on under Article 7-9 (1) of the Act: *<Amended on Aug. 4, 2020; Sep. 12, 2023>*

1. Cross-border transfer of personal information;
2. Other sectors deemed necessary by the Protection Commission.

(2) An expert committee established under paragraph (1) shall be composed of up to 20 members with gender equality being taken into consideration, including one chairperson, who are designated or commissioned by the Chairperson of the Protection Commission from among the following persons; and the chairperson of the expert committee shall be designated by the Chairperson of the Protection Commission from among the expert committee members: *<Amended on Jul. 22, 2016; Aug. 4, 2020; Sep. 12, 2023>*

1. Commissioners of the Protection Commission;
2. Public officials of a central administrative agency who are responsible for personal information protection-related work;
3. Persons with abundant expertise and experience in personal information protection;
4. Persons belonging to, or recommended by, personal information protection-related organizations or trade associations.

(3) Except as provided in paragraphs (1) and (2), matters necessary for the composition, operation, etc. of expert committees shall be determined by the Chairperson of the Protection Commission subject to resolution by the Protection Commission. *<Newly Inserted on Sep. 12, 2023>*

Article 5-2 (Personal Information Protection Policy Council)

(1) For the consistent implementation of personal information protection policies, and to facilitate consultation among relevant central administrative agencies with respect to matters related to the protection of personal information, the Personal Information Protection Policy Council (hereinafter referred to as the "Policy Council") may be established within the Protection Commission.

(2) The Policy Council shall discuss the following matters:

1. Major personal information protection policies, including the Master Plan for the protection of personal information under Article 9 of the Act and the implementation plan under Article 10 of the Act;
2. The enactment and amendment of major statutes or regulations related to the protection of personal information;
3. Cooperation and coordination of opinions on major personal information protection policies;
4. The prevention of and response to personal information breach incidents;
5. The development of technology and professional workforce for the protection of personal information;
6. Other matters requiring consultation among relevant central administrative agencies in connection with the protection of personal information.

(3) The Policy Council shall be comprised of the Senior Executive Service members of the relevant central administrative agencies or equivalent public officials in charge of work related to personal information protection, and they shall be appointed by the head of the relevant central administrative agencies, but the chairperson of the Policy Council (hereinafter referred to as the "Chairperson" in this Article) shall be the Vice Chairperson of the Protection Commission.

(4) If necessary to do the work, the Policy Council may have working-level councils or sector-specific councils.

(5) The chairpersons of the sector-specific councils and working-level councils shall be the Protection Commission's public officials designated by the Chairperson of the Protection Commission.

(6) If necessary to do the work, the Policy Council, and working-level councils and sector-specific councils may request attendance, submission of materials or opinions, or other necessary cooperation from the related agency, organization, expert, etc.

(7) Except as provided in paragraphs (1) through (6), matters necessary for the operation of the Policy Council shall be determined by the chairperson through a resolution of the Policy Council.

Article 5-3 (City/Provincial Inter-Agency Personal Information Protection Council)

(1) In order to efficiently implement personal information protection policies and strengthen autonomous protection of personal information, each Special Metropolitan City, Metropolitan City, Special Self-Governing City, Do and Special Self-Governing Province (hereinafter collectively referred to as "City/

Do") may have a City/Do inter-agency personal information protection council (hereinafter referred to as the "City/Do Council").

(2) The City/Do Councils shall discuss the following matters:

1. Personal information protection policies of the City/Do;
2. Collection and delivery of opinions from/to related agencies/organizations;
3. Sharing of best practices on protecting personal information;
4. Other matters requiring discussion at the City/Do Councils in relation to the protection of personal information.

(3) Except as provided in paragraphs (1) and (2), matters necessary for the composition and operation of a City/Do Council shall be determined by the ordinance of City/Do.

Article 6 (Disclosure of Proceedings)

Meetings of the Protection Commission shall be open to the public: Provided, that a meeting may be held as a closed session, if deemed necessary by the Chairperson of the Protection Commission.

Article 7 (Dispatch of Public Officials)

The Protection Commission may request a public institution to dispatch a public official, executive officer, or employee who works for the public institution, where it deems necessary to perform its work.

Article 8 Deleted. *<Aug. 4, 2020>*

Article 9 (Allowances for Attendance)

A Commissioner who attends a meeting of the Protection Commission, the expert committee, or the Policy Council; or a person who attends a meeting of the Protection Commission, the expert committee, or the Policy Council pursuant to Article 7-9 (2) of the Act may be paid allowances, travel expenses, and other necessary costs within budgetary limits: Provided, that this shall not apply where any public official attends a meeting directly related with his or her own work. *<Amended on Aug. 4, 2020>*

Article 9-2 (Procedures for Advising Improvement of Policies, Systems, Statutes, and Regulations)

(1) The Protection Commission shall advise the improvement of policies, systems, statutes, and regulations to the relevant agency pursuant to Article 7-9 (4) of the Act, along with the details of and reasons for such improvement. *<Amended on Aug. 4, 2020>*

(2) The Protection Commission may request the relevant agency to submit materials about the results of the implementation of its advice in order to examine whether such advice has been implemented pursuant to Article 7-9 (5) of the Act. *<Amended on Aug. 4, 2020>*

Article 9-3 (Procedures for Assessment of Personal Information Breach Incident Factors)

(1) The head of a central administrative agency who intends to request an assessment of personal information breach incident factors pursuant to Article 8-2 (1) of the Act (hereinafter referred to as "assessment of personal information breach incident factors") shall submit to the Protection Commission a written request (or an electronic request form) for an assessment of personal information breach incident factors which contains the following matters:

1. The purposes and major contents of the policy and systems in need of personal information processing to be adopted or changed by the statutes or regulations (including the draft);
2. Self-analysis of personal information breach incident factors with respect to the matters prescribed in paragraph (2) following the adoption and change of the policy and system in need of personal information processing;
3. Measures to protect personal information following the adoption and change of the policy and system in need of personal information processing.

(2) Upon receipt of a written request under paragraph (1), the Protection Commission shall assess data breach incident factors taking into account the following matters, and shall notify the result thereof to the head of the related central administrative agency:

1. Necessity for processing personal information;
2. Appropriateness of guarantees for the rights of data subjects;
3. Safety in the management of personal information;
4. Other matters necessary to assess data breach incident factors.

(3) The head of a central administrative agency who has been advised as prescribed in Article 8-2 (2) of the Act shall endeavor to implement as advised, such as incorporating such advice in the relevant draft statute or regulation: Provided, that where it is impracticable to implement as advised by the Protection Commission, the reason therefor shall be notified to the Protection Commission.

(4) The Protection Commission may request materials necessary to assess data breach incident factors from the head of the related central administrative agency.

(5) The Protection Commission may establish guidelines necessary to assess data breach incident factors, including detailed criteria for and methods of the assessment of data breach incident factors; and shall notify the heads of central administrative agencies of the guidelines.

(6) The Protection Commission may seek counsel, etc. from relevant experts where necessary to assess data breach incident factors.

Article 10 Deleted. *<Aug. 4, 2020>*

CHAPTER III PROCEDURES TO ESTABLISH MASTER PLANS AND IMPLEMENTATION PLANS

Article 11 (Procedures to Establish Master Plans)

(1) The Protection Commission shall establish a Master Plan to protect personal information under Article 9 of the Act (hereinafter referred to as "Master Plan") every three years no later than June 30 of the year preceding the start of the third-year plan. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 22, 2016; Aug. 4, 2020>*

(2) To establish the Master Plan pursuant to paragraph (1), the Protection Commission may receive sub-plans by sector, in which mid- and long-term plans, policies, etc. related to personal information protection are reflected, from the heads of the related central administrative agencies, and may reflect them in the Master Plan. In such cases, the Protection Commission shall consult with the heads of the related central administrative agencies about the goals of the Master Plan, intended directions, guidelines to prepare sub-plans by sector, and other relevant matters. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 22, 2016>*

(3) Upon finalizing the Master Plan, the Protection Commission shall notify the heads of the related central administrative agencies of the Master Plan without delay. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 22, 2016>*

Article 12 (Procedures to Establish Implementation Plans)

(1) The Protection Commission shall develop guidelines on how to establish implementation plans for the next year no later than June 30 each year, and notify the heads of the related central administrative agencies of such guidelines. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 22, 2016; Aug. 4, 2020>*

(2) The head of a related central administrative agency shall establish the implementation plan for the sector under his or her jurisdiction, to be implemented during the following year based upon the Master Plan according to the guidelines notified under paragraph (1); and shall submit the same to the Protection Commission no later than September 30 each year. *<Amended on Aug. 4, 2020>*

(3) The Protection Commission shall deliberate and resolve on the implementation plans submitted pursuant to paragraph (2) no later than December 31 of that year. *<Amended on Aug. 4, 2020>*

Article 13 (Scope of Materials Requested and Methods of Request)

(1) The Protection Commission may request materials or opinions regarding the following from a personal information controller pursuant to Article 11 (1) of the Act: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 22, 2016; Sep. 12, 2023>*

1. Matters concerning the management of personal information and personal information files processed by the personal information controller and the installation and operation of fixed or mobile visual data processing devices;
2. Matters concerning whether the privacy officer has been designated pursuant to Article 31 of the Act;
3. Matters concerning technical, managerial, and physical measures to ensure the safety of personal information;

4. Matters concerning access by data subjects, requests for correction, deletion, suspension of personal information processing, and the status of measures taken;

5. Other matters necessary to establish and implement a Master Plan, such as compliance with the Act and this Decree.

(2) When requesting materials, opinions, etc. pursuant to paragraph (1), the Protection Commission shall request the same to the minimum extent necessary to efficiently establish and implement the Master Plan. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 22, 2016>*

(3) Paragraphs (1) and (2) shall apply mutatis mutandis where the head of a central administrative agency requests materials, etc. from a personal information controller under his or her jurisdiction pursuant to Article 11 (3) of the Act. In such cases, the "Protection Commission" shall be construed as the "head of a central administrative agency", and "Article 11 (1) of the Act" as "Article 11 (3) of the Act", respectively. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 22, 2016>*

Article 14 (Promotion and Support of Self-Regulation)

The Protection Commission may provide necessary support to agencies and organizations related to the protection of personal information within budgetary limits to promote self-regulating data-protection activities of personal information controllers pursuant to subparagraph 2 of Article 13 of the Act. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

CHAPTER IV PROCESSING OF PERSONAL INFORMATION

Article 14-2 (Standards on Additional Use and Provision of Personal Information)

(1) If a personal information controller uses or provides personal information (hereinafter referred to as "additional use or provision of personal information") without the consent of the data subject in accordance with Article 15 (3) or Article 17 (4) of the Act, the personal information controller shall consider the following matters:

1. Whether it is reasonably related to the original purpose for which the personal information was collected;

2. Whether additional use or provision of personal information is foreseeable in light of the circumstances under which the personal information was collected and processing practices;

3. Whether additional use or provision of personal information does not unfairly infringe on the interests of the data subject;

4. Whether the measures required to ensure safety such as pseudonymization or encryption have been taken.

(2) Where additional use or provision of personal information continues to take place, a personal information controller shall disclose the criteria for assessing the matters referred to in the subparagraphs of paragraph (1) in the Privacy Policy under Article 30 (1) of the Act, and a privacy officer under Article

31 (1) of the Act shall check whether the personal information controller is using or providing additional personal information in accordance with the relevant criteria. *<Amended on Sep. 12, 2023>*

Article 15 (Control of Out-of-Purpose Use of Personal Information or Provision Thereof to Third Parties)

Where a public institution uses personal information for other than the intended purpose, or provides it to a third party pursuant to Article 18 (2) of the Act, it shall record the following in the Register for Control of Out-of-Purpose Use or Provision of Personal Information in the form prescribed by Notification of the Protection Commission; and shall manage the Register: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

1. The name of the personal information or personal information file to be used or provided;
2. The name of the institution that uses, or is provided with, personal information;
3. The purpose of use or provision;
4. The statutory ground for such use or provision;
5. Particulars of personal information to be used or provided;
6. The date, frequency, or period for using or providing personal information;
7. Methods of use or provision of personal information;
8. Any limitation or necessary measure that the personal information controller has requested from the recipient pursuant to Article 18 (5) of the Act.

Article 15-2 (Matters Subject to Notification, such as Sources of Personal Information Collected, and Methods and Procedures for Notification)

(1) "Personal information controller satisfying the criteria prescribed by Presidential Decree" in the main clause of Article 20 (2) of the Act means any of the following personal information controllers; in such cases, the number of data subjects prescribed in the following shall be calculated based on the daily average during the immediately preceding three months as of the end of the previous year: *<Amended on Sep. 12, 2023>*

1. A person who processes sensitive information defined in Article 23 of the Act (hereinafter referred to as "sensitive information") or personally identifiable information defined in Article 24 (1) of the Act (hereinafter referred to as "personally identifiable information") of at least 50 thousand data subjects;
2. A person who processes personal information of at least one million data subjects.

(2) A personal information controller who falls under any subparagraph of paragraph (1) shall notify data subjects of the matters referred to in the subparagraphs of Article 20 (1) of the Act by any of the following methods within three months from the date of being provided with their personal information: Provided, that where the personal information controller is regularly provided with and processes personal information at least twice a year to the extent that the personal information controller has obtained consent from the data subjects under Article 17 (1) 1 of the Act about the matters prescribed in Article 17 (2) 1

through 4 of the Act, he or she shall notify the data subjects within three months from the date of being provided with their personal information, or at least once a year counting from the date of the consent: *<Amended on Sep. 12, 2023>*

1. A method by which the data subjects can easily confirm the details of the notification, such as in writing, electronic mail, telephone, or text message;
2. Giving notification in the course of providing goods or services through a notification window so that the data subjects can easily recognize the relevant matters.

(3) A personal information controller may notify the matters regarding the source of collected personal information, etc. pursuant to Article 20 (2) of the Act while notifying the details of the use and provision of personal information under Article 20-2 (1) of the Act. *<Newly Inserted on Sep. 12, 2023>*

(4) A personal information controller specified in any subparagraph of paragraph (1) who has made notification under paragraph (2) shall retain and manage the following matters until the relevant personal information is destroyed pursuant to Article 21 or 37 (5) of the Act: *<Amended on Sep. 12, 2023>*

1. The fact that data subjects are notified;
2. When notification is made;
3. How notification is made.

Article 15-3 (Notification of Details of Use and Provision of Personal Information)

(1) "Personal information controller who meets the criteria prescribed by Presidential Decree" in the main clause of Article 20-2 (1) of the Act means any of the following personal information controllers; in such cases, the number of data subjects prescribed in the following subparagraphs shall be calculated based on the daily average during the immediately preceding three months as of the end of the previous year:

1. A person who processes sensitive information or personally identifiable information of at least 50 thousand data subjects;
2. A person who processes personal information of at least one million data subjects.

(2) A data subject to be given notification under Article 20-2 (1) of the Act shall be a data subject except the following:

1. A data subject who expresses his or her intention to refuse notification;
2. Where a personal information controller processes the personal information of executive officers and employees under his or her control to perform his or her work, the relevant data subject;
3. Where a personal information controller processes the personal information of executive officers or employees of other public institutions, corporations, or organizations or individuals, including their contact information, to perform his or her work, the relevant data subject;
4. A data subject of personal information that is used or provided under provisions otherwise provided in statutes or for the purpose of complying with legal obligations;
5. A data subject of personal information that is used or provided by public institutions for the purpose of performing their work prescribed in statutes, regulations, etc.

(3) Information to be notified to data subjects under Article 20-2 (1) of the Act shall be as follows:

1. The purpose of collecting and using personal information and the particulars of the personal information collected and used;

2. A third party provided with personal information, the purpose of providing the personal information, and the particulars of the personal information provided: Provided, That excluded herefrom shall be information provided under Articles 13, 13-2, and 13-4 of the Protection of Communications Secrets Act and Article 83 (3) of the Telecommunications Business Act.

