PERSONAL INFORMATION PROTECTION ACT

Act No. 10465, Mar. 29, 2011
Amended by Act No. 11690, Mar. 23, 2013
Act No. 11990, Aug. 6, 2013
Act No. 12504, Mar. 24, 2014
Act No. 12844, Nov. 19, 2014
Act No. 13423, Jul. 24, 2015
Act No. 14107, Mar. 29, 2016
Act No. 14765, Apr. 18, 2017
Act No. 14839, Jul. 26, 2017
Act No. 16930, Feb. 4, 2020

Article 1 (Purpose)

The purpose of this Act is to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information. *<Amended by Act No. 12504, Mar. 24, 2014>*

Article 2 (Definitions)

The terms used in this Act shall be defined as follows: *<Amended by Act No. 12504, Mar. 24, 2014; Act No. 16930, Feb. 4, 2020>*

1. The term "personal information" means any of the following information relating to a living individual:

(a) Information that identifies a particular individual by his or her full name, resident registration number, image, etc.;

(b) Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured;

(c) Information under items (a) or (b) above that is pseudonymized in accordance with subparagraph 1-2 below and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (hereinafter referred to as “pseudonymized information”);

1-2. The term “pseudonymization” means a procedure to process personal information so that the information cannot identify a particular individual without additional information, by deleting in part, or replacing in whole or in part, such information;

2. The term “processing” means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of personal information and other similar activities;

3. The term “data subject” means an individual who is identifiable through the information processed and is the subject of that information;

4. The term “personal information file” means a set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy search of the personal information;

5. The term “personal information controller” means a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities;

6. The term "public institution" means any of the following institutions:

(a) The administrative bodies of the National Assembly, the Courts, the Constitutional Court, and the National Election Commission; the central administrative agencies (including agencies under the Presidential Office and the Prime Minister’s Office) and their affiliated entities; and local governments;

(b) Other national agencies and public entities prescribed by Presidential Decree;

7. The term "visual data processing devices" means the devices prescribed by Presidential Decree, which are continuously installed at a certain place to take pictures of persons or images of things, or transmit such pictures or images via wired or wireless networks.

8. The term “scientific research” means research that applies scientific methods, such as technological development and demonstration, fundamental research, applied research and privately funded research.

Article 3 (Principles for Protecting Personal Information)

(1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.

(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.

(3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed.

(4) The personal information controller shall manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the possibility of infringement on the data subject’s rights and the severity of the relevant risks.

(5) The personal information controller shall make public its privacy policy and other matters related to personal information processing; and shall guarantee the data subject's rights, such as the right to access their personal information.

(6) The personal information controller shall process personal information in a manner to minimize the possibility of infringing the privacy of a data subject.

(7) If it is still possible to fulfil the purposes of collecting personal information by processing anonymized or pseudonymised personal information, the personal information controller shall endeavor to process personal information through anonymization, where anonymization is possible, or through pseudonymisation, if it is impossible to fulfil the purposes of collecting personal information through anonymization. *<Amended by Act No. 16930, 4. February, 2020 >*

(8) The personal information controller shall endeavor to obtain trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act and other related statutes.

Article 4 (Rights of Data Subjects)

A data subject has the following rights in relation to the processing of his or her own personal information:

1. The right to be informed of the processing of such personal information;
2. The right to determine whether or not to consent and the scope of consent regarding the processing of such personal information;
3. The right to confirm whether or not personal information is being processed and to request access (including the provision of copies; hereinafter the same applies) to such personal information;
4. The right to suspend the processing of, and to request correction, deletion, and destruction of such personal information;
5. The right to appropriate redress for any damage arising out of the processing of such personal information through a prompt and fair procedure.

Article 5 (Obligations of State, etc.)

(1) The State and a local government shall formulate policies to prevent harmful consequences of beyond-purpose collection, abuse and misuse of personal information, indiscrete surveillance and tracking, etc. and to enhance the dignity of human beings and individual privacy.

(2) The State and a local government shall establish policy measures, such as improving statutes, necessary to protect the data subject's rights as provided for in Article 4.

(3) The State and local government shall respect, promote, and support self-regulating data protection activities of personal information controllers to improve unreasonable social practices relating to the processing of personal information.

