ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT

[Enforcement Date 05. Aug, 2020.] [Presidential Decree No.30892, 04. Aug, 2020., Partial Amendment]

개인정보보호위원회 (개인정보보호정책과), 02-2100-3043

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose) The purpose of this Decree is to prescribe matters delegated 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 by Presidential Decree No. 30833, 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 Agency for High Ranking Public Officers under Article 3 (1) of the Act on Corruption Investigation Agency for High Ranking Public Officers;
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) "Devices prescribed by Presidential Decree" in subparagraph 7 of Article 2 of the Act means any of the following:

1. A closed-circuit television means any of the following devices:
   (a) A device that shoots videos, etc. through a permanently installed camera at a certain place, or transmits such videos, etc. to the specified place via transmission channel of wired or wireless closed circuits, etc.;
   (b) A device that can videotape or record the visual information filed or transmitted under item (a);
2. A network camera means a device with which its installer or operator may collect, store, or process visual information, filmed through a permanently installed device at a certain place, via the wired or wireless Internet at any place.

CHAPTER II PERSONAL INFORMATION PROTECTION COMMISSION

Article 4 Deleted. <by Presidential Decree No. 30892, Aug. 4, 2020>

Article 4-2 (Prohibition on For-profit Work) 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 conduct any of the following works in accordance with Article 7-6 (1) of the Act for the purpose of making profits:

1. Works related to the matters to be deliberated and resolved by the Protection Commission in accordance with Article 7-9 (1) of the Act;
2. Works 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").

[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 5 (Expert Committees) (1) The Protection Commission may establish an expert committee by sector (hereinafter referred to as "expert committee") to review in advance the matters for deliberation and resolution subject to Article 7-9 (1) of the Act in a professional manner. <Amended by Presidential Decree No. 30892, Aug. 4, 2020>

(2) The expert committee established under paragraph (1) shall be comprised of not more than 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 by Presidential Decree No. 27370, Jul. 22, 2016; Presidential Decree No. 30892, Aug. 4, 2020>

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) Deleted. <by Presidential Decree No. 30892, Aug. 4, 2020>

Article 5-2 (Personal Information Protection Policy Council) (1) For the consistent implementation of personal information protection policies, and to facilitate consultation among the related 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 toincidents of infringement with respect to personal information;
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 the 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. [This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 5-3 (City/ <italic>Do </italic> 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.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

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, or employee who works for the public institution, where it deems necessary to do its work.

Article 8 Deleted. <by Presidential Decree No. 30892, 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 works. <Amended by Presidential Decree No. 30892, 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 by Presidential Decree No. 30892, 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 by Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

Article 9-3 (Procedures for Assessment of Factors of Infringement) (1) The head of a central administrative agency who intends to request an assessment of factors of infringement with respect to personal information pursuant to Article 8-2 (1) of the Act (hereinafter referred to as "assessment of factors of infringement") shall submit to the Protection Commission a written request (or an electronic request form) for an assessment of factors of infringement 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 factors of infringement with respect to personal information regarding 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 factors of infringement 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 factors of infringement.

(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 factors of infringement from the head of the related central administrative agency.

(5) The Protection Commission may establish guidelines necessary to assess factors of infringement, including detailed criteria for, and methods of the assessment of factors of infringement; 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 factors of infringement.

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

Article 10 Deleted. <by Presidential Decree No. 30892, 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 by no later than June 30 of the year preceding the start of the third-year plan. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, Jul. 22, 2016; Presidential Decree No. 30892, 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 this case, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, 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 by no later than June 30 each year, and notify the heads of the related central administrative agencies of such guidelines. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, Jul. 22, 2016; Presidential Decree No. 30892, 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 by no later than September 30 each year. <Amended by Presidential Decree No. 30892, Aug. 4, 2020>

(3) The Protection Commission shall deliberate and resolve on the implementation plans submitted pursuant to paragraph (2) by no later than December 31 of that year. <Amended by Presidential Decree No. 30892, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, Jul. 22, 2016>

1. Matters concerning the management of personal information and personal information files processed by the personal information controller and the installation and operation of 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, delection, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, 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 this case, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>CHAPTER IV PROCESSING OF PERSONAL INFORMATION

CHAPTER IV-II SPECIAL PROVISIONS ON 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. As prescribed and publicly notified 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. As prescribed and publicly notified 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. As prescribed and publicly notified by the Protection Commission, the agency shall have financial capabilities; and
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 and publicly notified by 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 cancelled:

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 an incident of infringement with respect to personal information, 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 cancelled 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 and publicly notified by the Protection Commission.