(4) Notification under Article 20-2 (1) of the Act shall be given at least once a year by any of the following methods:

1. A method by which a data subject can easily confirm the details of notification, such as in writing, electronic mail, telephone, or text message;

2. Giving notification in the course of providing goods or services through a notification window so that a data subject can easily recognize the relevant details (limited to where notification is given regarding the methods of accessing the information system through which the details of the use and provision of personal information are confirmed under Article 20-2 (1) of the Act).

Article 16 (Methods of Destroying Personal Information)

(1) A personal information controller shall destroy personal information pursuant to Article 21 of the Act by the following methods: *<Amended on Aug. 6, 2014; Jul. 19, 2022>*

1. Personal information in electronic files shall be permanently deleted so that it cannot be restored: Provided, That where it is substantially impracticable to permanently delete the files due to technical characteristics, the personal information controller shall take measures to make it impossible to restore the information by treating it as information falling under Article 58-2 of the Act;

2. Other records, printouts, paper documents, and media containing personal information, other than those referred to in subparagraph 1, shall be shredded or incinerated.

(2) Detailed matters concerning the safe destruction of personal information subject to paragraph (1) shall be prescribed by Notification of the Protection Commission. *<Newly Inserted on Aug. 6, 2014; Nov. 19, 2014; Jul. 26, 2017; Sep. 29, 2016>*

Article 17 (Methods of Obtaining Consent)

(1) A personal information controller shall meet all of the following requirements when obtaining consent from a data subject to the processing of his or her personal information pursuant to Article 22 of the Act: *<Newly Inserted on Sep. 12, 2023>*

1. The data subject shall be able to decide whether to give his or her consent based on his or her free will;

2. Details requiring the consent of the data subject shall be specific and clear;

3. The personal information controller shall use phrases that are easily readable and understandable for the relevant details;

4. The personal information controller shall provide the data subject with the methods of clearly indicating whether to give consent.

(2) A personal information controller shall obtain consent from a data subject to the processing of his or her personal information pursuant to Article 22 of the Act by any of the following methods: *<Amended on Sep. 12, 2023>*

1. To issue a document stating the matters requiring consent, either in person or by mail or facsimile, to the data subject, and obtain a written consent on which the data subject has affixed his or her signature or seal;

2. To inform the data subject of the matters requiring consent, and confirm his or her intent of consent by telephone;

3. To inform the data subject of the matters requiring consent by telephone, have the data subject confirm the matters requiring his or her consent posted on a designated website, etc.; and reconfirm his or her intent of consent by telephone;

4. To post the matters requiring consent on a designated website, etc., and have the data subject express his or her consent thereto;

5. To send an electronic mail containing the matters requiring consent to the data subject, and receiving an e-mail indicating his or her consent thereto;

6. Other methods to inform the data subject of the matters requiring consent by a method similar to those referred to in subparagraphs 1 through 5 and confirm his or her intent of consent.

(3) "Important matters prescribed by Presidential Decree" in Article 22 (2) of the Act means the following: *<Newly Inserted on Oct. 17, 2017; Sep. 12, 2023>*

1. The fact that a data subject may be contacted to promote goods or services or solicit purchase thereof using the data subject's personal information with respect to the purpose of collecting and using personal information;

2. The following matters with respect to the particulars of personal information to be processed:

(a) Sensitive information;

(b) Passport numbers, driver's license numbers, and alien registration numbers as set forth in subparagraphs 2 through 4 of Article 19;

3. The period for retaining and using personal information (in the case of provision, meaning the period for retaining and using personal information by the recipient);

4. The recipient of personal information and the purpose for which the recipient of the personal information uses such information.

(4) Where a personal information controller intends to obtain consent from a data subject under the subparagraphs of Article 22 (1) of the Act, he or she shall clearly indicate the fact that the data subject may choose whether to give consent. *<Amended on Sep. 12, 2023>*

(5) “Means prescribed by Presidential Decree” in the former part of Article 22 (3) of the Act means in writing, or by electronic mail, facsimile, telephone, or text message, or any other means equivalent thereto (hereinafter referred to as “in writing, etc.”). *<Amended on Sep. 12, 2023>*

(6) The head of a central administrative agency may establish the standards for appropriate methods of obtaining consent, out of the various methods of consent stated in paragraph (2), through the personal information protection guidelines under Article 12 (2) of the Act (hereinafter referred to as “personal information protection guidelines”), in consideration of the work of each personal information controller under his or her jurisdiction, the characteristics of their business, the number of data subjects, etc., and may encourage personal information controllers to obtain consent in accordance with such standards. *<Newly Inserted on Dec. 30, 2015; Oct. 17, 2017; Sep. 12, 2023>*

Article 17-2 (Protection of Children's Personal Information)

(1) A personal information controller shall confirm whether a legal representative has granted consent pursuant to Article 22-2 (1) of the Act by any of the following methods:

1. Requesting the legal representative to indicate whether to give consent on the website where matters requiring consent are posted, and informing him or her by mobile phone text message that the personal information controller confirms the indication of the consent;
2. Requesting the legal representative to indicate whether to give consent on the website where matters requiring consent are posted, and being provided with information on his or her card, such as a credit card or debit card;
3. Requesting the legal representative to indicate whether to give consent on the website where matters requiring consent are posted, and verifying the identity of the legal representative through identity verification on his or her mobile phone;
4. Issuing the legal representative a document specifying matters requiring consent, either in person or by mail or fax, and requesting him or her to submit the document after signing and affixing seal on it with respect to such matters;
5. Sending the legal representative an electronic mail that specifies matters requiring consent, and requesting him or her to send an electronic mail with consent indicated;
6. Notifying the legal representative of matters requiring consent by telephone to obtain consent, or providing him or her with information on the methods of confirming matters requiring consent, such as via the Internet address, to obtain consent by telephone;
7. Other methods equivalent to those prescribed in subparagraphs 1 through 6 by which matters requiring consent are notified to the legal representative and an indication of his or her consent is confirmed.

(2) "Information prescribed by Presidential Decree" in Article 22-2 (2) of the Act means information on the name and contact details of a legal representative.

(3) Where it is impracticable for a personal information controller to indicate all matters requiring consent due to the characteristics of a medium by which personal information is collected, the personal information controller may provide a legal representative with information on the methods of confirming matters requiring consent, such as the Internet address or the telephone number of the place of business.

Article 18 (Scope of Sensitive Information)

"Information prescribed by Presidential Decree" in the main clause, with the exception of the subparagraphs, of Article 23 (1) of the Act means the following data or information: Provided, that where the public institutions process any of the following data or information pursuant to Article 18 (2) 5 through 9 of the Act, the said information shall be excluded herefrom: *<Amended on Sep. 29, 2016; Aug. 4, 2020>*

1. DNA information acquired from genetic testing, etc.;
2. Data that constitute a criminal history record defined in subparagraph 5 of Article 2 of the Act on the Lapse of Criminal Sentences;
3. Personal information resulting from specific technical processing of data relating to the physical, physiological or behavioral characteristics of an individual for the purpose of uniquely identifying that individual;
4. Personal information revealing racial or ethnic origin.

Article 19 (Scope of Personally Identifiable Information)

"Information prescribed by Presidential Decree" in the provisions, with the exception of the subparagraphs, of Article 24 (1) of the Act means any of the following information: Provided, that such information does not include any of the following information processed by the public institutions pursuant to Article 18 (2) 5 through 9 of the Act: *<Amended on Sep. 29, 2016; Jun. 27, 2017; Aug. 4, 2020>*

1. Resident registration numbers under Article 7-2 (1) of the Resident Registration Act;
2. Passport numbers under Article 7 (1) 1 of the Passport Act;
3. Driver's license numbers under Article 80 of the Road Traffic Act;
4. Alien registration numbers under Article 31 (5) of the Immigration Act.

Article 20 Deleted. *<Aug. 6, 2014>*

Article 21 (Measures to Ensure Safety of Personally Identifiable Information)

(1) Article 30 shall apply mutatis mutandis to measures to ensure the safety of personally identifiable information under Article 24 (3) of the Act. In such cases, "Article 29 of the Act" shall be construed as "Article 24 (3) of the Act"; and "personal information" as "personally identifiable information", respectively. *<Amended on Aug. 4, 2020; Sep. 12, 2023>*

(2) “Personal information controller meeting the criteria prescribed by Presidential Decree” in Article 24 (4) of the Act means any of the following personal information controllers:

1. A public institution;

2. A person who processes personally identifiable information of at least 50 thousand data subjects.

(3) The Protection Commission shall inspect, at least once every two years, whether the personal information controllers who falls under any subparagraph of paragraph (2) have taken measures necessary to ensure safety pursuant to Article 24 (4) of the Act. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

(4) The inspection referred to in paragraph (3) shall be conducted by requiring the personal information controllers provided for in paragraph (2) to submit necessary material online or in writing.

(5) “Specialized institutions prescribed by Presidential Decree” in Article 24 (5) of the Act means any of the following institutions: *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

1. The Korea Internet and Security Agency established under Article 52 of the Act on Promotion of Information and Communications Network Utilization and Information Protection. (hereinafter referred to as the “Korea Internet and Security Agency”);

2. A corporation, organization, or institution determined and prescribed by Notification of the Protection Commission as deemed to have technical and financial capacity and equipment to conduct the inspection pursuant to Article 24 (4) of the Act.

Article 21-2 (Persons Who Must Encrypt Resident Registration Numbers)

(1) Any personal information controller who retains resident registration numbers by electronic means shall take encryption measures pursuant to Article 24-2 (2) of the Act.

(2) The encryption of resident registration numbers by a personal information controller under paragraph (1) shall start from one of the following dates:

1. As to the personal information controllers who retain the resident registration numbers of less than one million data subjects: January 1, 2017;

2. As to the personal information controllers who retain the resident registration numbers of at least one million data subjects: January 1, 2018.

(3) The Protection Commission may determine and publicly notify the detailed matters regarding encryption measures under paragraph (1), taking into account the technical and economic feasibility and other factors. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 22 (Exception to Restriction on Installation and Operation of Fixed Visual Data Processing Devices)

(1) "Cases prescribed by Presidential Decree" in Article 25 (1) 6 of the Act means any of the following cases: *<Newly Inserted on Sep. 12, 2023>*

1. Where any photographed visual data is temporarily processed to compute statistical values or statistical characteristic values, such as the number, genders, and ages of visitors;

2. Other cases equivalent to that prescribed in subparagraph 1, which have been deliberated and resolved on by the Protection Commission.

(2) "Facilities prescribed by Presidential Decree" in the proviso of Article 25 (2) of the Act means the following facilities: *<Amended on May 29, 2017; Aug. 4, 2020; Sep. 12, 2023>*

1. Correctional facilities defined in subparagraph 1 of Article 2 of the Execution of Sentences and Treatment of Inmates;

2. Mental medical institutions (with accommodation facilities), mental treatment facilities, and mental patient rehabilitation facilities defined in subparagraph 5 through 7 of Article 3 of the Act on the Improvement of Mental Health and the Support for Welfare Services for Mental Patients.

(3) The head of a central administrative agency may establish a Privacy Policy which includes the detailed matters necessary to minimize infringement on the privacy of data subjects; and may encourage the personal information controllers under his or her jurisdiction to comply with the Privacy Policy when they install and operate fixed visual data processing devices at the facilities referred to in the subparagraphs of paragraph (2) pursuant to the proviso of Article 25 (2) of the Act. *<Amended on Sep. 12, 2023>*

Article 23 (Gathering Opinions on Installation of Fixed Visual Data Processing Devices)

(1) The head of a public institution that intends to install and operate fixed visual data processing devices pursuant to Article 25 (1) of the Act shall gather opinions from relevant experts and interested parties through any of the following procedures: *<Amended on Sep. 12, 2023>*

1. To give administrative advance notice or to hear opinions under the Administrative Procedures Act;

2. To hold an information session or to conduct a survey or polling with respect to the neighborhood residents, etc. directly affected by the installation of those fixed visual data processing devices.

(2) A person who intends to install and operate fixed visual data processing devices at the facilities specified in the proviso of Article 25 (2) of the Act shall gather opinions from the following persons: *<Amended on Sep. 12, 2023>*

1. Relevant experts;

2. Persons working in the relevant facilities, persons detained or accommodated in the relevant facilities, or interested parties, including the guardians of such persons.

Article 24 (Posting of Notice on Signboard)

(1) A person who installs and operates fixed visual data processing devices pursuant to Article 25 (1) of the Act (hereinafter referred to as "fixed visual data processing device operator") shall post the matters referred to in the subparagraphs of Article 25 (4) of the Act on a signboard so that data subjects may easily recognize that such devices have been installed and in operation: Provided, that a signboard, indicating the operation of fixed visual data processing devices in the pertinent facilities and whole area, may be posted at the entry and other easily noticeable place where several fixed visual data processing devices are installed in a building: *<Amended on Sep. 29, 2016; Sep. 12, 2023>*

1. Deleted; <*Sep. 29, 2016*>

2. Deleted; <*Sep. 29, 2016*>

3. Deleted. <*Sep. 29, 2016*>

(2) Notwithstanding paragraph (1), where any of the following applies to a fixed visual data processing device installed and operated by a fixed visual data processing device operator, the operator may post the matters referred to in the subparagraphs of Article 25 (4) of the Act on its website, in lieu of posting them on the signboard: <*Amended on Sep. 29, 2016; Sep. 12, 2023*>

1. Where the fixed visual data processing device is installed by a public institution for such purposes as long range photographing, over-speed and traffic signal violation enforcement service, or traffic flow survey, while the possibility of a personal information breach is significantly low;

2. Where a signboard cannot be posted because of the characteristics of the location or is not easily noticeable by data subjects even if posted, e.g., a fixed visual data processing device installed for surveillance of mountain fire.

(3) If the matters referred to in the subparagraphs of Article 25 (4) of the Act cannot be posted on a website under paragraph (2), a fixed visual data processing device operator shall make public the said matters in one or more of the following methods: <*Amended on Sep. 29, 2016; Aug. 2020; Sep. 12, 2023*>

1. Posting at easily noticeable places of the fixed visual data processing device operator's workplace, business premise, office, shop, etc. (hereinafter referred to as "workplace, etc.");

2. Publishing them in the Official Gazette (only where the fixed visual data processing device operator is a public institution) or a general daily newspaper, weekly newspaper or online newspaper, as defined in subparagraph 1 (a) and (c), or 2 of Article 2 of the Act on the Promotion of Newspapers circulating mainly over the Special Metropolitan City, Metropolitan City, Do, or Special Self-Governing Province (hereinafter referred to as "City/ Do") where the fixed visual data processing device operator's workplace is located.

(4) "Facilities prescribed by Presidential Decree" in the proviso, with the exception of the subparagraphs, of Article 25 (4) of the Act means the national security facilities provided for in Article 32 of the Regulations on Security Work. <*Amended on Sep. 29, 2016*>

Article 25 (Policy on Operation and Management of Fixed Visual Data Processing Devices)

(1) Each fixed visual data processing device operator shall establish a policy to operate and manage fixed visual data processing devices including the following matters pursuant to Article 25 (7) of the Act: <*Amended on Sep. 12, 2023*>

1. The statutory ground and purpose for installing the fixed visual data processing devices;

2. The number of the fixed visual data processing devices installed, the locations of installation, and the scope of photographing;

3. The manager and department in charge, and the person who is entitled to access the visual data;

4. The duration of filming, retention period, retention place, and processing method of the visual data;
5. How and where the fixed visual data processing device operator checks the visual data;
6. The measures taken to deal with the data subject's request to access the visual data;
7. The technical, managerial, and physical safeguards to protect the visual data;
8. Other matters necessary to install, operate, and manage the fixed visual data processing devices.