(4) The State and a local government shall enact or amend any statutes or municipal ordinances in conformity with the purpose of this Act.

Article 6 (Relationship to other Acts)

The protection of personal information shall be governed by this Act, except where special provisions exist in other laws. *<Amended by Act No. 12504, Mar. 24, 2014>*

Article 7 (Personal Information Protection Commission)

(1) The Personal Information Protection Commission (hereinafter referred to as the "Protection Commission") shall be established under the Prime Minister to independently conduct work relating to the protection of personal information. *<Amended by Act No. 16930, 4. February, 2020 >*

(2) The Protection Commission shall be deemed a central administrative agency under Article 2 of the Government Organization Act: Provided, That Article 18 of the Government Organization Act shall not apply to any of the following matters: *<Amended by Act No. 16930, 4. February, 2020 >*

1. Affairs specified in subparagraphs 3 and 4 of Article 7-8 (1);
2. Matters falling under subparagraph 1 among those to be deliberated and resolved on under Article 7-9 (1).

(2) through (9) Deleted. *<by Act No. 16930, Feb. 4, 2020>*

Article 7-2 (Composition of the Protection Commission)

(1) The Protection Commission shall be comprised of nine Commissioners including two Standing Commissioners (one Chairperson and one Vice Chairperson).

(2) Commissioners of the Protection Commission shall be selected from among any of the following persons with sufficient experience and expertise in the protection of personal information, with the Chairperson and Vice Chairperson being proposed by the Prime Minister, two other Commissioners being proposed by Chairperson, two other Commissioners being recommended by the negotiation body of the political party to which the President belongs or belonged, and three other persons being recommended by another negotiation body and named or appointed by the President:

1. A person who serves, or served, as a public official of Grade III or higher (including public officials belonging to the Senior Executive Service) who is responsible for personal information protection;
2. A person who has been serving, or served, as a judge, prosecutor or lawyer for ten years or longer;
3. A person who served as an officer at a public institution or group (including groups comprised of personal information controllers) for three years or longer or a person recommended by the above public institution or group who was in charge of personal information protection for three years or longer;
4. A person who has expertise in a field relating to personal information and has been serving, or served, as an associate professor or higher at a school set forth in subparagraph 1 of Article2 of the Higher Education Act for five years or longer.

(3) The Chairperson and the Vice Chairperson shall be appointed from among public officials in political service.

(4) The Chairperson, Vice Chairperson and the head of the secretariat under Article 7-13 shall become cabinet member, notwithstanding Article 10 of the Government Organization Act.

Article 7-3 (Chairperson)

(1) The Chairperson shall represent the Protection Commission, preside over meetings of the Protection Commission, and oversee the related work.

(2) If the Chairperson cannot perform his/her duties for inevitable reasons, the Vice Chairperson shall act on his or her behalf, and if both the Chairperson and Vice Chairperson cannot perform his/her duties for inevitable reasons, another Commissioner, determined by the Protection Commission in advance, shall act on behalf of Chairperson.

(3) The Chairperson may attend the National Assembly and make statements in relation to the work of the Protection Commission, and if required by the National Assembly, he or she shall attend the National Assembly to make a report or respond to questions.

(4) The Chairperson may attend a meeting of the State Council and recommend the Prime Minister to submit a bill concerning the affairs under his/her jurisdiction.

Article 7-4 (Term of Office of Commissioners)

(1) A Commissioner shall serve for a term of three years but may be consecutively appointed one time.

(2) When the post of a Commissioner becomes vacant, a new Commissioner shall be named or appointed without delay. In such cases, the term of the named or appointed succeeding Commissioner shall be newly commenced.

Article 7-5 (Status Guarantee for Commissioners)

(1) No Commissioner shall be dismissed or de-commissioned against his or her will except in the following cases:

1. Where he or she is unable to perform his/her duties for a long period due to mental or physical disorder;
2. Where he or she falls under any ground for disqualification provided for in Article 7-7;
3. Where he or she violates his/her official duties under this Act or any other Act.

(2) Each Commissioner shall independently perform his or her duties in compliance with the law and his/her conscience.