[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 29-3 (Combination 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 determined and publicly notified prescribed by the Protection Commission's notification, 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 determined by 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 and publicly notified by 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 security 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 safety 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 the Protection Commission's notification. .[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

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 determined and publicly notified by 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 determined and publicly notified by the Protection Commission.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 29-5 (Measures to Ensure Safety of Pseudonymized Information)(1) A personal information controller shall implement the following security measures for pseudonymized information and additional information to restore pseudonymized information to the original state (hereinafter referred to as "additional information" in this Article) in accordance with Article 28-4 (1) of the Act:

1. Security measures under Article 30 or Article 48-2 of the Act;
2. Separate storage of pseudonymized information and additional information: Provided, That any unnecessary additional information shall be destroyed; and
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 justifiable reasons such as the personal information controller being a micro enterprise under Article 2 of the Act on the Protection of and Support for 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 (2) of the Act mean any of the following:

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. Other matters publicly notified by the Protection Commission as deemed necessary for the management of the processing of pseudonymized information.

[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 29-6 (Standards on Imposition of Penalty Surcharges with Respect to Processing of Pseudonymized Information)(1) The sales under Article 28-6 (1) of the Act shall refer to the relevant personal information controller's annual average sales revenue over the previous three business years: Provided, That if three years have not passed since the 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 revenue from the commencement of business until the end of the immediately preceding business year into the annual average sales revenue, and if the personal information controller has commenced business during the business year in which the violation occurrs, the total sales shall be the amount calculated by converting the sales revenue from the commencement date of business until the date of violation into annual sales revenue.

(2) "Where prescribed by Presidential Decree" under the proviso of Article 28-6 (1) of the Act shall refer to any of the following cases:

1. The personal information controller has no sales because it fails to commence, or suspended, etc. its business;

2. It is difficult to objectively calculate the sales revenue because the sales materials are lost or damaged due to a disaster, etc.

(3) If the Protection Commission is in need of financial statements or other materials to calculate the sales revenue under paragraph (1), the Protection Commission may request the personal information controller to submit the relevant materials within a certain period not exceeding 20 days.

(4) The standards and procedures for calculating the penalty surcharges under Article 28-6 (1) of the Act shall be specified in attached Table 1.

[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

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:

1. To formulate and implement an internal management plan for the safe processing of personal information;
2. To control access to personal information and restrict the authority to access personal information;
3. To adopt encryption technology to safely store and transmit personal information and other equivalent measures;
4. To retain login records to respond to incidents of infringement with respect to personal information and to take measures to prevent the forgery and falsification thereof;
5. To install and upgrade security programs to protect personal information;
6. To take physical measures, such as a storage or locking system, to keep personal information safely.

(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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4. 2020>

(3) Detailed standards for the measures to ensure safety under paragraph (1) shall be prescribed and publicly notified by the Protection Commission. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

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 by Presidential Decree No. 27522, Sep. 29, 2016; Presidential Decree No. 30892, Aug. 4, 2020>

1. Particulars of personal information to be processed;
2. Deleted; <by Presidential Decree No. 30892, Aug. 4, 2020>
3. Matters concerning measures to ensure the safety of personal information subject to Article 30 or Article 48-2.

(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:

1. Posting at easily noticeable location of the personal information controller's workplace, etc.;
2. Publishing in the Official Gazette (only in case 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, Etc. 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 and services executed between the personal information controller and the data subjects and providing a copy of the same to the data subject

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 by Presidential Decree No. 27370, 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 therero;
   (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 under Article 2 of the Act on the Protection of and Support for 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 by Presidential Decree No. 30892, Aug. 4, 2020>

(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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

Article 33 (Registered Items of Personal Information Files) "Matters prescribed by Presidential Decree" in Article 32 (1) 7 of the Act means the following:

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.