(2) Article 31 (2) and (3) shall apply mutatis mutandis to the disclosure of the policy to operate and manage fixed visual data processing devices established pursuant to paragraph (1). In such cases, "personal information controller" shall be construed as "fixed visual data processing device operator", "Article 30 (2) of the Act" as "Article 25 (7) of the Act", and "Privacy Policy" as "policy to operate and manage fixed visual data processing devices", respectively. <*Amended on Sep. 12, 2023*>

Article 26 (Entrustment of Installation and Operation of Fixed Visual Data Processing Devices by Public Institutions)

(1) Where a public institution entrusts the installation and operation of fixed visual data processing devices to a third party pursuant to the proviso of Article 25 (8) of the Act, it shall do so in writing stating the following: <*Amended on Sep. 12, 2023*>

1. The purpose and scope of entrusted business affairs;
2. Matters concerning limitation to re-entrustment;
3. Matters concerning the measures to ensure safety, including limitation to access to visual data;
4. Matters concerning the inspection of the status of visual data retained;
5. Matters concerning damage liability in case of breach of contractual obligation on the part of a person to whom the work is entrusted .

(2) Where business affairs are entrusted pursuant to paragraph (1), the name and contact information of the person entrusting shall be posted on the signboard, etc. referred to in Article 24 (1) through (3).

Article 27 (Exception to Restriction on Operation of Mobile Visual Data Processing Devices)

"Cases prescribed by Presidential Decree" in the proviso of Article 25-2 (2) of the Act means where it is necessary to take photographs of a person or things related to such person (limited to where such photographs constitute personal information; hereinafter the same shall apply) for the lifesaving, first-aid services, etc. in the event of a crime, fire, disaster, or any other situation equivalent thereto.

[Previous Article 27 moved to Article 27-3 <*Sep. 12, 2023*>]

Article 27-2 (Indication of Photographing with Mobile Visual Data Processing Devices)

Where persons or things related to such persons are photographed with a mobile visual data processing device in cases falling under the subparagraphs of Article 25-2 (1) of the Act, the fact of photographing shall be indicated and informed by means of light, sound, signboard, written notice, or announcement, or other means or methods equivalent thereto so that data subjects can easily recognize such fact: Provided,

That the fact of photographing may be informed by the means notified on the website established by the Protection Commission where it is difficult to inform data subjects of the fact due to the characteristics of photographing methods, such as aerial photographing using a drone.

Article 27-3 (Guidelines for Installing and Operating Visual Data Processing Devices)

Except as provided in the Act and this Decree, the Protection Commission may establish the Standard Personal Information Protection Guidelines referred to in Article 12 (1) of the Act regarding the standards for installing and operating fixed visual data processing devices and for operating mobile visual data processing devices, the entrusting of their installation and operation, and other matters; and may encourage fixed visual data processing device operators and persons who operate mobile visual data processing devices to comply with the Standard Guidelines. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020; Sep. 12, 2023>*

[Moved from Article 27 *<Sep. 12, 2023>]*

Article 28 (Measures to be Taken when Entrusting Personal Information Processing)

(1) "Matters prescribed by Presidential Decree" in Article 26 (1) 3 of the Act means the following:

1. The purpose and scope of entrusted work;
2. Matters concerning limitation to re-entrustment;
3. Matters concerning measures to ensure safety, including limitation to access to personal information;
4. Matters concerning supervision and inspection of the status of management of personal information retained in relation to entrusted work;
5. Matters concerning liability, such as compensation for damages caused by a breach of contractual obligations on the part of a person entrusted under Article 26 (2) of the Act (hereinafter referred to as "person entrusted").

(2) "Manner prescribed by Presidential Decree" in Article 26 (2) of the Act means the method wherein a personal information controller that has entrusted personal information processing (hereinafter referred to as "person entrusting") continuously posts details of the entrusted work and the person entrusted on its website.

(3) Where it is impossible to post on the website as prescribed in paragraph (2), the entrusted work and the person entrusted shall make public in one or more of the following manners: *<Amended on Sep. 12, 2023>*

1. Posting at easily noticeable places such as workplace of a person entrusting;
2. Publishing in the Official Gazette (only where the person entrusting is a public institution) or a general daily newspaper, weekly newspaper, or online newspaper, as defined in subparagraphs 1 (a) and (c) and 2 of Article 2 of the Act on the Promotion of Newspapers which mainly covers the City/Do where the person entrusting's workplace, etc. is located;
3. Publishing at a periodical, newsletter, PR magazine, or invoice to be published under the same title at least twice annually and distributed to data subjects on a continual basis;

4. Stipulating in an agreement, etc. for the supply of goods and services executed between the person entrusting and the data subjects and providing a copy of the same to the data subjects.

(4) "Manners prescribed by Presidential Decree" in the former part of Article 26 (3) of the Act means in writing, etc. *<Amended on Sep. 12, 2023>*

(5) Where a person entrusting is unable to inform the data subjects of the entrusted work and the person entrusted in the manner stated in paragraph (4) without its negligence, the person entrusting shall post the relevant matters on its website for at least 30 days: Provided, that a person entrusting who has no website shall post them at easily noticeable places of its workplace, etc. for at least 30 days.

(6) Where a person entrusted processes personal information, the person entrusting shall supervise whether the person entrusting complies with the obligations of a personal information controller provided for in the Act and this Decree and the matters referred to in Article 26 (1) of the Act, pursuant to Article 26 (4) of the Act.

Article 29 (Notification of Transfer of Personal Information Following Business Transfer)

(1) "Manner prescribed by Presidential Decree" in the provisions, with the exception of the subparagraphs, of Article 27 (1) of the Act and the main clause of Article 27 (2) of the Act means in writing, etc. *<Amended on Aug. 4, 2020>*

(2) Where a person who intends to transfer personal information pursuant to Article 27 (1) of the Act (hereinafter referred to as "business transferor, etc." in this Article) fails to inform the data subjects of the matters stated in Article 27 (1) of the Act in the manner stated in paragraph (1) without his or her negligence, the person shall post the relevant matters on the website for at least 30 days: Provided, that if there is a good reason for not being able to post the required information on its website, the business transferor, etc. may inform the data subjects of the matters stated in each subparagraph of Article 27 (1) of the Act through any of the following methods: *<Amended on Aug. 4, 2020>*

1. Posting the information at easily noticeable places of the workplace, etc. of the business transferor, etc. for at least 30 days;

2. Publishing the information in a general daily newspaper, weekly newspaper, or online newspaper, as defined in subparagraphs 1 (a) and (c) or 2 of Article 2 of the Act on the Promotion of Newspapers which mainly covers the City/Do where the business transferor, etc.'s workplace, etc. is located.

CHAPTER IV-2 SPECIAL CASES CONCERNING PROCESSING OF PSEUDONYMIZED INFORMATION

Article 29-2 (Designation and Cancellation of Designation of Expert Data Combination Agency)

(1) The standards for the designation of an expert agency (hereinafter referred to as "Expert Data Combination Agency") pursuant to Article 28-3 (1) of the Act shall be as follows:

1. Under Notification prescribed by the Protection Commission, the agency shall have formed an organization responsible for the combination and release of pseudonymized information and employed at least three full-time personnel with qualifications or experience relating to personal information protection;

2. Under Notification prescribed by the Protection Commission, the agency shall have set up space, facilities and equipment necessary to combine pseudonymized information safely and prepared policies and procedures relating to the combination and release of pseudonymized information;

3. Under Notification prescribed by the Protection Commission, the agency shall have financial capabilities;

4. No disclosure shall have been made under Article 66 of the Act for the recent three years.

(2) Any corporation, organization, or institution intending to be designated as an Expert Data Combination Agency pursuant to Article 28-3 (1) of the Act shall submit to the head of the Protection Commission or the related central administrative agency an application for the Designation of Expert Data Combination Agency prescribed by Notification of the Protection Commission with the following documents attached (including electronic documents; the same shall apply hereinafter):

1. Articles of incorporation or bylaws;

2. Documents prescribed and notified by the Protection Commission supporting that the agency satisfies the designation standards under paragraph (1).

(3) The head of the Protection Commission or related central administrative agency may designate the corporation, organization, or institution which submitted the application for the Designation of Expert Data Combination Agency under paragraph (2) as an Expert Data Combination Agency if it satisfies the designation standards under paragraph (1).

(4) Designation as an Expert Data Combination Agency shall be effective for three years from the date of designation, and if the Expert Data Combination Agency requests extension of the effective period, and such request satisfies the designation standards under paragraph (1), the head of the Protection Commission or the related central administrative agency may re-designate it as an Expert Data Combination Agency.

(5) If the Expert Data Combination Agency falls under any of the following, the head of the Protection Commission or related central administrative agency may cancel the designation of the Expert Data Combination Agency: Provided, that in the cases of subparagraph 1 or 2, designation shall be canceled:

1. If the agency has received the designation by fraud or improper means;

2. If the agency voluntarily requests cancellation of its designation or discontinues its business;

3. If the agency becomes non-compliant with the standards for designation of an Expert Data Combination Agency under paragraph (1);

4. If a personal information breach incident, including divulgence of information, occurs in connection with data combination, release, etc.;

5. If the agency otherwise violates any obligation under the Act or this Decree.

(6) The head of the Protection Commission or related central administrative agency shall hold a hearing when seeking to cancel the designation of an Expert Data Combination Agency in accordance with paragraph (5).

(7) The head of the Protection Commission or related central administrative agency shall publicly announce any designation, re-designation or cancellation of designation of an Expert Data Combination Agency in the Official Gazette or the websites of the Protection Commission or related central administrative agency. In such cases, if the head of the related central administrative agency designated, re-designated, or canceled the designation of any Expert Data Combination Agency, the head of the central administrative agency shall notify the Protection Commission of the same.

(8) Except as provided in paragraphs (1) through (7), matters necessary in connection with the designation, re-designation and cancellation of designation of an Expert Data Combination Agency shall be prescribed by Notification of the Protection Commission.

Article 29-3 (Combination and Release of Pseudonymized Information Processed by Different Personal Information Controllers)

(1) Any personal information controller intending to request an Expert Data Combination Agency to combine pseudonymized information (hereinafter referred to as “Applicant”) shall submit the data combination request in the form prescribed by Notification of the Protection Commission, together with the following documents, to the relevant Expert Data Combination Agency:

1. Documents related to the Applicant such as business registration certificate, certified copy of register of corporation, etc.;
2. Documents related to the pseudonymized information for combination;
3. Documents proving the purpose of combination;
4. Other documents prescribed by Notification of the Protection Commission’s notification as necessary for combining and releasing pseudonymized information.

(2) Any Expert Data Combination Agency intending to combine pseudonymized information under Article 28-3 (1) of the Act shall make sure that the combined information does not identify a particular individual. In such cases, the Protection Commission may make the Korea Internet and Security Agency or other agencies designated by Notification of the Protection Commission assist with relevant work necessary to make a particular individual unidentifiable.

(3) The Applicant that intends to take the information which was combined by the Expert Data Combination Agency pursuant to Article 28-3 (2) of the Act out of the Expert Data Combination Agency shall pseudonymize or otherwise process the information combined pursuant to paragraph (2) as the information under Article 58-2 of the Act at a place which was established within the Expert Data Combination Agency and underwent the necessary technical, managerial and physical measures required to ensure safety and receive permission therefor from the Expert Data Combination Agency.

(4) The Expert Data Combination Agency shall permit the release pursuant to Article 28-3 (2), if each of the following standards are met. In such cases, the Expert Data Combination Agency shall form a Release Review Committee to grant permission for release of combined information:

1. There is a relationship between the purpose of combination and the released information;
2. It is not possible to identify any particular individual using such information;
3. A security plan is established with regard to the released information.

(5) The Expert Data Combination Agency may charge the Applicant for the costs necessary for the combination, release, etc. of information.

(6) Except as provided in paragraphs (1) through (5), the procedures and methods of combining pseudonymized information, release of combined information and permission therefor, shall be set forth in Notification of the Protection Commission.

Article 29-4 (Management, and Supervision of Expert Data Combination Agency)

(1) Any head of the Protection Commission or related central administrative agency who has designated an Expert Data Combination Agency shall manage and supervise, among others, whether the Expert Data Combination Agency has maintained the work performance capacity, technologies and facilities required.

(2) The Expert Data Combination Agency shall submit to the head of the Protection Commission or the related central administrative agency the following documents every year for the management and supervision pursuant to paragraph (1):

1. Report on the combination and release of pseudonymized information;
2. Documents supporting that the agency continues to meet the standards for designation as an Expert Data Combination Agency;
3. Documents prescribed by Notification of the Protection Commission supporting that the agency has taken measures to secure the safety of pseudonymized information.

(3) The Protection Commission shall manage/supervise the following matters:

1. The Expert Data Combination Agency’s violation of law in the process of approving the combination and release of pseudonymized information;
2. The Applicant’s processing status with respect to pseudonymized information;
3. Other necessary matters required for the safe processing of pseudonymized information prescribed by Notification of the Protection Commission.

Article 29-5 (Measures to Ensure Safety of Pseudonymized Information)

(1) A personal information controller shall implement the following safety measures for pseudonymized information and additional information to restore pseudonymized information to the original state (hereinafter in this Article referred to as “additional information”) in accordance with Article 28-4 (1) of the Act: *<Amended on Feb. 2, 2021; Sep. 12, 2023>*

1. Measures to ensure safety under Article 30;

2. Separate storage of pseudonymized information and additional information: Provided, That any unnecessary additional information shall be destroyed;

3. Separation of access rights to pseudonymized information and additional information: Provided, That if the personal information controller finds it difficult to separate access rights due to good reason such as the personal information controller being a micro enterprise defined in Article 2 of the Framework Act on Micro Enterprises which cannot afford an additional employee to handle pseudonymized information, it shall manage and control access rights by granting the minimum degree of access necessary to do the work and recording the status of access rights granted.

(2) "Matters prescribed by Presidential Decree" in Article 28-4 (3) of the Act mean any of the following: *<Amended on Sep. 12, 2023>*

1. Purpose of processing pseudonymized information;

2. Items of pseudonymized personal information;

3. Use history of pseudonymized information;

4. Recipient of pseudonymized information provided by a third party;

5. Processing period of pseudonymized information (limited to where the processing period of pseudonymized information is separately determined pursuant to Article 28-4 (2) of the Act);

6. Other matters prescribed by Notification of the Protection Commission as deemed necessary for the management of the processing of pseudonymized information.

Article 29-6 Deleted. *<Sep. 12, 2023>*

CHAPTER IV-3 Cross-Border Transfer of Personal Information

Article 29-7 (Means of Notifying Data Subjects in Cases of Cross-Border Entrusted Processing or Storage of Personal Information)

"Means prescribed by Presidential Decree, such as electronic mail" in Article 28-8 (1) 3 (b) of the Act means in writing, etc.

Article 29-8 (Certification of Cross-Border Transfer of Personal Information)

(1) Where the Protection Commission intends to publicly notify certification under the provisions, with the exception of the items, of Article 28-8 (1) 4 of the Act, it shall complete all of the following procedures:

1. Evaluation by an institution specializing in certifying personal information protection under Article 34-6;

2. Evaluation by an expert committee for cross-border transfer of personal information under Article 5 (1) 1 (hereinafter referred to as "expert committee for cross-border transfer");

3. Consultation with the Policy Council.

(2) When the Protection Commission publicly notifies certification under the provisions, with the exception of the items, of Article 28-8 (1) 4 of the Act, it may determine and publicly notify its effective period of up to five years.

(3) Except as provided in paragraphs (1) and (2), matters necessary for the procedures, etc. for publicly notifying certification shall be determined and publicly notified by the Protection Commission.