Article 7-6 (Prohibition on Dual Office Holding)

(1) Each Commissioner shall neither concurrently engage in any of the following posts, nor engage in any affairs for profits related to his or her duties:

1. Member of the National Assembly or Local Council;
2. State or local public official;
3. Other positions prescribed by Presidential Decree.

(2) Matters relating to for-profit businesses set forth in paragraph (1) shall be prescribed by Presidential Decree.

(3) A Commissioner shall not engage in political activities.

Article 7-7 (Grounds for Disqualification)

(1) Persons falling under any of the following cannot be a Commissioner:

1. Non-Korean national;
2. A person falling under any of the subparagraphs under Article 33 of the State Public Officials Act;

3. A Member of political party set forth in Article 22 of the Political Parties Act.

(2) A Commissioner falling under any of the above subparagraphs 1 through 3 shall be automatically discharged from his or her position: Provided, That, in the case of subparagraph 2 of Article 33 of the State Public Officials Act, this only applies to a person who was declared bankrupt and did not apply for immunity within the application deadline, or received a confirmed decision of immunity disapproval or cancellation, according to the Debtor Rehabilitation and Bankruptcy Act; in the case of subparagraph 5 of Article 33 of the Same Act, this only applies to Articles 129 through 132 of the Criminal Act, Article 2 of the Act on Special Cases Concerning the Punishment, Etc. of Sexual Crimes, subparagraph 2 of Article 2 of the Act on the Protection of Children and Youth against Sex Offenses and a person who committed a crime prescribed in Articles 355 or 356 of the Criminal Act with regard to his or her duties and received a suspended sentence of imprisonment without labor or a heavier punishment.

Article 7-8 (Affairs under Jurisdiction of the Protection Commission)

The Protection Commission shall perform the following affairs:

1. Matters concerning the improvement of law relating to personal information protection;
2. Matters concerning the establishment or execution of policies, systems or plans relating to personal information protection;
3. Matters concerning investigation into infringement upon the right of data subjects and the ensuing dispositions;
4. Handling of complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information;
5. Exchange and cooperation with international organizations and foreign personal information protection agencies to protect personal information;
6. Matters concerning the investigation and study, education and promotion of law, policies, systems and status relating to personal information protection;
7. Matters concerning the support of technological development and dissemination relating to personal information protection and nurturing of experts;
8. Matters provided for in this Act and other statutes as affairs under the jurisdiction of the Protection Commission.

Article 7-9 (Matters to be Deliberated and Resolved on by the Protection Commission)

(1) The Protection Commission shall deliberate and resolve on the following matters:

1. Matters concerning the assessment of data breach incident factors under Article 8-2;
2. Establishment of the Master Plan referred to in Article 9 and the Implementation Plan referred to in Article 10;
3. Matters concerning the improvement of policies, systems, and law relating to personal information protection;
4. Matters concerning the coordination of positions taken by public institutions with respect to the processing of personal information;

5. Matters concerning the interpretation and operation of law related to the protection of personal information;

6. Matters concerning the use and provision of personal information under Article 18 (2) 5;

7. Matters concerning the results of the privacy impact assessment under Article 33 (3);

8. Matters concerning the imposition of penalty surcharges under Articles 28-6, 34-2 and 39-15;

9. Matters concerning the presentation of opinions and recommendation for improvement under Article 61;

10. Matters concerning corrective measures under Article 64;

11. Matters concerning indictment and recommendation for disciplinary actions under Article 65;

12. Matters concerning the publication of processing results under Article 66;

13. Matters concerning the imposition of administrative fines under Article 75;

14. Matters concerning the enactment, amendment and abolition of law under its jurisdiction and rules of the Protection Commission;

15. Matters referred to a meeting by Chairperson or at least two Commissioners of the Protection Commission with respect to the protection of personal information;

16. Other matters which the Protection Commission deliberates or resolves pursuant to this Act or other statutes.

(2) The Protection Commission may take the following measures if necessary to deliberate and resolve matters provided for in paragraph (1):

1. Listening to the opinions of relevant public officials, experts in personal information protection, civic organizations and relevant business operators;

2. Requesting submission of relevant materials or facts with respect to relevant agencies.

(3) Relevant agencies in receipt of a request made under paragraph (2) 2 shall comply with the request unless there are extraordinary circumstances.