Article 34 (Registration, and Disclosure of Personal Information Files) (1) The head of a public institution that operates personal information files shall apply for registration of the matters provided for in Article 32 (1) of the Act and Article 33 of this Decree (hereinafter referred to as "registered matters") to the Protection Commission within 60 days from the date it starts operating the personal information files, as prescribed by Notification the Protection Commission. The same shall also apply to any modification of registered matters. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

(2) The Protection Commission shall post the status of personal information files registered pursuant to Article 32 (4) of the Act on the Protection Commission's website. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

(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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, 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 for in Article 30 (1) and Article 48-2 (1). <Amended by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

(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 considerable 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 determined and publicly notified by the Protection Commission. <Amended by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

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 determine and publicly notify 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 by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

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 by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

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 by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

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 by Presidential Decree No. 27522, Sep. 29, 2016; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

1. The Korea Internet and Security Agency;
2. A corporation or an organization or institution designated and publicly notified by 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 and publicly notified by the Protection Commission. <Amended by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

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 determined and publicly notified by 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 by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

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 improper 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 thepurpose for work without just 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 determined and publicly notified by the Protection Commission. <Amended by Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

[This Article Newly Inserted by Presidential Decree No. 27370, Jul. 22, 2016]

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 by Presidential Decree No. 27522, 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 (Consideration at the time of Privacy Impact Assessment) "Matters prescribed by Presidential Decree" in Article 33 (2) 4 of the Act means the following:

1. Whether sensitive information or personally identifiable information will be processed;
2. The retention period of personal information.

Article 37 (Designation of PIA 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 "PIA institution") pursuant to the latter part of Article 33 (1) of the Act: <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 26728, Dec. 22, 2015; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

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; hereafter 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 protection industry, as defined in subparagraph 2 of Article 2 of the Act on the Promotion of the Information Security Industry; or

(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 specified in attached Table 1-2;

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 a PIA institution shall file an application for designation as a PIA institution, in the form prescribed by Notification the Protection Commission, with the Protection Commission, along with the following documents (including electronic documents; hereinafter the same shall apply): <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 28355, Oct. 17, 2017; Presidential Decree No. 30892, 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 tthe Protection Commission.

(3) Upon receipt of an application for designation as a PIA 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, 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 a PIA institution pursuant to paragraph (1), the Protection Commission shall, without delay, issue a written designation to the relevant applicant, and publish the following matters in the Official Gazette. The same shall also apply to any revision to the published matters: <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

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

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

(5) The Protection Commission may revoke the designation of a PIA institution subject to paragraph (1) in any of the following cases: Provided, That the Protection Commission shall revoke the designation in cases falling under subparagraph 1 or 2: <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

1. Where the PIA institution is designated by fraud or other improper means;
2. Where the PIA institution wants revocation of such designation or has closed its business;
3. Where the PIA institution fails to satisfy the requirements for designation provided for in paragraph (1);
4. Where the PIA institution fails to submit a report subject to paragraph (6);
5. Where the PIA institution unconscientiously conducts the privacy impact assessment either by intention or gross negligence, and is deemed incapable of duly conducting the privacy impact assessment;
6. Where the PIA institution breaches any of the duties provided for in the Act or this Decree.

(6) A PIA 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 28355, Oct. 17, 2017; Presidential Decree No. 30892, 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 PIA institution, or similar event occurs.

(7) Where intending to revoke the designation of a PIA institution pursuant to paragraph (5), the Protection Commission shall hold a hearing. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

Article 38 (Criteria for Privacy Impact Assessment) (1) Criteria for privacy impact assessments referred to in Article 33 (6) of the Act are as follows: <Amended by Presidential Decree No. 27370, Jul. 22, 2016>

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 infringement with respect to personal information;
2. The level of measures to ensure safety taken under Articles 24 (3), 25 (6), and 29 of the Act, and the possibility of subsequent infringement with respect to personal information;
3. Countermeasures against risk factors of infringement with respect to personal information, if any;
4. Other necessary measures subject to the Act or this Decree, or any factor affecting breach of duties.