Article 29-9 (Recognition of Countries' Personal Information Protection Levels)

(1) If the Protection Commission intends to recognize that a country or an international organization (hereinafter referred to as "recipient country, etc.") where personal information is provided (including inquired), processed under entrustment, or stored (hereafter in this Chapter referred to as "transfer") under Article 28-8 (1) 5 of the Act has a personal information protection system, the scope of guarantee of the rights of data subjects, the procedures for damage relief, etc. at a level substantially equal to the level of personal information protection under this Act, it shall comprehensively take into account the following matters:

1. Whether the personal information protection system of the recipient country, etc., including its statutes, regulations, and rules, is in conformity with the principles of information protection under Article 3 of the Act and guarantees the rights of data subjects under Article 4 of the Act;

2. Whether the recipient country, etc. has an independent supervisory authority responsible for guaranteeing and implementing the personal information protection system;

3. Whether the public institutions (including institutions that conduct business affairs similar to those of public institutions) of the recipient country, etc. process personal information under statutes and whether means to protect data subjects, such as the procedures for damage relief, exist and are effectively guaranteed;

4. Whether the recipient country, etc. has the procedures for damage relief that are easily available to data subjects and whether such procedures effectively protect data subjects;

5. Whether the supervisory authority of the recipient country, etc. is able to facilitate mutual cooperation with the Protection Commission in protecting the rights of data subjects;

6. Other matters determined and publicly notified by the Protection Commission as necessary to recognize the personal information protection level of the recipient country, etc., such as the personal information protection system, the scope of guarantee of the rights of data subjects, the procedures for damage relief.

(2) If the Protection Commission intends to grant recognition under paragraph (1), it shall follow the following procedures:

1. Evaluation by an expert committee for cross-border transfer;

2. Consultation with the Policy Council.

(3) If necessary for the protection of the rights of data subjects, etc., the Protection Commission may, when granting recognition under paragraph (1), determine the scope of the personal information to be transferred to a recipient country, etc., the scope of the personal information controllers to which personal information is transferred, the recognition period, the conditions of cross-border transfer, and other relevant matters differently for each recipient country, etc.

(4) Upon granting recognition under paragraph (1), the Protection Commission shall examine whether a recipient country, etc. maintains its personal information protection level that is substantially equal to the level under this Act.

(5) Where any change is made to the personal information system, the scope of guarantee of the rights of data subjects, the procedures for damage relief, etc. of a recipient country, etc. that are recognized under paragraph (1), the Protection Commission may revoke the recognition of the recipient country, etc. or change the details of the recognition, after hearing its opinions.

(6) Where the Protection Commission grants recognition under paragraph (1) or revokes such recognition or changes the details thereof under paragraph (5), it shall give public notice of such fact in the Official Gazette and publish it on its website.

(7) Except as provided in paragraphs (1) through (6), matters necessary for the recognition of a recipient country, etc. shall be determined and publicly notified by the Protection Commission.

Article 29-10 (Protective Measures in Cases of Cross-Border Transfers of Personal Information)

(1) Where a personal information controller makes a cross-border transfer of personal information under the proviso, with the exception of the subparagraphs, of Article 28-8 (1) of the Act, he or she shall take the following protective measures under Article 28-8 (4) of the Act:

1. Measures to ensure safety for protecting personal information under Article 30 (1);
2. Measures to handle grievances and resolve disputes with respect to personal information breach;
3. Other measures necessary to protect the personal information of data subjects.

(2) Where a personal information controller makes a cross-border transfer of personal information under the proviso, with the exception of the subparagraphs, of Article 28-8 (1) of the Act, it shall have a prior consultation with the recipient of the personal information on the matters specified in the subparagraphs of paragraph (1) and shall reflect the results of such consultation in the details of a contract, etc.

Article 29-11 (Standards for Orders to Suspend Cross-Border Transfers)

(1) Where the Protection Commission orders the suspension of cross-border transfers of personal information under Article 28-9 (1) of the Act, it shall comprehensively consider the following matters:

1. The type and scale of personal information, the cross-border transfer of which has been made or any further cross-border transfer of which is expected;
2. The severity of a violation of Article 28-8 (1), (4), or (5) of the Act;

3. Whether any damage that occurs or is likely to occur to data subjects is material or irrecoverable;

4. Whether ordering the suspension of cross-border transfers obviously brings more benefits to data subjects than not doing so;

5. Whether it is possible to protect personal information and to prevent personal information breach with the measures taken under the subparagraphs of Article 64 (1) of the Act;

6. Whether the recipient of personal information or the recipient country, etc. to which personal information is transferred has effective means of relieving damage suffered by data subjects;

7. Whether there is any reason to deem that it is difficult to adequately protect personal information, such as that the recipient of personal information or the recipient country, etc. to which personal information is transferred suffers a serious personal information breach.

(2) If the Protection Commission orders the suspension of cross-border transfers of personal information under Article 28-9 (1) of the Act, it shall undergo the evaluation by the expert committee for cross-border transfer.

(3) When the Protection Commission orders the suspension of cross-border transfers of personal information pursuant to Article 28-9 (1) of the Act, it shall notify in writing the relevant personal information controller of the details of and the grounds for such order, the procedures and methods for filing objections, and other necessary matters.

(4) Except as provided in paragraphs (1) through (3), matters necessary for the standards, etc. for orders to suspend cross-border transfers of personal information shall be determined and publicly notified by the Protection Commission.

Article 29-12 (Filing Objections to Orders to Suspend Cross-Border Transfers)

(1) A person who intends to file an objection pursuant to Article 28-9 (2) of the Act shall submit to the Protection Commission a written objection determined by the Protection Commission along with a document substantiating the grounds for the objection, within seven days from the date of receipt of an order to suspend cross-border transfer under Article 28-9 (1) of the Act.

(2) The Protection Commission shall notify in writing the relevant personal information controller of the results of processing a written objection submitted under paragraph (1) within 30 days from the date of receipt of the written objection.

(3) Except as provided in paragraphs (1) and (2), matters necessary for the procedures, etc. for filing an objection shall be determined and publicly notified by the Protection Commission.

CHAPTER V SAFEGUARD OF PERSONAL INFORMATION

Article 30 (Measures to Ensure Safety of Personal Information)

(1) Each personal information controller shall take the following measures to ensure safety pursuant to Article 29 of the Act: *<Amended on Sep. 12, 2023>*

1. Formulating, implementing, and examining an internal management plan that includes the following to safely process personal information:

(a) Matters regarding the management, supervision, and education of a personal information handler under Article 28 (1) of the Act (hereinafter referred to as "personal information handler");

(b) Matters regarding the composition and operation of an organization responsible for protecting personal information, including the designation of privacy officers, under Article 31 of the Act;

(c) Details necessary to implement the measures provided in subparagraphs 2 through 8;

2. The following measures to restrict access authority to personal information:

(a) Establishing and implementing the standards for granting, changing, or canceling access authority to a system systematically designed to process personal information including a database system (hereinafter referred to as "personal information processing system");

(b) Establishing and operating the standards for applying authentication means necessary to verify whether access is made by a person with legitimate authority;

(c) Other measures necessary to restrict access authority to personal information;

3. The following measures to control access to personal information:

(a) Measures necessary to detect and block intrusions into a personal information processing system;

(b) Blocking Internet access to and from computers satisfying the standards determined and publicly notified by the Protection Commission, such as the computers of personal information handlers accessing a personal information processing system: Provided, That this shall apply only to a personal information controller with an average of at least one million daily users defined in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection whose personal information is stored and managed for the immediately preceding three months as of the end of the previous year;

(c) Other measures necessary to control access to personal information;

4. The following measures necessary to safely store and transmit personal information:

(a) Storing encrypted authentication information, including the storage of one-way encrypted passwords, or other measures equivalent thereto;

(b) Encrypting information determined and publicly notified by the Protection Commission for storage, including resident registration numbers, or other measures equivalent thereto;

(c) Where the personal information or authentication information of data subjects is transmitted or received through the information and communications network defined in Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, encrypting the relevant information or other measures equivalent thereto;

(d) Other measures to ensure security using encryption or other technologies equivalent thereto;

5. The following measures to retain the records of access and prevent such records from being forged or altered in case of a personal information breach incident:

(a) Storing, inspecting, confirming, and supervising the records of access, such as the date and time when persons access a personal information processing system, and the details of processing personal information;

(b) Safely storing the records of access to a personal information processing system;

(c) Other measures necessary to retain the records of access and prevent such records from being forged or altered;

6. Installing, operating, and periodically updating and inspecting programs that can detect at all times whether any malicious program, such as a computer virus, spyware, and ransomware, intrudes into a personal information processing system and an information technology equipment used by personal information handlers for processing personal information and that can delete such malicious program;

7. Preparing storage facilities and installing locking devices to safely store personal information, or taking other physical measures;

8. Other measures necessary to ensure safety of personal information.

(2) The Protection Commission may provide necessary assistance, such as building a system with which personal information controllers can take the measures to ensure safety pursuant to paragraph (1). *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4. 2020>*

(3) Detailed standards for the measures to ensure safety under paragraph (1) shall be prescribed by Notification of the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

Article 30-2 (Measures to Ensure Safety of Personal Information Taken by Institutions Operating Public Systems)

(1) Pursuant to Article 29, a public institution which operates a personal information processing system meeting the standards publicly notified by the Protection Commission (hereafter in this Article referred to as "public system"), such as the scale of personal information processed and the number of personal information handlers granted access authority (hereafter in this Article referred to as "institution operating public systems"), shall take the following measures in addition to the measures to ensure safety under Article 30 of this Decree:

1. Including measures to ensure safety prepared for each public system in an internal management plan under Article 30 (1) 1;

2. Measures necessary to safely manage access authority, such as allowing an institution that accesses a public system to process personal information (hereafter in this Article referred to as "institution using public systems") to grant access authority to a personal information handler with legitimate authority and to change and cancel such authority;

3. Measures such as storage, analysis, inspection, and management of the records of access to public systems to prevent illegal access to personal information and personal information breach incidents.

(2) Where an institution operating public systems or an institution using public systems finds out access to personal information without authority or beyond authorized access thereto, it shall without delay notify data subjects of the relevant fact and matters necessary for the prevention of any damage, etc.; in such cases, notification shall be deemed given in any of the following cases:

1. Where data subjects are notified of loss, theft, or divulgence of personal information under Article 34 (1) of the Act;
2. Where data subjects are notified of access to their personal information and matters necessary for the prevention of any damage, etc. pursuant to other statutes or regulations.

(3) An institution operating public systems (where there is a separate public institution that develops and distributes a public system, such public institution shall be included; hereafter in this Article, the same shall apply) shall designate and operate a department dedicated to work related to the safe management of personal information or shall assign personnel dedicated to such work, taking into account the size and characteristics of the relevant public system, the number of institutions using the relevant public system, and other relevant factors.

(4) An institution operating public systems shall designate the head of a department responsible for the general management of the relevant public system as a manager for each public system: Provided, That where there is no such department, it shall designate a manager from among the heads of relevant departments in consideration of work-relatedness, work capabilities, and other relevant factors.

(5) An institution operating public systems shall establish and operate a public system operation council comprised of the following institutions for each public system to consult on matters related to examining the implementation of measures to ensure the safety of public systems and improving such systems: Provided, That where one public institution operates at least two public systems, an integrated public system operation council may be established and operated:

1. The institution operating public systems;
2. Where the operation of public systems is entrusted, the person entrusted;
3. An institution using public systems deemed necessary by the institution operating public systems.

(6) The Protection Commission may provide institutions operating public systems with support necessary to implement measures to ensure the safety of personal information.

(7) Except as provided in paragraphs (1) through (6), matters necessary for the measures to ensure the safety of personal information taken by institutions operating public systems, etc. shall be determined and publicly notified by the Protection Commission.

Article 31 (Details of Privacy Policy and Methods for Disclosure Thereof)

(1) “Matters prescribed by Presidential Decree” in Article 30 (1) 8 of the Act means the following: *<Amended on Sep. 29, 2016; Aug. 4, 2020; Sep. 12, 2023>*

1. Particulars of personal information to be processed;

2. Deleted; *<Aug. 4, 2020>*

3. Matters regarding measures to ensure the safety of personal information under Article 30.

(2) A personal information controller shall post continuously the Privacy Policy established or modified pursuant to Article 30 (2) of the Act on its website.

(3) Where it is impossible to post the Privacy Policy on the website as prescribed in paragraph (2), the personal information controller shall make public the established or modified Privacy Policy in at least one of the following manners: *<Amended on Sep. 12, 2023>*

1. Posting at easily noticeable location of the personal information controller's workplace, etc.;

2. Publishing in the Official Gazette (only in cases the personal information controller is a public institution) or general daily newspaper, weekly newspaper, or online newspaper, as defined in subparagraphs 1 (a) and (c) and 2 of Article 2 of the Act on the Promotion of Newspapers circulating mainly over the City/Do where the personal information controller's workplace, etc. is located;

3. Publishing at a periodical, newsletter, PR magazine, or invoice to be published under the same title at least twice a year and distributed to data subjects on a continual basis;

4. Stipulating in an agreement, etc. for the supply of goods or services executed between the personal information controller and the data subjects and providing a copy of the same to the data subject.

Article 31-2 (Those Subject to, and Procedures for, Evaluation of Privacy Policy)

(1) Where the Protection Commission evaluates the Privacy Policy under Article 30-2 (1) of the Act, it shall select those subject to such evaluation, comprehensively considering the following matters:

1. The type and sales of a personal information controller;

2. The type and scale of personal information processed, such as sensitive information and personally identifiable information;

3. The legal grounds and methods for personal information processing;

4. Whether any statute is violated;

5. The characteristics of data subjects, such as children and youth.

(2) Upon selecting those subject to the evaluation of the Privacy Policy pursuant to paragraph (1), the Protection Commission shall notify the relevant personal information controller of an evaluation plan including the details, time schedule, procedures, etc. of the evaluation no later than 10 days before the commencement of the evaluation.

(3) Where necessary to evaluate the Privacy Policy under Article 30-2 of the Act, the Protection Commission may request the relevant personal information controller to present its opinion.

(4) The Protection Commission shall evaluate the Privacy Policy pursuant to Article 30-2 of the Act and notify the relevant personal information controller of the results of such evaluation without delay.

(5) Except as provided in paragraphs (1) through (4), the detailed standards and procedures for selecting those subject to the evaluation of the Privacy Policy shall be determined and publicly notified by the Protection Commission.

Article 32 (Work of Privacy Officer and Requirements for Designation)

(1) "Work prescribed by Presidential Decree" in Article 31 (2) 7 of the Act means the following:

1. To establish, modify, and implement the Privacy Policy pursuant to Article 30 of the Act;
2. To manage materials related to the protection of personal information;
3. To destroy personal information whose purpose of processing is attained or retention period expires.

(2) A personal information controller shall designate a privacy officer pursuant to Article 31 (1) of the Act according to the following classifications: <*Amended on Jul. 22, 2016*>

1. Public institutions: Public officials, etc. who satisfy the below standards:

   (a) The administrative bodies of the National Assembly, the Court, the Constitutional Court, and the National Election Commission; and central administrative agencies: A member of the Senior Executive Service (hereinafter referred to as "senior executive") or equivalent public official;

   (b) Other national agencies than item (a), headed by a public official in political service: A public official of Grade III or higher (including a senior executive) or equivalent thereto;

   (c) Other national agencies than items (a) and (b), headed by a senior executive, a Grade III or higher public official, or an equivalent public official: A public official of Grade IV or higher or equivalent thereto;

   (d) Other national agencies than items (a) through (c) (including their affiliated bodies): The head of a department in charge of the work related to personal information processing in the relevant agency;

   (e) City/Do, City/Do Offices of Education: A public official of Grade III or higher or equivalent thereto;

   (f) Si/Gun or autonomous Gu: A public official of Grade IV or equivalent thereto;

   (g) Schools of each level referred to in subparagraph 5 of Article 2: A person who takes overall control of the administrative affairs of the relevant school;

   (h) Other public institutions than items (a) through (g): The head of a department in charge of the work related to personal information processing in the relevant institution: Provided, That, where the heads of at least two departments are in charge of the work related to personal information processing, the head of the relevant institution shall designate the privacy officer from among them;

2. An institution other than public institutions: Any of the following persons:

   (a) The business owner or representative;

   (b) An executive officer (or the head of a department in charge of the work related to personal information processing, if no executive officer exists).