(4) Upon deliberating and resolving on matters provided for in paragraph (1) 3, the Protection Commission may advise on the improvement of such matters to the relevant agency.

(5) The Protection Commission may inspect whether the details of its advice given under paragraph (4) has been implemented or not.

Article 7-10 (Meetings)

(1) Meetings of the Protection Commission shall be convened by the Chairperson when he or she deems it necessary or at the request of not less than 1/4 of all incumbent Commissioners.

(2) The Chairperson or at least two Commissioners of the Protection Commission may propose a bill to the Protection Commission.

(3) The quorum for holding meetings of the Protection Commission shall be the presence of a majority of its members enrolled, and any resolution shall require the affirmative votes of a majority of the members present.

Article 7-11 (Disqualification of, Challenge to, and Refrainment by, Commissioners)

(1) A Commissioner of the Protection Commission shall be excluded from participating in deliberation and resolution for a case if:

1. The Commissioner or his or her current or former spouse is a party to the relevant case or is a joint right holder or a joint obligator with respect to the case;
2. The Commissioner is or was a relative of a party to the case;
3. The Commissioner has given any testimony, expert opinion, or legal advice with respect to the case;
4. The Commissioner is or was involved in the case as an agent or representative of a party to the case;
5. The Commissioner or a public institution, corporation or group where he or she belongs shares interests with a person who provides advice or other support for the case.

(2) When any party finds it impracticable to expect fair deliberation and resolution from a Commissioner, he or she may file an application for recusal, and the Protection Commission shall make a decision by resolution.

(3) A Commissioner may refrain from the case on the grounds provided for in paragraphs (1) or (3).

Article 7-12 (Subcommission)

(1) The Protection Commission may have sub-commissions which will deliberate and resolve minor personal information infringement cases or similar or repetitive matters to ensure more efficient work procedures.

(2) Each sub-commission shall be comprised of three members.

(3) Matters deliberated and resolved by the sub-commission pursuant to paragraph (1) shall be deemed deliberated and resolved by the Protection Commission.

(4) Resolution for a meeting of the sub-commission shall be made by the presence of all the members enrolled and affirmative votes of all members present.

Article 7-13 (Secretariat)

The Protection Commission shall have a secretariat to handle its work, and matters that are not specified in this Act in relation to the organization of the Protection Commission shall be prescribed by Presidential Decree.

Article 7-14 (Operation)

Matters that are not specified in this Act and other statutes in relation to the operation of the Protection Commission shall be prescribed by the rules of the Protection Commission.

Article 8 Deleted. *<by Act No. 16930, Feb. 4, 2020>*

Article 8-2 (Assessment of Data Breach Incident Factors)

(1) The head of a central administrative agency shall request the Protection Commission to assess the factors of data breach incident where a policy or system that entails personal information processing is adopted or changed by the enactment or amendment of any statute under his or her jurisdiction.

(2) Upon receipt of a request made pursuant to paragraph (1), the Protection Commission may advise the head of the relevant agency of the matters necessary to improve the relevant statute by analyzing and

reviewing the data breach incident factors of such statute.

(3) Necessary matters concerning the procedure and method to assess the data breach incident factors under paragraph (1) shall be prescribed by Presidential Decree.

Article 9 (Master Plan)

(1) The Protection Commission shall establish a Master Plan to protect personal information (hereinafter referred to as a "Master Plan") every three years in consultation with the heads of related central administrative agencies to ensure the protection of personal information and the rights and interests of data subjects. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015>*

(2) The Master Plan shall include the following:

1. Basic goals and intended directions of the protection of personal information;
2. Improvement of systems and statutes related to the protection of personal information;
3. Measure to prevent personal information breaches;
4. Vitalization of self-regulation to protect personal information;
5. Promoting education and public relations to protect personal information;
6. Training of specialists in the protection of personal information;
7. Other matters necessary to protect personal information.

(3) The National Assembly, the Court, the Constitutional Court, and the National Election Commission may establish and implement its own Master Plan to protect personal information of relevant institutions, (including affiliated entities).