(2) A PIA institution in receipt of a request for a privacy impact assessment pursuant to Article 33 (1) of the Act shall analyze and assess the risk factors of infringement with respect to personal information arising out of the operation of personal information files according to the criteria for privacy impact assessments prescribed in paragraph (1); prepare a privacy impact assessment report containing the following matters; and submit the report to the head of the relevant public

institution. The head of such public institution shall submit the report (including measures for improvement referred to in subparagraph 3, if any matter requiring improvement in such report) to the Protection Commission prior to building, operating, or changing personal information files provided for in Article 35: <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 27370, Jul. 22, 2016; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

1. Summary of the project related to, and the purpose of, the operation of personal information files;
2. General description of personal information files subject to the privacy impact assessment;
3. Analysis and assessment of risk factors of infringement with respect to personal information according to the criteria for privacy impact assessments, and matters requiring improvement;
4. Human resources and costs required to conduct the privacy impact assessment.

(3) Except as provided in the Act and this Decree, the Protection Commission may establish and publicly notify detailed standards for designating PIA institutions, procedures for privacy impact assessments, etc. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

Article 39 (Scope of Data Breach Notification and Where to Report) (1) "Personal information above the scale prescribed by Presidential Decree" in the former part of Article 34 (3) of the Act means personal information of at least one thousand data subjects. <Amended by Presidential Decree No. 28355, Oct. 17, 2017>

(2) "Specialized institution prescribed by Presidential Decree" in the former part and the latter part of Article 34 (3) of the Act means the Korea Internet and Security Agency. <Amended by Presidential Decree No. 26776, Dec. 30, 2015; Presidential Decree No. 27370, Jul. 22, 2016>

Article 40 (Method and Procedure for Data Breach Notification of Divulgence of Personal Information) (1) A personal information controller who becomes aware that personal information has been divulged shall, without delay, notify the aggrieved data subject of the matters prescribed in Article 34 (1) of the Act, in writing, etc.: Provided, That the personal information controller may give notice to the data subjects, right after it has taken contingent measures, including shut-down of the access route, check-up of weak points and deletion of divulged personal information, necessary to prevent the dissemination of divulged personal information and additional divulgence.

(2) Notwithstanding paragraph (1), where a personal information controller has become aware of personal information divulgence pursuant to the main clause of paragraph (1) or has taken contingent measures after awareness of the infringement with respect to personal information pursuant to the proviso of paragraph (1), but cannot confirm details of personal information divulgence provided for in Article 34 (1) 1 or 2 of the Act, the personal information controller may first notify the aggrieved data subject of the fact of personal information divulgence and the information divulged, in writing, etc.; and then notify the details confirmed additionally.

(3) Notwithstanding paragraphs (1) and (2), where personal information of at least one thousand data subjects has been divulged pursuant to Article 34 (3) of the Act and Article 39 (1) of this Decree, the relevant personal information controller shall notify the aggrieved data subjects of such divulgence in writing, etc. and post the matters provided for in Article 34 (1) of the Act on his or her website for at least seven days so that the data subjects may easily recognize them: Provided, that if a personal information controller has no website, the personal information

controller shall provide notice of the divulgence of personal information in writing, etc. and post the matters provided for in Article 34 (1) of the Act at easily noticeable places of his or her workplace, etc. for at least seven days. <Amended by Presidential Decree No. 28355, Oct. 17, 2017>

Article 40-2 (Criteria for Imposition of Penalty Surcharges)(1) Penalty surcharges provided for in Article 34-2 (1) of the Act shall be imposed in accordance with attached Table 1-3. <Amended by Presidential Decree No. 30892, Aug. 4, 2020>

(2) To impose a penalty surcharge pursuant to Article 34-2 (1) of the Act, the Protection Commission shall give a written notice stating the violation, amount of the penalty surcharge, and methods of, and period for filing an objection, to the violator. <Amended by Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

(3) A person in receipt of the written notice given under paragraph (2) shall pay a penalty surcharge to a collecting agency designated by the Protection Commission within 30 days from the receipt of such written notice: Provided, That, where the person cannot pay the penalty surcharge within such period due to a natural disaster or other unavoidable causes, he or she shall pay it within seven days from the date the relevant cause ceases to exist. <Amended by Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

(4) "Late-payment penalty prescribed by Presidential Decree" in the former part of Article 34-2 (3) of the Act means an amount calculated for the period from the day following the due date for payment until the day preceding the payment date of the penalty surcharge by adding the amount equivalent to 5/1,000 of the unpaid penalty surcharge for each month past due.