(3) Notwithstanding paragraph (2), if the personal information controller is a micro enterprise defined in Article 2 of the Framework Act on Micro Enterprises, it shall be deemed that the enterprise owner or representative has been designated as the privacy officer without separate designation: Provided, that this shall not apply if the personal information controller has separately designated a privacy officer. <*Newly Inserted on Aug. 4, 2020; Feb. 2, 2021*>

(4) The Protection Commission may provide necessary assistance, such as developing and providing educational programs for privacy officers so that they may efficiently perform the work provided for in Article 31 (2) of the Act. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

Article 32-2 (Scope of Those to Be Designated as Domestic Agents)

(1) “Who is prescribed by Presidential Decree” in the former part, with the exception of the subparagraphs, of Article 31-2 (1) of the Act means any of the following persons:

1. A person whose total sales for the previous year (referring to the previous business year in the case of a corporation) is at least one trillion won;
2. A person who has an average of at least one million domestic data subjects whose personal information is stored and managed for the immediately preceding three months as of the end of the previous year;
3. A person who is requested to submit relevant materials, such as articles and documents, pursuant to Article 63 (1) of the Act and for whom the Protection Commission deliberates and resolves on the need to designate a domestic agent.

(2) The total sales under paragraph (1) 1 shall be based on the amount converted into Korean won by applying the average exchange rate for the previous year.

Article 33 (Registered Matters of Personal Information Files)

(1) “Matters prescribed by Presidential Decree” in Article 32 (1) 7 of the Act means the following: *<Amended on Sep. 12, 2023>*

1. The name of the public institution that operates personal information files;
2. The number of data subjects whose personal information is retained in personal information files;
3. The department in charge of the work related to personal information processing in the relevant public institution;
4. The department that receives and processes requests for access to personal information pursuant to Article 41;
5. The scope of personal information to which access can be limited or denied pursuant to Article 35 (4) of the Act, among personal information in personal information files, and the grounds for limitation or denial.

(2) "Personal information files prescribed by Presidential Decree" in Article 32 (2) 4 of the Act means any of the following information files: *<Newly Inserted on Sep. 22, 2023>*

1. Personal information files that are operated to perform simple work, such as paying allowances for attending meetings, sending data and goods, and settling money, and that have little need for continuous management;
2. Personal information files that are urgently necessary for the public safety and security, public health, etc., and that are processed temporarily;

3. Other personal information files that are collected to handle one-off work and that are not stored or recorded.

Article 34 (Registration and Disclosure of Personal Information Files)

(1) The head of a public institution that operates personal information files (excluding the personal information files under Article 32 (2) of the Act and Article 33 (2) of this Decree; hereafter in this Article, the same shall apply) shall file for registration of the matters provided in Article 32 (1) of the Act and Article 33 (1) of this Decree (hereinafter referred to as "registered matters") with the Protection Commission within 60 days from the date it starts operating the personal information files, as prescribed by Notification of the Protection Commission. The same shall also apply to any modification of registered matters. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020; Sep. 12, 2023>*

(2) The Protection Commission shall post the status of personal information files registered pursuant to Article 32 (4) of the Act on the website established by the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020; Sep. 12, 2023>*

(3) The Protection Commission may build and operate a system so that the registration or modification of the registered matters, referred to in paragraph (1), of personal information files may be electronically processed. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

Article 34-2 (Criteria, Method, and Procedure for Certification of Personal Information Protection)

(1) The Protection Commission shall determine and publicly notify the criteria for certification referred to in Article 32-2 (1) of the Act, including the establishment of managerial, technical, and physical safeguards to protect personal information, taking into account the matters provided in the subparagraphs of Article 30 (1). *<Amended on Jul. 26, 2017; Aug. 4, 2020; Sep. 12, 2023>*

(2) A person who intends to obtain certification of personal information protection pursuant to Article 32-2 (1) of the Act (hereafter in this Article and Article 34-3, referred to as "applicant"), shall submit an application (including an electronic application) for certification of personal information protection which includes the following matters to an institution specializing in the certification of personal information protection referred to in Article 34-6 (hereinafter referred to as "certification institution"):

1. A list of personal information processing systems subject to certification;
2. Methods and procedures for establishing and operating the personal information protection system;
3. A list of documents related to the personal information protection system and the implementation of safeguards.

(3) Upon receipt of an application for certification pursuant to paragraph (2), a certification institution shall consult with the applicant regarding the scope, time schedule, etc. of certification.

(4) An examination to certify personal information protection under Article 32-2 (1) of the Act shall be either a paper-based examination or an on-site examination conducted by the certification examiners for personal information protection subject to Article 34-8.

(5) Each certification institution shall establish and operate a certification committee comprised of members with extensive knowledge and experience in information protection to deliberate on the results of examinations for certification conducted pursuant to paragraph (4).

(6) Except as provided in paragraphs (1) through (5), detailed matters necessary for certification of personal information protection, including filing an application for certification, examination for certification, establishment and operation of the certification committee, and issuance of certificates, shall be prescribed by Notification of the Protection Commission. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 34-3 (Fees for Certification of Personal Information Protection)

(1) Each applicant shall pay a fee incurred in examining certification of personal information protection to the certification institution.

(2) The Protection Commission shall provide Notification of the detailed standards for calculating fees referred to in paragraph (1), based upon the number of certification examiners required for examining certification of personal information protection, number of days necessary to examine certification, and other relevant matters. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 34-4 (Revocation of Certification)

(1) A certification institution that intends to revoke certification of personal information protection pursuant to Article 32-2 (3) of the Act shall submit the case for deliberation and resolution by the certification committee established under Article 34-2 (5).

(2) Upon revoking certification pursuant to Article 32-2 (3) of the Act, the Protection Commission or the certification institution shall notify the affected party of such revocation; and shall publicly announce or post the same in the Official Gazette or on the certification institution's website. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 34-5 (Follow-up Management of Certification)

(1) An examination for follow-up management subject to Article 32-2 (4) of the Act shall be either a paper-based examination or an on-site examination.

(2) Where a certification institution discovers any of the causes provided for in Article 32-2 (3) of the Act through its follow-up management pursuant to paragraph (1), the certification institution shall submit the case for deliberation by the certification committee established under Article 34-2 (5) for deliberation; and shall notify the Protection Commission of the results of such deliberation. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 34-6 (Institutions Specializing in Certifying Personal Information Protection)

(1) "Specialized institutions prescribed by Presidential Decree" in Article 32-2 (5) of the Act means the following: *<Amended on Sep. 29, 2016; Jul. 26, 2017; Aug. 4, 2020>*

1. The Korea Internet and Security Agency;

2. A corporation or an organization or institution designated by Notification of the Protection Commission among the corporations, organizations or institutions that satisfy all of the following requirements:

(a) To have at least five certification examiners for personal information protection referred to in Article 34-8;

(b) To have been qualified by the Protection Commission through an examination of requirements and capacity for performing its work.

(2) Detailed criteria, etc. necessary for designating a corporation, organization or institution referred to in paragraph (1) 2 and revocation of such designation shall be determined by Notification of the Protection Commission. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 34-7 (Certification Mark and Promotion)

Where a person who has obtained certification pursuant to Article 32-2 (6) of the Act intends to indicate or promote the certification, the person may use the personal information protection mark prescribed by Notification of the Protection Commission. In such cases, the person shall also indicate the scope and term of validity of the certification in the personal information protection mark. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 34-8 (Qualifications for Certification Examiners for Personal Information Protection and Grounds for Disqualification)

(1) A certification institution shall qualify persons with expertise in personal information protection, who pass an examination after having completed a specialized educational program necessary for certification examinations, as certification examiners for personal information protection (hereinafter referred to as "certification examiners") pursuant to Article 32-2 (7) of the Act.

(2) A certification institution may disqualify a certification examiner pursuant to Article 32-2 (7) of the Act in any of the following cases: Provided, that the certification examiner must be disqualified in cases falling under subparagraph 1:

1. Where the certification examiner has been qualified by fraud or other unjust means;

2. Where the certification examiner has received money, goods, or other profits in relation to the examination for certification of personal information protection;

3. Where the certification examiner has divulged any information acquired in the course of examining the certification of personal information protection, or has used such information for other than the purpose for work without good cause.

(3) Detailed matters concerning completion of the specialized educational programs, qualification and disqualification as certification examiners, and other relevant matters under paragraphs (1) and (2) shall be prescribed by Notification the Protection Commission. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

Article 35 (Object of Privacy Impact Assessment)

"Personal information files meeting the criteria prescribed by Presidential Decree" in Article 33 (1) of the Act means any of the following personal information files that can be processed electronically: *<Amended on Sep. 29, 2016>*

1. Personal information files that will be established, operated, or modified, and contain sensitive information or personally identifiable information of at least 50 thousand data subjects for processing;
2. Personal information files that is established and operated, and will be matched with other personal information files being established and operated inside or outside the relevant public institution, and, as a result of matching, will contain the personal information of at least 500 thousand data subjects;
3. Personal information files that will be established, operated, or modified, and contain the personal information of at least one million data subjects;
4. Personal information files whose operating system, including the data retrieval system, will be changed after the privacy impact assessment under Article 33 (1) of the Act (hereinafter referred to as "privacy impact assessment"). In such cases, the privacy impact assessment shall be limited to the changed system.

Article 36 (Designation of Assessment Institutions and Revocation of Designation)

(1) The Protection Commission may designate a corporation that satisfies all of the following requirements as a privacy impact assessment institution (hereinafter referred to as "assessment institution") pursuant to Article 33 (2) of the Act: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Dec. 22, 2015; Jul. 26, 2017; Aug. 4, 2020; Sep. 12, 2023>*

1. A corporation whose total revenue derived from any of the following work is 200 million won or more during the last five years:
   (a) Privacy impact assessments or work similar thereto;
   (b) Data protection consulting (which means the analysis and assessment of information systems and the provision of corresponding countermeasures against electronic infringement incidents; hereinafter the same shall apply) among the work related to establishing information systems, as defined in subparagraph 13 of Article 2 of the Electronic Government Act (including the information protection system);
   (c) Data protection consulting among the work related to monitoring information systems, as defined in subparagraph 14 of Article 2 of the Electronic Government Act;
   (d) Data protection consulting among the work related to the information security industry defined in Article 2 (1) 2 of the Act on the Promotion of the Information Security Industry;
   (e) Work prescribed in Article 23 (1) 1 and 2 of the Act on the Promotion of the Information Security Industry;

2. A corporation that employs at least 10 full-time experts who meet the qualification requirements determined and publicly notified by the Protection Commission, including work experience in the field related to privacy impact assessment;

3. A corporation with the following offices and facilities:

(a) An office with facilities for identification and access control;

(b) Facilities for the safe management of records and materials.

(2) A person who intends to be designated as an assessment institution shall file an application for designation as an assessment institution, in the form prescribed by Notification of the Protection Commission, with the Protection Commission, along with the following documents (including electronic documents; hereinafter the same shall apply): *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>*

1. The articles of incorporation;

2. The representative's name;

3. Documents verifying the qualifications of the experts referred to in paragraph (1) 2;

4. Other documents prescribed by Notification of the Protection Commission.

(3) Upon receipt of an application for designation as an assessment institution filed under paragraph (2), the Protection Commission shall verify the following documents through the sharing of administrative information pursuant to Article 36 (1) of the Electronic Government Act: Provided, That where the applicant does not give consent to the verification of subparagraph 2, the Protection Commission shall require the applicant to submit the relevant document: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

1. The corporation registration certificate;

2. The certificate of alien registration issued under Article 88 (2) of the Immigration Act (applicable only to aliens).

(4) Upon designating an assessment institution pursuant to paragraph (1), the Protection Commission shall, without delay, issue a written designation to the relevant applicant, and provide Notification thereof in the Official Gazette. The same shall also apply to any revision to the Notification: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

1. The name, address, and telephone number of the assessment institution, and the name of its representative;

2. Terms and conditions attached to the designation, if any.

(5) "Cases that fall under any ground prescribed by Presidential Decree" in Article 33 (7) 5 of the Act means any of the following cases: *<Amended on Sep. 12, 2023>*

1. Where an assessment institution fails to comply with the obligation to submit a report under paragraph (6);

2. Where an assessment institution has no records of privacy impact assessment for two consecutive years from the date of obtaining designation without good cause;

3. Where an assessment institution divulges any information that it has obtained in the course of conducting privacy impact assessments, such as a privacy impact assessment report under the provisions, with the exception of the subparagraphs, of Article 38 (2);

4. Other cases where an assessment institution breaches the duties under the Act or this Decree.

(6) An assessment institution designated under paragraph (1) shall, upon occurrence of any of the following events after designation, submit a report to the Protection Commission, as prescribed by Notification the Protection Commission, within 14 days from the date of occurrence: Provided, that it shall submit a report to the Protection Commission within 60 days from the date of occurrence in cases falling under subparagraph 3: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>*

1. Where any matter referred to in paragraph (1) is changed;

2. Where any matter referred to in paragraph (4) 1 is changed;

3. Where the transfer, acquisition, or merger of the assessment institution, or similar event occurs.

(7) Deleted. *<Sep. 12, 2023>*

[Moved from Article 37; previous Article 36 moved to Article 37 *<Sep. 12, 2023>]*

Article 37 (Consideration at the time of Privacy Impact Assessment)

"Matters prescribed by Presidential Decree" in Article 33 (3) 4 of the Act means the following: *<Amended on Sep. 12, 2023>*

1. Whether sensitive information or personally identifiable information will be processed;

2. The retention period of personal information.

[Moved from Article 36; previous Article 37 moved to Article 36 *<Sep. 12, 2023>]*

Article 38 (Criteria for Privacy Impact Assessment)

(1) The criteria for privacy impact assessments (hereinafter referred to as "assessment criteria") under Article 33 (9) of the Act shall be as follows: *<Amended on Jul. 22, 2016; Sep. 12, 2023>*

1. The type and nature of personal information contained in the relevant personal information files, the number of data subjects, and the possibility of subsequent personal information breach;

2. The level of measures to ensure safety taken under Articles 23 (2), 24 (3), 24-2 (2), 25 (6) (including cases applied mutatis mutandis in Article 25-2 (4)), and 29 of the Act, and the subsequent possibility of personal information breach;

3. Countermeasures against risk factors of personal information breach, if any;

4. Other necessary measures subject to the Act or this Decree, or any factor affecting breach of duties.

(2) An assessment institution requested to conduct a privacy impact assessment under Article 33 (2) of the Act shall, in accordance with the assessment criteria, analyze and assess the risk factors of personal information breaches that result from the operation of personal information files, and shall prepare a privacy impact assessment report based on the results of the evaluation that includes the following and send such report to the head of the relevant public institution, who shall submit the report to the Protection

Commission before operating and changing personal information files falling under the subparagraphs of Article 35: *<Amended on Sep. 12, 2023>*

1. Those subject to the privacy impact assessment and the scope thereof;
2. Fields and items of the evaluation;
3. Analysis and assessment of the risk factors of personal information breaches in accordance with the assessment criteria;
4. The details of measures taken based on the results of the analysis and evaluation under subparagraph 3 and a plan for improvement;
5. The results of the privacy impact assessment;
6. A summary of the matters prescribed in subparagraphs 1 through 5.