Article 10 (Implementation Plan)

(1) The head of a central administrative agency shall establish an implementation plan to protect personal information each year in accordance with the Master Plan and submit it to the Protection Commission, and shall execute the implementation plan subject to the deliberation and resolution of the Protection Commission.

(2) Matters necessary for the establishment and execution of the implementation plan shall be prescribed by Presidential Decree.

Article 11 (Request for Materials, etc.)

(1) To efficiently establish the Master Plan, the Protection Commission may request materials or opinions regarding the status of regulatory compliance, personal information management, etc. by personal information controllers from personal information controllers, the heads of relevant central administrative agencies, the heads of local governments and related organizations or associations, etc. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015>*

(2) The Protection Commission may conduct an investigation with respect to data controllers, the competent head of the central administrative departments or agencies and local governments, and the competent agencies and organizations about the level and actual status of how personal data is managed where necessary to implement policies for personal data protection and to evaluate performance, etc. *<Newly Inserted by Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No. 16930, 4. February, 2020 >*

(3) The head of a central administrative agency may request the materials referred to in paragraph (1) from personal information controllers in the fields under his or her jurisdiction to efficiently establish and promote Implementation Plans. *<Amended by Act No. 13423, Jul. 24, 2015>*

(4) Any person in receipt of a request to furnish the materials under paragraphs (1) through (3) shall comply with the request unless there are extraordinary circumstances. *<Amended by Act No. 13423, Jul. 24, 2015>*

(5) The scope and method to furnish the materials under paragraphs (1) through (3) and other necessary matters shall be prescribed by Presidential Decree. *<Amended by Act No. 13423, Jul. 24, 2015>*

Article 12 (Personal Information Protection Guidelines)

(1) The Protection Commission may establish the Standard Personal Information Protection Guidelines (hereinafter referred to as the "Standard Guidelines") regarding the personal information processing standard, types of personal information breaches, preventive measures, etc., and recommend that personal information controllers comply with such Guidelines. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(2) The head of a central administrative agency may establish the personal information protection guidelines regarding the personal information processing in the fields under his or her jurisdiction in accordance with the Standard Guidelines; and may recommend that personal information controllers comply with such guidelines.

(3) The National Assembly, the Court, the Constitutional Court, and the National Election Commission may establish and implement its own personal information protection guidelines for each relevant institution (including affiliated entities).

Article 13 (Promotion and Support of Self-Regulation)

The Protection Commission shall establish policies necessary for the following matters to promote and support self-regulating activities of personal information controllers to protect personal information: *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

1. Education and public relations concerning the protection of personal information;
2. Promotion and support of agencies and organizations related to the protection of personal information;
3. Introduction and facilitation of privacy mark;
4. Support for personal information controllers in the establishment and implementation of self-regulatory rules;
5. Other matters necessary to support the self-regulating data protection activities of personal information controllers.

Article 14 (International Cooperation)

(1) The Government shall establish policy measures necessary to enhance the personal information protection standard in the international environment.

(2) The Government shall establish relevant policy measures so that the rights of data subjects may not be infringed on owing to the cross-border transfer of personal information.

Article 15 (Collection and Use of Personal Information)

(1) A personal information controller may collect personal information in any of the following circumstances, and use it with the scope of the purpose of collection:

1. Where consent is obtained from a data subject;
2. Where special provisions exist in other laws or it is inevitable to observe legal obligations;
3. Where it is inevitable for a public institution's performance of its duties under its jurisdiction as prescribed by statutes, etc.;
4. Where it is inevitably necessary to execute and perform a contract with a data subject;
5. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses, etc.;
6. Where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope.

(2) A personal information controller shall inform a data subject of the following matters when it obtains consent under paragraph (1) 1. The same shall apply when any of the following is modified.