[This Article Newly Inserted by Presidential Decree No. 25531, Aug. 6, 2014]

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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 28355, 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 by Presidential Decree No. 28355, 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 just 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 determined and publicly notified by the Protection Commission. In such cases, the Protection Commission shall forward the Personal Information Access Request to the relevant public institution without delay. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 28355, Oct. 17, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

(4) “Period prescribed by Presidential Decree” in the former part of Article 35 (3) of the Act means 10 days.

(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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 28355, Oct. 17, 2017; Presidential Decree No. 30892, 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 ten days from the receipt of the access request. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, 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 erase 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 by Presidential Decree No. 28355, Oct. 17, 2017>

(2) Upon receipt of a request to correct or erase 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 erase the personal information, and take necessary measures based on the result of such processing. <Amended by Presidential Decree No. 28355, 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 erase 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 Deletion 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 28355, Oct. 17, 2017; Presidential Decree No. 30892, 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 by Presidential Decree No. 28355, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 28355, Oct. 17, 2017; Presidential Decree No. 30892, 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 by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

Article 46 (Confirmation of Data Subjects or Representatives)(1) Upon receipt of request for access under Article 41 (1), correction or erasure of personal information under Article 43 (1), suspension of processing of personal information under Article 44 (1) or withdrawal of consent under Article 39-7 (1) of the Act (hereafter referred to as "Access Request, etc." in this Article, and Articles 47 and 48), a personal information controller shall confirm whether the person who has submitted the Access Request, etc. is the principal or the duly authorized representative. <Amended by Presidential Decree No. 30892, Aug. 4, 2020>

(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 Access Request, 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 Access Request, etc. lies with the personal information controller.

(3) Any fee and postage provided for 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 referred to as "national agency" in this Article) or a local government, may claim such fee and postage by the electronic payment means, as defined in subparagraph 11 of Article 2 of the Electronic Financial Transactions Act, or telecommunications billing services, as defined in subparagraph 10 of Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.:

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 Access Request, 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 Access Request, etc. for personal information they possess and notify the results thereof. <Amended by Presidential Decree No. 24425, Mar. 23, 2013; Presidential Decree No. 25751, Nov. 19, 2014; Presidential Decree No. 28211, Jul. 26, 2017; Presidential Decree No. 30892, Aug. 4, 2020>

CHAPTER VI-II SPECIAL PROVISIONS ON PROCESSING OF PERSONAL INFORMATION BY INFORMATION AND COMMUNICATIONS SERVICE PROVIDERS

Article 48-2 (Special Provisions on Measures to Ensure Safety of Personal Information)

(1) Any information and communications service provider (as set forth in Article 2 (1) 3 of the Act on Promotion of Information and Telecommunications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) and any third party who receives personal information of users (as set forth in Article 2 (1) 4 of the same Act; hereinafter the same shall apply) from the information and communications service provider in accordance with Article 17 (1) 1 of the Act (hereinafter collectively referred to as "Information and Communications Service Providers, etc.") shall implement the following measures to ensure safety when processing users' personal information in accordance with Article 29 of the Act, notwithstanding Article 30:

1. Establishment and implementation of an internal management plan which includes each of the following for safe processing of personal information:
   (a). Matters concerning the structure and operation of the personal information protection organization, including the designation of a privacy officer;
   (b). Matters concerning training of the persons who process users' personal information under the direction and supervision of Information and Communications Service Providers, etc. (hereinafter referred to as "personal information handlers" in this Article);
   (c). Detailed matters required for implementing measures under subparagraphs 2 through 6.
2. Each of the following measures for preventing illegal access to personal information:
   (a). Establishment and implementation of standards on granting, changing, cancelling, etc. the access to the database system which was systematically configured to process personal information (hereinafter referred to as the "Personal Information Processing System" in this Article);
   (b). Establishment and operation of an intrusion prevention system and intrusion detection system for the Personal Information Processing System;
   (c). Blocking of external Internet access to the computers, etc. of personal information handlers connected to the Personal Information Processing System [only applicable to the Information and Communications Service Providers, etc. (as set forth in Article 2 (1) 2 of the Act on Promotion of Information and Telecommunications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) who stores and manages personal information of one million users or more on average per day during the three-month period immediately preceding the end of the previous year, or who generates sales revenue of 10 billion won or more in the information and communications service sector during the previous year (previous business year for a corporation)];
   (d). Establishment and implementation of the standards on the methods of creating passwords, password change interval, etc.; and
   (e). Other measures necessary to control access to personal information.
3. Each of the following measures to prevent falsification and alteration of access records:

(a). Storage, confirmation and monitoring of the dates on which the Personal Information Processing System was accessed, details of personal information processed, etc. if a personal information handler processes personal information by accessing the Personal Information Processing System; and

(b). Back-up storage of records on access to the Personal Information Processing System in a separate storage device.