(3) The Protection Commission or the head of a public institution may disclose the details of a summary of a privacy impact assessment report prescribed in paragraph (2) 6. *<Newly Inserted on Sep. 12, 2023>*

(4) Except as provided in the Act and this Decree, the Protection Commission may determine and publicly notify the detailed standards for designating assessment institutions, procedures for privacy impact assessments, etc. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020; Sep. 12, 2023>*

Article 39 (Notification of Divulgence of Personal Information)

(1) When a personal information controller becomes aware of loss, theft, or divulgence (hereafter in this Article and Article 40 referred to as "divulgence, etc.") of personal information, the personal information controller shall notify data subjects of the matters specified in the subparagraphs of Article 34 (1) of the Act in writing, etc. within 72 hours: Provided, That notification may be given to data subjects without delay after the relevant cause ceases to exist in any of the following cases:

1. Where urgent measures need to be taken to prevent widespread divulgence, etc. of personal information and any further divulgence, etc., such as blocking access routes, inspecting and addressing vulnerabilities, and recovering and deleting the relevant personal information;
2. Where it is impracticable to give notification within 72 hours due to a natural disaster or any other unavoidable cause.

(2) Notwithstanding paragraph (1), where a personal information controller intends to give notification under paragraph (1) but fails to confirm the specific details of the matters prescribed in Article 34 (1) 1 or 2 of the Act, the personal information controller shall first give notification of the divulgence of personal information, the details that have already been confirmed, and the matters specified in Article 34 (1) 3 through 5 of the Act in writing, etc., and shall notify the details further confirmed immediately upon confirmation.

(3) Notwithstanding paragraphs (1) and (2), where the contact information of a data subject is unknown or any other good cause exists, a personal information controller shall post the matters provided in the subparagraphs of Article 34 (1) of the Act on its website for at least 30 days to ensure that the data subject can easily recognize such matters, in lieu of giving notification under paragraphs (1) and (2), pursuant to

the proviso, with the exception of the subparagraphs, of Article 34 (1) of the Act: Provided, That in the case of a personal information controller that does not operate its website, the matters specified in the subparagraphs of Article 34 (1) of the Act may be posted at a conspicuous place of the workplace, etc. for at least 30 days in lieu of giving notification under paragraphs (1) and (2).

[Moved from Article 40; previous Article 39 moved to Article 40 *<Sep. 12, 2023>*]

Article 40 (Reporting on Divulgence of Personal Information)

(1) When a personal information controller becomes aware of divulgence, etc. of personal information in any of the following cases, the personal information controller shall, in writing, etc., file a report with the Protection Commission or a specialized institution prescribed in the former part of Article 34 (3) of the Act with regard to the matters provided in the subparagraphs of Article 34 (1) of the Act within 72 hours: Provided, That where it is impracticable to file a report within 72 hours due to a natural disaster or any other unavoidable cause, a report may be filed without delay after the relevant cause ceases to exist; and where the possibility of infringing on the rights and interests of data subjects is substantially reduced after the path of divulgence, etc. of personal information is confirmed and measures are taken such as the recovery and deletion of the relevant personal information, the personal information controller need not file a report thereon:

1. Where divulgence, etc. of personal information of at least 1,000 data subjects occurs;
2. Where divulgence, etc. of sensitive information or personally identifiable information occur;
3. Where divulgence, etc. of personal information occurs due to illegal external access to personal information processing systems or information technology equipment used by personal information handlers for processing personal information.

(2) Notwithstanding paragraph (1), where a personal information controller intends to file a report pursuant to paragraph (1) but fails to confirm the specific details of the matters provided in Article 34 (1) 1 or 2 of the Act, the personal information controller shall first file a report on divulgence, etc. of personal information, the details that have already been confirmed, and the matters specified in Article 34 (1) 3 through 5 of the Act in writing, etc., and shall notify the details further confirmed immediately upon confirmation.

(3) "Specialized institution designated by Presidential Decree" in the former and latter parts of Article 34 (3) of the Act means the Korea Internet and Security Agency.

[Moved from Article 39; previous Article 40 moved to Article 39 *<Sep. 12, 2023>*]

Article 40-2 (Institution Requesting Erasure and Blocking of Exposed Personal Information)

“Specialized institution designated by Presidential Decree” in Article 34-2 (2) of the Act means the Korea Internet and Security Agency.

CHAPTER VI GUARANTEE OF RIGHTS OF DATA SUBJECTS

Article 41 (Procedures for Access to Personal Information)

(1) A data subject who intends to request access to his or her own personal information processed by a personal information controller pursuant to Article 35 (1) of the Act shall submit a request, stating the information that he or she intends to access among the following information, in the manner and following the procedure determined by the personal information controller; *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017>*

1. Particulars and substance of personal information;
2. The purpose of collecting and using personal information;
3. The period for retaining and using personal information;
4. Status of personal information provided to a third party;
5. The fact that the data subject has given consent to the processing of his or her personal information and the content thereof.

(2) To determine the manner and procedure for requesting access under paragraph (1), a personal information controller shall comply with the following to ensure that such manner and procedure are not more difficult than the manner and procedure that the personal information controller uses to collect the relevant personal information: *<Newly Inserted on Oct. 17, 2017>*

1. To provide the requested personal information in a data subject-friendly manner, such as in writing, by telephone or electronic mail, or via the Internet;
2. To allow data subjects to request access to their own personal information at least through the same window or in the same manner that the personal information controller uses to collect such personal information, unless good cause exists, such as difficulty in continuously operating such window;
3. To post on a website the manner and procedure for requesting access if the personal information controller operates the website.

(3) A data subject who intends to request access to his or her own personal information via the Protection Commission pursuant to Article 35 (2) of the Act shall submit to the Protection Commission a Personal Information Access Request specifying the information to access among the information referred to in paragraph (1), as prescribed by Notification of the Protection Commission. In such cases, the Protection Commission shall forward the Personal Information Access Request to the relevant public institution without delay. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>*

(4) “Period prescribed by Presidential Decree” in the former part of Article 35 (3) of the Act means 10 days. *<Amended on Oct. 17, 2017>*

(5) Where a personal information controller allows a data subject to access the relevant personal information within 10 days from the receipt of the Personal Information Access Request under paragraph (1) or (3), or limits access to the relevant person information under Article 42 (1), the personal information controller shall serve the data subject with the Access Notice, stating the accessible personal information,

date and time, venue, etc. for access (in the case of partial access pursuant to Article 42 (1), the ground therefor and how to appeal shall be included), in the form prescribed by Notification of the Protection Commission: Provided, That where he or she allows immediate access, the Access Notice may be omitted. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>*

Article 42 (Limitation to, and Postponement and Denial of, Access to Personal Information)

(1) Where any information to which a personal information controller receives a request for access pursuant to Article 41 (1) falls under Article 35 (4) of the Act, the personal information controller may limit access to such information; and shall allow the data subject to access other personal information than the restricted part.

(2) Where a personal information controller intends to postpone a data subject's access to his or her own personal information pursuant to the latter part of Article 35 (3) of the Act, or to deny the access pursuant to Article 35 (4) of the Act, the personal information controller shall serve the data subject with the Access Postponement or Denial Notice, stating the grounds for postponement or denial and how to appeal, in the form prescribed by Notification of the Protection Commission within 10 days from the receipt of the access request. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

Article 43 (Correction, and Erasure of Personal Information)

(1) A data subject who intends to request a personal information controller to correct or erasure his or her own personal information pursuant to Article 36 (1) of the Act shall submit a request in the manner and following the procedure determined by the personal information controller. In such cases, Article 41 (2) shall apply mutatis mutandis where the personal information controller determines the manner and procedure for requesting the correction or erasure of personal information; and "access" shall be construed as "correction or erasure". *<Amended on Oct. 17, 2017>*

(2) Upon receipt of a request to correct or erasure personal information pursuant to Article 36 (1) of the Act, a personal information controller who processes personal information files provided by other personal information controller shall correct or erase the relevant personal information as requested; or shall, without delay, notify the personal information controller who has provided the relevant personal information of the request to correct or erasure the personal information, and take necessary measures based on the result of such processing. *<Amended on Oct. 17, 2017>*

(3) A personal information controller shall inform the relevant data subject of the fact that he or she has duly corrected or erased the relevant personal information pursuant to Article 36 (2) of the Act within 10 days from the receipt of a request to correct or erasure personal information under paragraph (1) or (2); otherwise, if the erasure of personal information is denied because it falls under the proviso of Article 36 (1) of the Act, the personal information controller shall serve the data subject with the Personal Information Correction or erasure Outcome Notice, stating the fact and grounds for the denial and how to appeal, in the form determined and publicly notified by prescribed by Notification of the Protection

Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>*

Article 44 (Suspension of Processing Personal Information)

(1) A data subject who intends to request a personal information controller to suspend the processing of his or her own personal information pursuant to Article 37 (1) of the Act shall submit a request in the manner and following the procedure determined by the personal information controller. In such cases, Article 41 (2) shall apply mutatis mutandis where the personal information controller determines the manner and procedure for requesting the suspension of processing personal information; and "access" shall be construed as "suspension of processing". *<Amended on Oct. 17, 2017>*

(2) A personal information controller shall inform the relevant data subject of the fact that it has duly suspended the processing of personal information pursuant to the main clause of Article 37 (2) of the Act within 10 days from the receipt of a request to suspend the processing of personal information made under paragraph (1); otherwise, if the suspension of processing personal information is denied because it falls under the proviso of Article 37 (2) of the Act, the personal information controller shall serve the relevant data subject with the Personal Information Processing Suspension Outcome Notice, stating the fact and grounds for the denial and how to appeal, in the form prescribed by Notification of the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>*

Article 45 (Scope of Representative)

(1) A person who can represent a data subject under Article 38 of the Act shall be any of the following:

1. A legal representative of the data subject;
2. A person delegated by the data subject.

(2) A representative referred to in paragraph (1), representing a data subject pursuant to Article 38 of the Act, shall submit a power of attorney of the data subject, in the form prescribed by Notification of the Protection Commission, to the personal information controller. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

Article 46 (Confirmation of Data Subjects or Representatives)

(1) Upon receipt of a request for access under Article 41 (1), correction or erasure of personal information under Article 43 (1), suspension of processing of personal information or withdrawal of consent under Article 37 (1) of the Act (hereafter in this Article and Articles 47 and 48 referred to as "request for access, etc."), a personal information controller shall confirm whether the person who has submitted the request for access, etc. is the principal or the duly authorized representative. *<Amended on Aug. 4, 2020; Sep. 12, 2023>*

(2) Any personal information controller, which is a public institution eligible for the sharing of administrative information pursuant to Article 36 (1) of the Electronic Government Act, shall confirm as provided in paragraph (1) through the sharing of administrative information: Provided, that this shall not

apply where the public institution is unable to share administrative information or the data subject does not consent to such confirmation.

Article 47 (Amounts of Fees)

(1) The amounts of fees and postage provided for in Article 38 (3) of the Act shall be determined by the relevant personal information controller within the actual expenses necessary for the processing of the request for access, etc.: Provided, that where a personal information controller is a local government, they shall be prescribed by ordinance of the relevant local government.

(2) A personal information controller shall not demand any fee or postage if the cause for submitting the request for access, etc. lies with the personal information controller.

(3) Any fee and postage provided in Article 38 (3) of the Act shall be paid as follows: Provided, that a personal information controller, which is the National Assembly, the Court, the Constitutional Court, the National Election Commission, a central administrative agency, or its affiliated body (hereafter in this Article referred to as "national agency") or a local government, may claim such fee and postage by the electronic payment means defined in subparagraph 11 of Article 2 of the Electronic Financial Transactions Act, or telecommunications billing services defined in Article 2 (1) 10 of the Act on Promotion of Information and Communications Network Utilization and Information Protection: *<Amended on Sep. 12, 2023>*

1. Where the fee or postage is paid to a personal information controller that is a national agency: Revenue stamp;
2. Where the fee or postage is paid to a personal information controller that is a local government: Revenue certificate;
3. Where the fee and postage is paid to other personal information controller than a national agency or local government: In the manner determined by the relevant personal information controller.

Article 48 (Establishing Access Request Support System)

(1) A personal information controller may establish and operate a support system that enables the request for access, etc. to be processed and notified electronically, and determine other work procedures.

(2) The Protection Commission may establish and operate a system to support the public institutions which are personal information controllers efficiently process the request for access, etc. for personal information they possess and notify the results thereof. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

CHAPTER VI-2 Deleted.

Article 48-2 Deleted. *<Sep. 12, 2023>*

Article 48-3 Deleted. <*Sep. 12, 2023*>

Article 48-4 Deleted. <*Sep. 12, 2023*>

Article 48-5 Deleted. <*Sep. 12, 2023*>

Article 48-6 Deleted. <*Sep. 12, 2023*>

Article 48-7 (Scope, and Standards of the Parties Required to Purchase an Insurance for Performance of Damage Compensation Responsibilities)

(1) A provider of information and communications services meeting all of the following requirements (referring to those who fall under Article 2 (1) 3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection; hereafter in this Article, the same shall apply) and a person who is provided by such provider with the personal information of users (referring to those who fall under Article 2 (1) 4 of that Act; hereafter in this Article, the same shall apply) under Article 17 (1) 1 of the Act shall purchase insurance or join a mutual aid organization or accumulate reserves pursuant to Article 39-9 (1) of the Act: <*Amended on Sep. 12, 2023*>

1. The Information and Communications Service Providers, etc. whose sales revenue for the previous business year (the previous business year for a corporation) was 50 million won or more;
2. The Information and Communications Service Providers, etc. who stored and managed personal information of one thousand users or more on average per day during the three-month period immediately preceding the end of the previous year.

(2) The standards for the minimum insurance subscription amount (referring to a minimum reserve amount in cases of accumulating reserves; hereafter in this Article the same shall apply) applicable to the Subject Personal Information Controllers (referring to a provider of information and communications services meeting all of the requirements specified in the subparagraphs of paragraph (1) and a person who is provided by such provider with the personal information of users under Article 17 (1) 1 of the Act; hereafter in this Article, the same shall apply) in cases of purchasing insurance, joining a mutual aid organization or accumulating reserves shall be as set forth in attached Table 1-4: Provided, that if any Subject Personal Information Controller purchases insurance or joins a mutual aid organization, and accumulates reserves at the same time, the sum of the insured or mutual aid amount and reserves shall be equal to or exceed the minimum insurance subscription amount set forth in attached Table 1-4. <*Amended on Sep. 12, 2023*>

(3) If a Subject Personal Information Controller purchases insurance, joins a mutual aid organization or accumulates reserves which guarantee the performance of the damage liabilities under Articles 39 and 39-2 of the Act in accordance with other statutes, the Subject Business Entity shall be deemed to have

purchased insurance, joined a mutual aid organization or accumulated reserves pursuant to Article 39-9 (1) of the Act.

Article 48-8 Deleted. *<Sep. 12, 2023>*

Article 48-9 Deleted. *<Sep. 12, 2023>*

Article 48-10 Deleted. *<Sep. 12, 2023>*

Article 48-11 Deleted. *<Sep. 12, 2023>*

Article 48-12 Deleted. *<Sep. 12, 2023>*

Article 48-13 Deleted. *<Sep. 12, 2023>*

CHAPTER VIII PERSONAL INFORMATION DISPUTE MEDIATION

Article 48-14 (Ex Officio Members)

The ex officio members of the Dispute Mediation Committee shall be appointed by the Chairperson of the Protection Commission from among members in general service of the Senior Executive Service of the Protection Commission, who are in charge of the work related to the protection of personal information. *<Amended on Jul. 26, 2017; Aug. 4, 2020>*

[Moved from Article 48-2 *<Aug. 4, 2020>]*

Article 49 (Composition and Operation of Mediation Panels)

(1) The mediation panel referred to in Article 40 (6) of the Act (hereinafter referred to as “mediation panel”) shall be comprised of up to five members appointed by the chairperson of the Dispute Mediation Committee, and one of whom shall be a commissioner with an attorney-in-law license. *<Amended on Jul. 22, 2016>*

(2) The chairperson of the Dispute Mediation Committee shall convene the meetings of the mediation panel.

(3) The chairperson of the Dispute Mediation Committee shall notify each member of the mediation panel of the date, time, venue, and agenda no later than seven days prior to the meeting: Provided, That this shall not apply in case of emergency.

(4) The presider of the mediation panel shall be elected by and from among its members.