1. The purpose of the collection and use of personal information;
2. Particulars of personal information to be collected;
3. The period for retaining and using personal information;
4. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(3) A personal information controller may use personal information without the consent of a data subject within the scope reasonably related to the initial purpose of the collection as prescribed by Presidential Decree, in consideration whether disadvantages have been caused to the data subject and whether necessary measures have been taken to secure such as encryption, etc. < *This Article Newly Inserted by Act No. 16930, 4. February, 2020* >

Article 16 (Limitation to Collection of Personal Information)

(1) A personal information controller shall collect the minimum personal information necessary to attain the purpose when collecting personal information pursuant to Article 15 (1). In such cases, the burden of proof that the minimum personal information is collected shall be borne by the personal information controller.

(2) A personal information controller shall collect personal information by specifically informing a data subject of the fact that he or she may deny the consent to the collection of other personal information than

the minimum information necessary in case of collecting the personal information through the consent of the data subject. *<Newly Inserted by Act No. 11990, Aug. 6, 2013>*

(3) A personal information controller shall not deny the provision of goods or services to a data subject on ground that the data subject does not consent to the collection of personal information exceeding minimum requirement. *<Amended by Act No. 11990, Aug. 6, 2013>*

Article 17 (Provision of Personal Information)

(1) A personal information controller may provide (or share; hereinafter the same shall apply) the personal information of a data subject to a third party in any of the following circumstances: *<Amended by Act No 16930, February. 4, 2020>*

1. Where the consent is obtained from the data subject;
2. Where the personal information is provided within the scope of purposes for which it is collected pursuant to Articles 15 (1) 2, 3 and 5 and 39-3 (2) 2 and 3.

(2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified:

1. The recipient of personal information;
2. The purpose for which the recipient of personal information uses such information;
3. Particulars of personal information to be provided;
4. The period during which the recipient retains and uses personal information;
5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(3) A personal information controller shall inform a data subject of the matters provided for in paragraph (2), and obtain the consent from the data subject in order to provide personal information to a third party overseas; and shall not enter into a contract for the cross-border transfer of personal information in violation of this Act.

(4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether necessary measures to secure safety, such as encryption, have been taken, etc. . *<Newly Inserted by Act No. 16930, 4. February, 2020 >*

Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information)

(1) A personal information controller shall not use personal information beyond the scope provided for in Articles 15 (1) and 39-3 (1) and (2), or provide it to any third party beyond the scope provided for in Article 17 (1) and (3). *<Amended by Act No. 16930, Feb. 4, 2020>*

(2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may use personal information or provide it to a third party for other purposes, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That information and communications service providers (as set forth in Article 2 (1) 3 of the Act on Promotion

of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) processing the personal information of users (as set forth in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) are only subject to subparagraphs 1 and 2, and subparagraphs 5 through 9 are applicable only to public institutions: *<Amended by Act No. 16930, Feb. 4, 2020>*

1. Where additional consent is obtained from the data subject;
2. Where special provisions exist in other laws;
3. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses;
4. Deleted; *<by Act No. 16930, Feb. 4, 2020>*
5. Where it is impossible to perform the duties under its jurisdiction as provided for in any Act, unless the personal information controller uses personal information for other purpose than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution by the Commission;
6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention;
7. Where it is necessary for the investigation of a crime, indictment and prosecution;
8. Where it is necessary for a court to proceed with trial-related duties;
9. Where it is necessary for the enforcement of punishment, probation and custody.

(3) A personal information controller shall inform the data subject of the following matters when it obtains the consent under paragraph (2) 1. The same shall apply when any of the following is modified.

1. The recipient of personal information;
2. The purpose of use of personal information (in the case of provision of personal information, it means the purpose of use by the recipient);
3. Particulars of personal information to be used or provided;
4. The period for retaining and using personal information (where personal information is provided, it means the period for retention and use by the recipient);
5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(4) Where a public institution uses personal information, or provides it to a third party for other purpose than the intended one collected under paragraph (2) 2 through 6, 8, and 9, the public institution shall post the legal grounds for such use or provision, purpose and scope, and other necessary matters on the Official Gazette or its website requirements for such use or provision including the legal basis, purpose, scope, etc. as prescribed by Notification of the Protection Commission. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(5) Where a personal information controller provides personal information to a third party for other purpose than the intended one in any case provided for in paragraph (2), the personal information controller shall request the recipient of the personal information to limit the purpose and method of use and other necessary matters, or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person in receipt of such request shall take necessary measures to ensure the safety of the personal information.