4. Each of the following measures to ensure safe storage and transmission of personal information:

(a). Storage of passwords in one-way encrypted format;

(b). Encrypted storage of resident registration numbers, account information, information under subparagraph 3 of Article 18 and other information determined and publicly notified by the Protection Commission;

(c). Establishment of secure server, etc. if user's personal and authentication information is transmitted or received via telecommunications network;

(d). Other security measures using encryption technology.

5. Installation, periodic update and inspection of vaccine software to detect and cure at all times any malicious program, including computer virus and spyware, which may intrude the Personal Information Processing System and other information appliance used by any personal information handler to process personal information;

6. Other measures necessary to ensure the safety of personal information.

(2) The Protection Commission may provide necessary assistance, such as building a system with which Information and Communications Service Providers, etc can take the measures to ensure safety pursuant to paragraph (1).

(3) Detailed standards for the measures to ensure safety under paragraph (1) shall be determined and publicly notified by the Protection Commission.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-3 (Method of Confirming Legal Representative's Consent)(1) In accordance with Article 39-3 (4) of the Act, an information and communications service provider shall confirm whether the legal representative has provided his or her consent through any of the following means:

1. Having the legal representative indicate whether he or she consents on the website that specifies the consent items, and informing the legal representative via mobile text message that the information and communications service provider confirmed the indication of consent;
2. Having the legal representative indicate whether he or she consents on the website that specifies the consent items, and receiving credit, debit, etc. card information of the legal representative's;
3. Having the legal representative indicate whether he or she consents on the website that specifies the consent items, and verifying the identity of the legal representative via the identity verification process on the legal representative's mobile phone, etc.;
4. Issuing or delivering the document that specifies the consent items to the legal representative directly or via mail or fax, and having the legal representative submit the document after signing and affixing seal on the document with respect to the consent items;
5. Sending an electronic email that specifies the consent items and having the legal representative send an e-mail with an indication of consent;

6. Informing the legal representative of the consent items and receiving the legal representative's consent via phone call, or providing the legal representative with the means (e.g., web address) to confirm the consent items and obtaining the legal representative's consent via a phone call;
7. Other method of informing the legal representative of the consent items and confirming the legal representative's indication of consent in a comparable manner to subparagraphs 1 through 6.

(2) If it is difficult for anI Information and Communications Service Provider, etc. to indicate all the consent items due to the particular nature of the medium by which the personal information is collected, the information and communications service provider may provide the legal representative with the means to confirm the consent items (e.g., web address, telephone number of the workplace, etc.).[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-4 (Special Provisions on Notification and Report of Divulgence of Personal Information)(1) The "specialized institution prescribed by Presidential Decree" in the main clause of Article 39-4 (1), with the exception of its subpargraphs, and Article 39-4 (2) of the Act means the Korea Internet and Security Agency.

(2) If an Information and Communications Service Provider, etc. becomes aware of any loss, theft or divulgence of personal information, the Information and Communications Service Provider, etc. shall inform the users of all information listed under Article 39-4 (1) of the Act in writing, etc. without delay, and report the loss, theft or divulgence to the Protection Commission or Korea Internet and Security Agency.

(3) If an Information and Communications Service Provider, etc. has yet to ascertain the specifics of the information under Article 39-4 (1) 1 or 2 of the Act when filing the notification/report under paragraph (2), the Information and Communications Service Provider, etc. shall first notify/report the details ascertained up to date and the information under subparagraphs3 through 5 of the same paragraph, and later notify and report any other information as soon as such information is confirmed.

(4) If an Information and Communications Service Provider, etc. has a justifiable reason under the proviso of Article 39-4 (1), with the exception of its subpargraphs, of the Act, the Information and Communications Service Provider, etc. may publish matters prescribed in each subparagraph under Article 39-4 (1) of the Act on its website for at least 30 days in lieu of the notification under paragraph (2).