(5) Except as provided in paragraphs (1) through (4), matters necessary for the composition and operation of the mediation panel, and other necessary matters, shall be determined by the chairperson of the Dispute Mediation Committee subject to the resolution of the Dispute Mediation Committee.

Article 49-2 (Specialized Committee for Dispute Mediation)

(1) The Dispute Mediation Committee may establish a specialized committee for each field (hereinafter referred to as "specialized committee for dispute mediation") to conduct a specialized examination of the matters related to mediation of disputes regarding personal information.

(2) Each specialized committee for dispute mediation shall be composed of up to 10 members, including one chairperson.

(3) Members of each specialized committee for dispute mediation shall be appointed or commissioned by the chairperson of the Dispute Mediation Committee from among the following persons, and the chairperson of each specialized committee for dispute mediation shall be designated by the chairperson of the Dispute Mediation Committee from among the members of the relevant specialized committee for dispute mediation:

1. A member of the Dispute Mediation Committee;
2. A relevant public official of a central administrative agency who is responsible for work related to personal information protection;
3. A person who holds or has held the position of assistant professor or higher in a university or college in the field of personal information protection;
4. A person who has at least five years' research experience at an accredited research institute in the field related to personal information protection;
5. A person who has at least one year's work experience in the field related to personal information protection after being qualified as an attorney-at-law;
6. Other persons with extensive expertise and experience in personal information protection and dispute mediation.

(5) Except as provided in paragraphs (1) through (3), matters necessary for the composition, operation, etc. of specialized committees for dispute mediation shall be determined by the chairperson of the Dispute Mediation Committee following its resolution.

Article 50 (Secretariat)

(1) The secretariat of the Protection Commission shall conduct administrative affairs necessary for dispute mediation, such as receiving dispute mediation cases and fact-finding pursuant to Article 40 (8) of the Act. *<Amended on Aug. 4, 2020>*

(2) The secretariat may establish and operate a dispute mediation system in order to electronically process the business affairs required for dispute mediation, including receiving dispute mediation requests, advancing the dispute mediation process and providing notifications to the parties. *<Newly Inserted on Aug.*

4, 2020>

Article 51 (Operation of Dispute Mediation Committee)

(1) The chairperson of the Dispute Mediation Committee shall convene and preside over meetings of the Dispute Mediation Committee.

(2) The chairperson of the Dispute Mediation Committee shall notify each member of the Dispute Mediation Committee of the date, time, venue, and agenda no later than seven days prior to the meeting: Provided, That this shall not apply in case of emergency.

(3) The meetings of the Dispute Mediation Committee and the mediation panel shall not be open to the public: Provided, That attendance of the parties or interested parties is allowed by the resolution of the Dispute Mediation Committee, if deemed necessary.

Article 51-2 (Notification of Intention Not to Respond to Mediation)

Where a personal information controller intends not to respond to dispute mediation due to any compelling reason under Article 43 (3) of the Act, the personal information controller shall notify the Dispute Mediation Committee of such intention specifying the grounds therefor within 10 days from the date of being notified of dispute mediation.

Article 51-3 (Secretariat of, and Investigation and Inspection by, Dispute Mediation Committee)

(1) "Secretariat prescribed by Presidential Decree" in the former part of Article 45 (2) of the Act means the secretariat of the Protection Commission, which is in charge of conducting administrative affairs necessary for dispute mediation pursuant to Article 50 (1).

(2) Where the Dispute Mediation Committee intends to conduct an investigation or inspection pursuant to Article 45 (2) of the Act, it shall notify a person subject to such investigation or inspection of the following matters in writing no later than seven days before the investigation or inspection: Provided, That where the purpose of the investigation or inspection is likely to be compromised, prior notification need not be given:

1. The purpose of the investigation and inspection;
2. The period and place of the investigation and inspection;
3. The position and name of a person who conducts the investigation or inspection;
4. The scope and details of the investigation and inspection;
5. The fact that the person may refuse the investigation or inspection, where there is good cause;
6. The details of disadvantageous measures, where the person refuses, obstructs, or evades the investigation or inspection without good cause;
7. Other matters necessary for the investigation or inspection for dispute mediation.

(3) When the Dispute Mediation Committee conducts an investigation or inspection pursuant to Article 45 (2) of the Act, it may request disputing parties or persons designated by the disputing parties to be present

during the investigation or inspection or to present their opinions.

(4) To hear the opinions of disputing parties or relevant witnesses pursuant to Article 45 (5) of the Act, the Dispute Mediation Committee shall determine the date, time, and place of a meeting and notify the disputing parties or relevant witnesses thereof no later than 15 days before the meeting is held.

Article 51-4 (Notification of Intention to Reject Proposal of Mediation)

(1) When the Dispute Mediation Committee presents each party with a proposal of mediation pursuant to Article 47 (2) of the Act, it shall notify him or her of the fact that the proposal of mediation is deemed accepted unless he or she notifies the Dispute Mediation Committee of his or her acceptance or denial within 15 days from the date of being presented with the decision pursuant to paragraph 47 (3) of the Act.

(2) Where each party presented with a proposal of mediation pursuant to Article 47 (2) of the Act intends to reject the proposal of mediation, he or she shall notify the Dispute Mediation Committee of his or her intention by a person, registered mail, or electronic mail within 15 days from the date of being presented with the decision.

Article 52 (Incidents Eligible for Collective Dispute Mediation)

"Incident is prescribed by Presidential Decree" in Article 49 (1) of the Act means any incident that satisfies all of the following conditions:

1. The number of data subjects suffering from damage or infringement on their rights shall be not less than 50 persons, except the following:

   (a) Data subjects who have agreement with the personal information controller on the dispute settlement or compensation for damage;

   (b) Data subjects whose dispute is based on the same cause and is dealt with by a dispute mediation body established by other statutes or regulations;

   (c) Data subjects who have filed a lawsuit with a court regarding damages from the relevant personal information breach;

2. Major issues of the incident are common factually or legally.

Article 53 (Commencement of Collective Dispute Mediation Proceedings)

(1) "Period prescribed by Presidential Decree" in the latter part of Article 49 (2) of the Act means a period of at least 14 days.

(2) Public announcement of commencing the collective dispute mediation proceedings referred to in the latter part of Article 49 (2) of the Act shall be posted on the website of the Dispute Mediation Committee or a general daily newspaper circulating nationwide under the Act on the Promotion of Newspapers. *<Amended on Dec. 30, 2015>*

Article 54 (Applications for Participation in Collective Dispute Mediation Proceedings)

(1) A data subject or personal information controller, other than the parties to collective dispute mediation subject to Article 49 of the Act (hereinafter referred to as "collective dispute mediation"), who intends to participate in such collective dispute mediation additionally as a party pursuant to Article 49 (3) of the Act, shall file a written application during the notice period subject to the latter part of Article 49 (2) of the Act.

(2) Upon receiving a written application for collective dispute mediation as a party pursuant to paragraph (1), the Dispute Mediation Committee shall inform the applicant of whether it has accepted his or her application within 10 days from the expiry of the application period referred to in paragraph (1).

Article 55 (Collective Dispute Mediation Proceedings)

(1) After the collective dispute mediation proceedings commence, a data subject who falls under any of subparagraph 1 (a) through (c) of Article 52 shall be excluded from participation as a party.

(2) Once the collective dispute mediation proceedings of the case which satisfies the conditions referred to in Article 52 commence, such proceedings shall not be suspended even if the conditions referred to in subparagraph 1 of Article 52 are not satisfied because a data subject falls under any of subparagraph 1 (a) through (c) of that Article.

Article 56 (Allowances and Travel Expenses)

Members, etc. who attend a meeting of the Dispute Mediation Committee, the mediation panel, or a specialized committee for dispute mediation may be paid allowances and travel expenses within the budget: Provided, that this shall not apply where a public official attends any meeting in direct relation to his or her work. *<Amended on Sep. 12, 2023>*

Article 57 (Dispute Mediation Rule)

Except as provided in the Act and this Decree, matters necessary for the operation of the Dispute Mediation Committee and collective dispute mediation, such as the procedures for dispute mediation and dealing with dispute mediation, shall be determined by the chairperson of the Dispute Mediation Committee following its resolution. *<Amended on Sep. 12, 2023>*

CHAPTER VIII SUPPLEMENTARY PROVISIONS AND PENALTY PROVISIONS

Article 58 (Recommendation for Improvements and Disciplinary Action)

(1) An advice for improvement under Article 61 (2) and (3) of the Act and an advice for disciplinary action under Article 65 (2) and (3) of the Act shall be made in writing that explicitly state the matters to be advised, grounds therefor, outcomes of the action, reply period, etc.

(2) A person who has received an advice under paragraph (1) shall take necessary measures as advised, and notify the Protection Commission or the head of the related central administrative agency of the outcome in writing: Provided, That special circumstances, in which it is deemed impracticable to take measures as advised, shall be explained in the notice. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017: Aug. 4, 2020>*

Article 59 (Reporting on Infringements)

The Protection Commission shall designate the Korea Internet and Security Agency as a specialized institution to efficiently receive and handle the claim reports on infringements on personal information-related rights or interests pursuant to Article 62 (2) of the Act. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>*

Article 60 (Requests for Materials and Inspections)

(1) “Cases prescribed by Presidential Decree” in Article 63 (1) 3 of the Act means circumstances in which a case or incident which infringes on data subject’s right or interest related to personal information, such as a divulgence of personal information, has occurred or is likely to occur.

(2) The Protection Commission may request the head of the Korea Internet and Security Agency to provide necessary assistance, including technical advice, in order to request materials and to conduct inspections, etc. pursuant to Article 63 (1) and (2) of the Act. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Dec. 30, 2015; Jul. 26, 2017; Aug. 4, 2020>*

(3) Deleted. *<Sep. 12, 2023>*

(4) Deleted. *<Sep. 12, 2023>*

(5) Deleted. *<Sep. 12, 2023>*

(6) Deleted. *<Sep. 12, 2023>*

(7) Deleted. *<Sep. 12, 2023>*

Article 60-2 (Criteria for Calculation of Penalty Surcharges)

(1) The total sales under the main clause, with the exception of the subparagraphs, of Article 64-2 (1) of the Act shall be the average annual sales of the relevant personal information controller for three business years immediately preceding the business year in which any violation is committed (hereafter in this Article referred to as the "relevant business year"): Provided, That where three years have not elapsed since the date of commencement of business as of the first day of the relevant business year, the total sales shall be the amount calculated by converting the sales from the date of commencement of business to the end of the immediately preceding business year into the average annual sales; and where business commences in the relevant business year, the total sales shall be the amount calculated by converting the sales from the date of commencement of business to the date a violation is committed into the average annual sales.

(2) “Cases prescribed by Presidential Decree” in the proviso, with the exception of the subparagraphs, of Article 64-2 (1) of the Act means any of the following cases:

1. Where there is no sales records due to any of the following reasons:

(a) No commencement of business;

(b) Suspension of business;

(c) Any other reason equivalent to those specified in items (a) and (b), such as no engagement in profit-making business;

2. Where it is impracticable to objectively calculate the sales because sales calculation data are lost or damaged due to a disaster, etc.

(3) Sales unrelated to a violation under Article 64-2 (2) of the Act shall be any of the following amounts of the total sales specified in paragraph (1):

1. Sales of goods or services which are unrelated to personal information processing;

2. Sales recognized by the Protection Commission as not the sales of goods or services directly or indirectly affected by a violation, based on the data, etc. submitted pursuant to paragraph (4).

(4) Where the Protection Commission needs financial statements or other data for the calculation of sales, etc. under paragraphs (1) through (3), it may request the relevant personal information controller to submit the relevant data within a specified period not exceeding 20 days.

(5) "Ground prescribed by Presidential Decree" in Article 64-2 (5) 4 of the Act means where the relevant personal information controller rectifies a violation and meets the criteria determined and publicly notified by the Protection Commission.

(6) The criteria and procedures for calculating penalty surcharges under Article 64-2 (6) of the Act shall be as specified in attached Table 1-5.

Article 60-3 (Imposition and Payment of Penalty Surcharges)

(1) Where the Protection Commission intends to impose a penalty surcharge under Article 64-2 of the Act, it shall investigate and verify the relevant violation and shall give the person subject to the penalty surcharge written notification specifying the violation, the amount imposed, the methods and period of filing an objection, etc.

(2) A person notified under paragraph (1) shall pay the relevant penalty surcharge to a financial institution designated by the Protection Commission within 30 days from the date of being notified.

(3) Upon receipt of a penalty surcharge under paragraph (2), a financial institution shall issue a receipt to the person who has paid the penalty surcharge.

(4) Upon receipt of a penalty surcharge pursuant to paragraph (2), a financial institution shall notify the Protection Commission of such fact without delay.

Article 60-4 (Extensions of Payment Deadline for Penalty Surcharges and Payment by Installment)

(1) Where the Protection Commission extends the payment deadline for penalty surcharges specified in Article 64-2 (1) of the Act pursuant to Article 29 of the Framework Act on Administration and Article 7 of the Enforcement Decree of that Act, an extended payment period shall not exceed two years from the date of expiry of the initial payment deadline.

(2) Where the Protection Commission allows a penalty surcharge under Article 64-2 (1) of the Act to be paid in installments pursuant to Article 29 of the Framework Act on Administration and Article 7 of the Enforcement Decree of that Act, the interval between each deadline for payment in installments shall not exceed six months and the number of installments shall not exceed six times.

(3) Except as provided in paragraphs (1) and (2), matters necessary for an extension of the payment deadline for penalty surcharges, an application for payment in installments, etc. shall be determined and publicly notified by the Protection Commission.

Article 60-5 (Interest Rate on Additional Refund)

"Interest rate prescribed by Presidential Decree" in Article 64-2 (9) of the Act means the interest rate prescribed in the main clause of Article 43-3 (2) of the Enforcement Decree of the Framework Act on National Taxes.

Article 61 (Publication of Results)

(1) The Protection Commission may publish the following matters by posting them on its website, etc. under Article 66 (1) of the Act:

1. The details of violations;
2. The violators;
3. Recommendations for improvement, orders to take corrective measures, the imposition of penalty surcharges, accusations, and recommendations for disciplinary actions, and the details and outcomes of imposition of administrative fines.

(2) The Protection Commission may order a person subject to a recommendation for improvement, an order to take corrective measures, the imposition of a penalty surcharge, an accusation, a recommendation for a disciplinary action, the imposition of an administrative fine, etc. under Article 66 (2) of the Act (hereafter in this Article referred to as "disposition, etc.") to publish the following matters; in such cases, the Protection Commission shall, when issuing such order, determine the details, frequency, media of such publication, the size of pages, etc., and may consult with the person subject to the disposition, etc. on the text of the publication, etc.:

1. The details of violations;
2. The violators;
3. The fact that the person is subject to the disposition, etc.

(3) Where the Protection Commission intends to make the publication under paragraph (1) or to issue an order for publication under paragraph (2), it shall take into account the details, severity, period, and

frequency of a violation, the scope and consequences of the damage caused by such violation, and other relevant matters.

(4) The Protection Commission shall provide a person subject to a disposition, etc. with an opportunity to submit explanatory materials or to present his or her opinion before deliberating and resolving on publication or an order for publication.

Article 62 (Entrustment of Work)

(1) Deleted. *<Dec. 30, 2015>*

(2) The Protection Commission may entrust the work to support the provision of alternative sign-up tool subject to Article 24-2 (4) of the Act to the following institutions under Article 68 (1) of the Act: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Dec. 30, 2015; Jul. 26, 2017; Aug. 4, 2020; Jul. 19, 2022>*

1. The Korea Local Information Research and Development Institute established under Article 72 (1) of the Electronic Government Act;
2. The Korea Internet and Security Agency;
3. A corporation, institution, or organization prescribed by Notification of the Protection Commission after being recognized as having technical and financial capacity and facilities to develop, provide, and manage the alternative sign-up tool safely.