Article 19 (Limitation to Use and Provision of Personal Information on Part of Its Recipients)

A person who receives personal information from a personal information controller shall not use the personal information, or provide it to a third party, for any purpose other than the intended one, except in the following circumstances:

1. Where additional consent is obtained from the data subject;
2. Where special provisions exist in other laws.

Article 20 (Notification on Sources, etc. of Personal Information Collected from Third Parties)

(1) When a personal information controller processes personal information collected from third parties, the personal information controller shall immediately notify the data subject of the following matters at the request of such data subject:

1. The source of collected personal information;
2. The purpose of processing personal information;
3. The fact that the data subject is entitled to demand suspension of processing of personal information, as prescribed in Article 37.

(2) Notwithstanding paragraph (1), when a personal information controller satisfying the criteria prescribed by Presidential Decree taking into account the types and amount of processed personal information, number of employees, amount of sales, etc., collects personal information from third parties and processes the same pursuant to Article 17 (1) 1, the personal information controller shall notify the data subject of the matters referred to in paragraph (1): Provided, That this shall not apply where the information collected by the personal information controller does not contain any personal information, such as contact information, through which notification can be given to the data subject. *<Newly Inserted by Act No. 14107, Mar. 29, 2016; Act No 16930, February. 4, 2020>*

(3) Necessary matters in relation to the time, method, and procedure of giving notification to the data subject pursuant to the main sentence of paragraph (2), shall be prescribed by Presidential Decree. *<Newly Inserted by Act No. 14107, Mar. 29, 2016>*

(4) Paragraph (1) and the main clause of paragraph (2) shall not apply to any of the following circumstances: Provided, That this shall be the case only where it is manifestly superior to the rights of data subjects under this Act: *<Amended by Act No. 14107, Mar. 29, 2016>*

1. Where personal information, which is subject to a notification request, is included in the personal information files referred to in any of the subparagraphs of Article 32 (2);

2. Where such notification is likely to cause harm to the life or body of any other person, or unfairly damages the property and other interests of any other person.

Article 21 (Destruction of Personal Information)

(1) A personal information controller shall destroy personal information without delay when the personal information becomes unnecessary owing to the expiry of the retention period, attainment of the purpose of processing the personal information, etc.: Provided, That this shall not apply where the retention of such personal information is mandatory by other statutes.

(2) When a personal information controller destroys personal information pursuant to paragraph (1), necessary measures to prevent recovery and revival shall be taken.

(3) Where a personal information controller is obliged to retain, rather than destroy, personal information pursuant to the proviso to paragraph (1), the relevant personal information or personal information files shall be stored and managed separately from other personal information.

(4) Other necessary matters, such as the methods to destroy personal information and its destruction process, shall be prescribed by Presidential Decree.

Article 22 (Methods of Obtaining Consent)

(1) Where a personal information controller intends to obtain the consent of the data subject (including his or her legal representative as stated in paragraph (6): hereafter in this Article the same applies) to the processing of his or her personal information, the personal information controller shall present the request for consent to the data subject in a clearly recognizable manner where each matter requiring consent is distinctly presented, and obtain his or her consent thereto, respectively. *<Amended by Act No. 14765, Apr. 18, 2017>*

(2) Where a personal information controller obtains the consent under paragraph (1) in writing (including electronic documents under Article 2, subparagraph 1 of the Framework Act on Electronic Documents and Transactions), the personal information controller shall clearly specify important matters prescribed by Presidential Decree such as the purpose of collection and use of personal information and the items of personal information to be collected and used, in the manner prescribed by Notification of the Protection Commission, so as to make such matters easy to be understood. *<Newly Inserted by Act No. 14765, Apr. 18, 2017; Act No. 14839, Jul. 26, 2017; Act No. 16930, 4. February, 2020 >*

(3) Where a personal information controller obtains the consent of a data subject to the processing of his or her personal information pursuant to Articles 15 (1) 1, 17 (1) 1, 23 (1) 1, and 24 (1) 1, the personal information controller shall distinguish personal information that may be processed without the data subject's consent for the purpose of executing a contract with the data subject, etc., from personal information that may be processed only with the data subject's consent. In such cases, the burden of proof that no consent is required in processing the personal information shall be borne by the personal information controller. *<Amended by Act No. 14107, Mar. 29, 2016; Act No. 14765, Apr. 18, 2017>*