(5) If it is difficult to publish on the website in accordance with paragraph (4) due to a force majeure event or another unavoidable cause, public announcement of the required information on two or more general daily nationwide newspapers under the Act on the Promotion of Newspapers, Etc. on at least one occasion may be provided in lieu of the online disclosure under paragraph (4).

(6) An Information and Communications Service Provider, etc. shall explain the justifiable reason under the main clause or proviso of under Article 39-4 (1),with the exception of its subpargraphs, of the Act to the Protection Commission without delay in writing.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-5 (Special Provisions on Destruction of Personal Information)(1) If any user of an information and communications service does not use the service for the period under Article 39-6 (1) of the Act, the Information and Communications Service Provider, etc. shall immediately destroy the user's personal information, or store and manage such information separately from other users' personal information after expiration of the period: Provided, That if retaining the user's

personal information is required by other statutes or regulations even after the expiration of the period under the main clause of Article 39-6 (1) of the Act (or any other period determined at the request of the user in accordance with the proviso of Article 39-6 (1) of the Act), the personal information of such user shall be stored and managed separately from other users' personal information until the preservation period required by other statutes or regulation expires.

(2) When storing and managing personal information in a segregated manner in accordance with paragraph (1), the Information and Communications Service Provider, etc. shall not use or provide the personal information, except asotherwise provided in the Act or other statutes or regulations.

(3) The "matters prescribed by Presidential Decree such as the fact that their personal information will be destroyed, the expiration date, and the particulars of personal information to be destroyed" in Article 39-6 (2) of the Act means to the following:

1. If personal information will be destroyed: The fact that personal information will be destroyed, expiration date of the retention period and items of personal information to be destroyed;
2. If personal information is stored and managed separately from other users' personal information: The fact that the storage and management of personal information is segregated, expiration date of the retention period and items of personal information that are separately stored and managed.

(4) The "method prescribed by Presidential Decree such as e-mail" in Article 39-6 (2) of the Act means written notice, etc.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-6 (Notification of Details of Personal Information Usage)(1) The "information and communications service provider, etc. meeting standards prescribed by President Decree" in the main clause of Article 39-8 (1) of the Act means any of the following providers:

1. Any Information and Communications Service Provider, etc. who generated sales revenue of 10 billion won or more in the information and communications service sector during the previous year (previous business year for a corporation);
2. Any Information and Communications Service Provider, etc. who stored and managed personal information of one million users or more on average per day during the three-month period immediately preceding the end of the previous year.

(2) The types of information which shall be notified to users in accordance with Article 39-8 (1) of the Act shall be as follows:

1. Purpose of collecting and using personal information, and items of personal information collected;
2. The recipient of personal information, the purpose for which the personal information was provided and items of provided personal information: Provided, That this shall not apply to the information provided in accordance with Articles 13, 13-2 and 13-4 of the Protection of Communications Secrets Act and Article 83 (3) of the Telecommunications Business Act.

(3) The notification under Article 39-8 (1) of the Act shall be made on at least one occasion per year in writing, etc.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-7 (Scope, and Standards of the Parties Required to Purchase an Insurance for Performance of Damage Compensation Responsibilities)(1) The Information and Communications Service Providers, etc. which meet all of the following requirements (hereafter in this Article referred to as the "Subject Personal Information Controllers") shall purchase insurance, join a mutual aid organization or accumulate reserves in accordance with Article 39-9 (1) of the Act:

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 (minimum reserve amount in case of accumulating reserves; the same applies hereafter in this Article) applicable to the Subject Personal Information Controllers in case 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 should be equal to or exceed the minimum insurance subscription amount set forth in attached Table 1-4.

(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.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-8 (Institution Receiving Request for Deletion and Blocking of Exposed Personal Information)The "specialized institution designated by Presidential Decree" in Article 39-10 (2) of the Act means the Korea Internet and Security Agency.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-9 (Scope of Persons Required to Designate Local Representative)(1) The "information and communications service provider, etc. meeting the criteria prescribed by Presidential Decree" in the main clause of Article 39-11 (1), with the exception of its subpargraphs, of the Act means any of the following providers:

1. Any provider whose sales revenue for the previous year (previous business year for a corporation) is one trillion won or more;
2. Any provider who generates sales revenue of 10 billion won or more in the information and communications service sector during the previous year (previous business year for a corporation);
3. Any provider who stores and manages personal information of one million users or more on average per day during the three-month period immediately preceding the end of the previous year;
4. Any provider who violates the Act and was requested to submit relevant materials, including articles and documents, in accordance with Article 63 (1) of the Act for having caused, or having the potential to cause a case or incident of infringement with respect to personal information.