(3) The Protection Commission may entrust the following business affairs to an institution provided in paragraph (4), under Article 68 (1) of the Act: *<Amended on Mar. 23, 2013; Nov. 19, 2014; Dec. 30, 2015; Jul. 26, 2017; Aug. 4, 2020; Jul. 19, 2022; Sep. 12, 2023>*

1. Exchange and cooperation with international organizations and foreign personal information protection agencies for the protection of personal information under subparagraph 5 of Article 7-8 of the Act;
2. Surveys and research on statutes and regulations, policies, systems, actual conditions, etc. related to the protection of personal information under subparagraph 6 of Article 7-8 of the Act;
3. Support for and dissemination of technology development for the protection of personal information under subparagraph 7 of Article 7-8 of the Act;
4. Education and public relations regarding the protection of personal information under subparagraph 1 of Article 13 of the Act;
5. Promotion of and support for agencies and organizations related to the protection of personal information under subparagraph 2 of Article 13 of the Act;
6. Training of relevant specialists and development of criteria for privacy impact assessments under Article 33 (6) of the Act;
7. Receipt and processing of access requests under Article 35 (2) of the Act;
8. Requests for materials and inspections under Article 63 of the Act that are related to the following matters:

(a) Technical assistance for reporting under the former part of Article 34 (3) of the Act;

(b) Receipt and processing of, and counseling on, reports received by the Privacy Call Center pursuant to Article 62 of the Act;

9. Receipt of applications for designating an assessment institution under Article 36 (2) and receipt of reports under Article 37 (6).

(4) The institutions to which the Protection Commission may entrust its work regarding the matters specified in the subparagraphs of paragraph (3) shall be as follows: *<Newly Inserted on Jul. 19, 2022>*

1. The Korea Internet and Security Agency;

2. A corporation, institution, or organization determined and publicly notified by the Protection Commission as having expertise in the field of personal information protection.

(5) Where the Protection Commission entrusts its work pursuant to paragraphs (2) through (4), it shall publicly announce the institutions to be entrusted with the affairs and details of the entrusted affairs in the Official Gazette or on its website. *<Amended on Jul. 19, 2022>*

Article 62-2 (Processing of Sensitive Information and Personally Identifiable Information)

(1) The Protection Commission (including persons entrusted with the authority of the Protection Commission under Article 62 (3)) may process sensitive information and data that contain resident registration numbers, passport numbers, driver's license numbers, or alien registration numbers referred to in Article 19, if inevitable to perform the following business affairs: *<Amended on Aug. 4, 2020; Sep. 12, 2023>*

1. Business affairs regarding deliberation and resolution on any matter under Article 7-9 (1) 4 through 6 of the Act;

2. Business affairs regarding preparing for and supporting the establishment of systems providing alternative sign-up tools under Article 24-2 (4) of the Act;

3. Deleted; *<Sep. 12, 2023>*

4. Business affairs regarding work of the Privacy Call Center established pursuant to Article 62 (3) of the Act;

5. Business affairs regarding submission of materials and inspections under Articles 63 (1) and (2);

6. Business affairs regarding preliminary fact-finding inspections conducted under Article 63-2 of the Act;

7. Business affairs regarding imposing and collecting penalty surcharges under Article 64-2 of the Act.

(2) The Dispute Mediation Committee may process sensitive information and data that contain resident registration numbers, passport numbers, driver's license numbers, or alien registration numbers referred to in Article 19, if inevitable to perform the business affairs related to personal information dispute mediation under Articles 45, 47, and 49 of the Act. *<Amended on Aug. 4, 2020; Sep. 12, 2023>*

Article 62-3 (Re-Examination of Regulation)

(1) The Protection Commission shall examine the appropriateness of the following matters every three years, counting from each base date specified in the following (referring to the period that ends on the day before the base date of every third year), and shall take measures, such as making improvements: *<Newly Inserted on Aug. 4, 2020; Mar. 8, 2022; Sep. 12, 2023>*

1. Those eligible to be designated as assessment institutions, the requirements for revocation of designation, and the grounds for reporting changes under Article 36: January 1, 2022;

2. Scope of the persons required to be notified of the details of the use and provision of personal information, the types of information required to be notified, and the frequency and method of notification under Article 15-3: September 15, 2023;

3. Scope and standards of the parties required to purchase an insurance, etc. for performance of damage compensation responsibilities under Article 48-7: August 5, 2020.

(2) The Protection Commission shall examine the appropriateness of the following matters every two years, counting from each base date specified in the following (referring to the period that ends on the day before the base date of every second year), and shall take measures, such as making improvements: *<Amended on Dec. 30, 2015; Jul. 26, 2017; Aug. 4, 2020; Mar. 8, 2022>*

1. Combination of pseudonymized information processed by different personal information controllers under Article 29-3: January 1, 2022;

2. Details, and method of disclosure, of the Privacy Policy under Article 31: January 1, 2015;

2-2. Deleted; *<Mar. 8, 2022>*

3. Deleted; *<Dec. 24, 2018>*

4. Deleted; *<Dec. 24, 2018>*

5. Deleted. *<Dec. 24, 2018>*

(3) Deleted. *<Mar. 8, 2022>*

Article 63 (Criteria for Imposition of Administrative Fines)

The criteria for the imposition of administrative fines under Article 75 of the Act shall be as specified in attached Table 2. *<Amended on Aug. 4, 2020; Sep. 12, 2023>*

ADDENDA *<Presidential Decree No. 23169, Sep. 29, 2011>*

Article 1 (Enforcement Date)

This Decree shall enter into force on September 30, 2011: Provided, That Article 20 and subparagraph 2 (i) of attached Table 2 shall enter into force on March 30, 2012.

Article 2 (Repeal of other Acts)

The Enforcement Decree of the Act on the Protection of Personal Information Maintained by Public Institutions is hereby repealed.

Article 3 (Transitional Measures concerning Establishment of Master Plans and Implementation Plans)

(1) Notwithstanding Article 11, the Minister of Public Administration and Security shall establish the Master Plan for the period from 2012 to 2014 by December 31, 2011 subject to the deliberation and resolution of the Protection Commission.

(2) Notwithstanding Article 12, the head of a central administrative agency shall submit the implementation plan for the period from 2012 and 2013 according to the relevant Master Plan established under paragraph (1) and submit it to the Protection Commission by February 28, 2012 and establish it by April 30, 2012 subject to the deliberation and resolution of the Protection Commission.

Article 4 (Transitional Measures concerning Encryption of Personal Information Collected and Retained by Personal Information Controllers)

Personal information controllers who have collected and retained personal information as at the time this Decree enters into force shall complete the encryption of the personal information stored in electronic media (including the encryption of personally identifiable information to which Article 21 shall apply mutatis mutandis) pursuant to Article 30 (1) 3 by no later than December 31, 2012.

Article 5 (Transitional Measures concerning Registration of Personal Information Files)

The head of a public institution that operates personal information files as at the time this Decree enters into force (excluding institutions that have already registered personal information files before this Decree enters into force) shall apply for the registration thereof to the Minister of Public Administration and Security pursuant to Article 34 within 60 days from the date this Decree enters into force.

Article 6 (Transitional Measures concerning Privacy Impact Assessment)

The head of a public institution operating, or building up to operate, personal information files prescribed in the subparagraphs of Article 35 as at the time this Act enters into force shall conduct a privacy impact assessment of such personal information and submit the result thereof to the Minister of Public Administration and Security within five years from the date this Decree enters into force.

Article 7 Omitted.

Article 8 (Relationship with Other Statutes or Regulations)

A citation of the former Enforcement Decree of the Act on the Protection of Personal Information Maintained by Public Institutions or the provisions thereof in any other Act or subordinate statute as at the time this Decree enters into force shall be deemed a citation of this Decree or the provisions of this Decree in lieu of the former provisions, if corresponding provisions exist herein.

ADDENDA <*Presidential Decree No. 24425, Mar. 23, 2013*>

Article 1 (Enforcement Date)

This Decree shall enter into force on the date of its promulgation: Provided, That any amendment made by Presidential Decree promulgated before this Act enters into force, but the dates on which such

amendment enters into force has yet arrived among the Presidential Decrees amended pursuant to Article 6 of the Addenda shall respectively enter into force on the date such Presidential Decree enters into force.

Articles 2 through 6 Omitted.

ADDENDUM <*Presidential Decree No. 25531, Aug. 6, 2014*>

This Decree shall enter into force on August 7, 2014.

ADDENDA <*Presidential Decree No. 25751, Nov. 19, 2014*>

Article 1 (Enforcement Date)

This Decree shall enter into force on the date of its promulgation: Provided, That any amendment made by Presidential Decree promulgated before this Act enters into force, but the dates on which such amendment enters into force has yet arrived among the Presidential Decrees amended pursuant to Article 5 of the Addenda shall respectively enter into force on the date such Presidential Decree enters into force.

Articles 2 through 5 Omitted.

ADDENDA <*Presidential Decree No. 25840, Dec. 9, 2014*>

Article 1 (Enforcement Date)

This Decree shall enter into force on January 1, 2015.

Articles 2 through 16 Omitted.

ADDENDA <*Presidential Decree No. 26140, Mar. 11, 2015*>

Article 1 (Enforcement Date)

This Decree shall enter into force on the date of its promulgation.

Articles 2 and 3 Omitted.

ADDENDA <*Presidential Decree No. 26728, Dec. 22, 2015*>

Article 1 (Enforcement Date)

This Decree shall enter into force on December 23, 2015.

Articles 2 and 3 Omitted.

ADDENDUM <*Presidential Decree No. 26776, Dec. 30, 2015*>

This Decree shall enter into force on the date of its promulgation: Provided, That the amended provisions of Articles 21-2, 62 (2), 62-2 (1) 1, and attached Table 2 shall enter into force on January 1, 2016.

ADDENDA <*Presidential Decree No. 27370, Jul. 22, 2016*>

Article 1 (Enforcement Date)

This Decree shall enter into force on July 25, 2016.

Article 2 (Transitional Measures concerning Establishment of Master Plans and Implementation Plans)

(1) The Master Plan for 2015 to 2017 established pursuant to the former provisions of Article 11 shall be deemed the Master Plan established pursuant to the amended provisions of Article 11.

(2) The implementation plans for 2016 and 2017 established pursuant to the former provisions of Article 12 shall be deemed the implementation plans established pursuant to the amended provisions of Article 12, respectively.

ADDENDUM <*Presidential Decree No. 27522, Sep. 29, 2016*>

This Decree shall enter into force on September 30, 2016.

ADDENDA <*Presidential Decree No. 28074, May 29, 2017*>

Article 1 (Enforcement Date)

This Decree shall enter into force on May 30, 2017.

Articles 2 through 4 Omitted.

ADDENDA <*Presidential Decree No. 28150, Jun. 27, 2017*>

Article 1 (Enforcement Date)

This Decree shall enter into force on July 1, 2017: Provided, That the amended provisions of Article 3 of this Addenda shall enter into force on the date of its promulgation.

Articles 2 and 3 Omitted.

ADDENDA <*Presidential Decree No. 28211, Jul. 26, 2017*>

Article 1 (Enforcement Date)

This Decree shall enter into force on the date of its promulgation: Provided, That any amendment of the Presidential Decrees made pursuant to Article 8 of this Addenda, which were promulgated before this Decree comes into force, but the enforcement date of which has yet to arrive, shall enter into force on the date the corresponding Presidential Decree takes effect.

Articles 2 through 8 Omitted.

ADDENDA <*Presidential Decree No. 28355, Oct. 17, 2017*>

Article 1 (Enforcement Date)

This Decree shall enter into force on October 19, 2017.

Article 2 (Applicability to Reporting on Data Breach Notification)

The amended provisions of Articles 39 (1) and 40 (3) shall begin to apply from the first divulgence of any personal information after this Decree enters into force.

Article 3 (Transitional Measures concerning Request for Access, etc. to Personal Information)

Notwithstanding the amended provisions of Articles 41 (1), 43 (1), and 44 (1), a person who has requested access to, correction or erasure, or suspension of processing of, his/her personal information before this Decree enters into force shall be governed by the former provisions.

ADDENDUM <*Presidential Decree No. 29421, Dec. 24, 2018*>

This Decree shall enter into force on January 1, 2019.

ADDENDUM <*Presidential Decree No. 30509, Mar. 3, 2020*>

This Decree shall enter into force on the date of its promulgation.

ADDENDUM <*Presidential Decree No. 30833, Jul. 14, 2020*>

This Decree shall enter into force on July 15, 2020.

ADDENDA <*Presidential Decree No. 30892, Aug. 4, 2020. >*

Article 1 (Date of Enforcement)

This Decree shall enter into force on August 5, 2020: Provided, That the amended provisions of Article 5-3 shall enter into force six months after the date of its promulgation.

Article 2 (General Transitional Measures)

Before this Decree enters into force, designation, measures, notifications, reports, and other acts performed by Information and Communications service providers, etc. pursuant to theEnforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. shall be deemed to have been performed in accordance with the provisions of this Decree.

Article 3 (Transitional Measures on Processing Sensitive Information)

Personal information that has been lawfully processed pursuant to this Decree or other statutes or regulations before this Decree enters into force and falls under the amended provisions of subparagraphs 3 and 4 of Article 18 shall be deemed to have been processed in accordance with this Decree or other statutes and regulations.

Article 4 (Transitional Measures on Calculating Penalty Surcharge)

Administrative dispositions received pursuant to the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. for violations prior to the enforcement of this Decree shall be included in the calculation of the number of violations stipulated in the amended provisions of attached Table 1-5.

Article 5 (Transitional Measures on Imposing Penalty Surcharge)

Penalty surcharges imposed pursuant to the Act on Promotion of Information and Communication Network Utilization and Information Protection, Etc. or the previous provisions for violations prior to the enforcement of this Decree shall be included in the calculation of the number of violations stipulated in the amended provisions of attached Table 2.

Article 6 Omitted

Article 7 (Relationship to Other Statutes or Regulations)

Upon the enforcement of this Decree, if other statutes and regulations in relation to the protection of personal information refer to the Enforcement Decree of the Act on Promotion of Information and Communication Network Utilization and Information Protection, Etc. or its provisions, and if there are concerning regulations, it shall be deemed that this Decree or the relevant regulations of this Decree was referred in place of the previous regulations.

ADDENDA <*Presidential Decree No. 31429, Feb. 2, 2021*>

Article 1 (Enforcement Date)

This Decree shall enter into force on February 5, 2021.

Articles 2 and 3 Omitted.

ADDENDUM <*Presidential Decree No. 32528, Mar. 8, 2022*>

This Decree shall enter into force on the date of its promulgation.

ADDENDA <*Presidential Decree No. 32813, Jul. 19, 2022*>

Article 1 (Enforcement Date)

This Decree shall enter into force three months after the date of its promulgation: Provided, That the amended provisions of Articles 16 (1) and 62 shall enter into force on the date of the promulgation.

Article 2 (Applicability to Standards for Calculation of Penalty Surcharge)

The amended provisions of attached Tables 1, 1-3 and 1-5 shall also apply to violations committed before this Decree enters into force.

ADDENDA <*Presidential Decree No. 33723, Sep. 12, 2023*>

Article 1 (Enforcement Date)

This Decree shall enter into force on September 15, 2023: Provided, That the following amended provisions shall enter into force on the date prescribed in the relevant subparagraph:

1. The amended provisions of Articles 17 (1) and 30-2: September 15, 2024;
2. The amended provisions of the latter part of Article 15-2 (1): January 1, 2024;
3. The amended provisions of subparagraph 2 (a), (ac), (ah), (ai), and (al) of attached Table 2: March 15, 2024.

Article 2 (Transitional Measures concerning Imposition of Administrative Fines)

Notwithstanding the amended provisions of attached Table 2, the previous provisions shall apply to violations under subparagraph 2 (a), (b), (h), and (al) of the previous attached Table 2 committed before this Decree enters into force.

Article 3 Omitted.

Last updated : 2023-10-25