(2) The sales revenue under paragraph (1) 1 and2 shall be based on the amount converted into Korean won at the average exchange rate of the previous year (previous business year for a corporation).[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-10 (Safeguards in the Event of Overseas Transfer of Personal Information)(1) If any Information and Communications Service Provider, etc. intends to transfer personal information overseas in accordance with the main clause under Article 39-12 (2) of the Act, it shall implement the following safeguards according to paragraph (4) of the same Article:

1. Measures to ensure safety for protection of personal information in accordance with Article 48-2 (1);
2. Matters concerning handling of complaints and dispute resolution concerning infringement with respect to personal information;
3. Other measures necessary to protect users' personal information.

(2) If any Information and Communications Service Provider, etc. intends to transfer personal information overseas in accordance with the main clause under Article 39-12 (2) of the Act, the Information and Communications Service Provider, etc. shall discuss each subparagraph of paragraph (1) with the recipient in advance and incorporate the same into the terms of the agreement.

(3) The "method prescribed by Presidential Decree such as e-mail" in the proviso of Article 39-12 (2) of the Act means written notice, etc.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-11 (Special Provisions on the Calculation Standards of Penalty Surcharges)

(1) The revenue pursuant to Article 39-15 (1) of the Act shall be the annual average sales revenue generated by the relevant Information and Communications Service Provider, etc. from the information and communications service related to the violation over the previous three business years: Provided, That if three years have not passed since the 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 revenue from the commencement of business until the end of the immediately preceding business year into the annual average sales revenue, and if the Information and Communications Service Provider, etc. commenced business during the business year in which the violation occurred, the total sales shall be the amount calculated by converting the sales revenue from the commencement date of business until the date of violation into annual sales revenue.

(2) "As prescribed by Presidential Decree" in the proviso of Article 39-15 (2) of the Act means any of the following cases:

1. The personal information controller has no sales because it did not commence, or suspended, etc. its business;
2. It is difficult to objectively calculate the sales revenue because the sales materials were lost or damaged due to a disaster, etc.

(3) If the Protection Commission is in need of financial statements or other materials to calculate the sales revenue under paragraph (1), the Protection Commission may request the Information and Communications Service Provider, etc. to submit the relevant materials within a period of no more than 20 days.

(4) The standards and procedures for calculating the penalty surcharges under Article 39-15 (4) of the Act shall be as specified in attached Table 1-5.

[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-12 (Imposition and Payment of Penalty Surcharges)(1) If the Protection Commission intends to impose a penalty surcharge in accordance with Article 39-15 of the Act, the

Protection Commission shall investigate and verify the violation, and then provide the imposed party with written notice specifying the violation, imposed amount, appealing procedures, deadline for filing an appeal, etc.

(2) The violator who received the notice under paragraph (1) shall pay the penalty surcharge to a financial institution designated by the Protection Commission within 30 days from the date of receiving the notice: Provided, that if the violator is unable to pay the penalty surcharge within the deadline due to a force majeure event or other unavoidable cause, the violator shall pay the surcharge within seven days from the date on which such cause no longer exists.

(3) The financial institution which received the penalty surcharge in accordance with paragraph (2) shall issue a receipt to the payer of penalty surcharge.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

Article 48-13 (Interest Rate of Surcharge Refund)The "interest rate prescribed by Presidential Decree" in Article 39-15 (7) of the Act means the interest rate in the main clause of Article 43-3 (2) of the Enforcement Decree of the Framework Act on National Taxes.[This Article Newly Inserted by Presidential Decree No. 30892, Aug. 4, 2020]

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

Article 1 (Enforcement Date)

⊡ 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)

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

Article 1 (Enforcement Date)

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

Article 1 (Enforcement Date)

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

Article 1 (Enforcement Date)

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

This Decree shall enter into force on the date of its promulgation: <italic>Provided</italic>, 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)

⊡ 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)

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

Article 1 (Enforcement Date)

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

Article 1 (Enforcement Date)

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

Article 1 (Enforcement Date)

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.