(4) Where a personal information controller intends to obtain the consent of the data subject to the processing of his or her personal information in order to promote goods or services or solicit purchase

thereof, the personal information controller shall notify the data subject of the fact in a clearly recognizable manner, and obtain his/her consent thereto. *<Amended by Act No. 14765, Apr. 18, 2017>*

(5) A personal information controller shall not deny the provision of goods or services to a data subject on ground that the data subject would not consent to the matter eligible for selective consent pursuant to paragraph (3), or would not consent pursuant to paragraph (4) and Article 18 (2) 1. *<Amended by Act No. 14765, Apr. 18, 2017>*

(6) When it is required to obtain consent pursuant to this Act to process personal information of a child under 14 years of age, a personal information controller shall obtain the consent of his/her legal representative. In such cases, minimum personal information necessary to obtain the consent of the legal representative may be collected directly from such child without the consent of his/her legal representative. *<Amended by Act No. 14765, Apr. 18, 2017>*

(7) Except as otherwise expressly provided for in paragraphs (1) through (6), other matters necessary in relation to detailed methods to obtain the consent of data subjects and the minimum information referred to in paragraph (6) shall be prescribed by Presidential Decree, in consideration of the collection media of personal information. *<Amended by Act No. 14765, Apr. 18, 2017>*

Article 23 (Limitation to Processing of Sensitive Information)

(1) A personal information controller shall not process any information prescribed by Presidential Decree (hereinafter referred to as “sensitive information”), including ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject: Provided, That this shall not apply in any of the following circumstances: *<Amended by Act No. 14107, Mar. 29, 2016>*

1. Where the personal information controller informs the data subject of the matters provided for in Article 15 (2) or 17 (2), and obtains the consent of the data subject apart from the consent to the processing of other personal information;
2. Where other statutes require or permit the processing of sensitive information.

(2) Where a personal information controller processes sensitive information pursuant to paragraph (1), the personal information controller shall take measures necessary to ensure safety pursuant to Article 29 so that the sensitive information may not be lost, stolen, divulged, forged, altered, or damaged. *<Newly Inserted by Act No. 14107, Mar. 29, 2016>*

Article 24 (Limitation to Processing of Personally Identifiable Information)

(1) A personal information controller shall not process any information prescribed by Presidential Decree that can be used to identify an individual in accordance with statutes (hereinafter referred to as "personally identifiable information"), except in any of the following cases:

1. Where the personal information controller informs a data subject of the matters provided for in Article 15 (2) or 17 (2), and obtains the consent of the data subject apart from the consent to the processing of other personal information;

2. Where other statutes specifically require or permit the processing of unique identification information .

(2) Deleted. *<Act No. 11990, Aug. 6, 2013>*

(3) Where a personal information controller processes personally identifiable information pursuant to paragraph (1), the personal information controller shall take measures necessary to ensure safety, including encryption, as prescribed by Presidential Decree, so that the personally identifiable information may not be lost, stolen, divulged, forged, altered, or damaged. *<Amended by Act No. 13423, Jul. 24, 2015>*

(4) The Protection Commission shall regularly inspect whether a personal information controller meeting the criteria prescribed by Presidential Decree taking into account the types and amount of processed personal information, number of employees, amount of sales, etc., has taken the measures necessary to ensure safety pursuant to paragraph (3), as prescribed by Presidential Decree. *<Newly Inserted by Act No. 14107, Mar. 29, 2016; Act No. 14839, Jul. 26, 2017 ; Act No 16930, February. 4, 2020>*

(5) The Protection Commission may authorize specialized institutions prescribed by Presidential Decree to conduct the inspection referred to in paragraph (4). *<Newly Inserted by Act No. 14107, Mar. 29, 2016; Act No. 14839, Jul. 26, 2017 ; Act No 16930, February. 4, 2020>*

Article 24-2 (Limitation to Processing of Resident Registration Numbers)

(1) Notwithstanding Article 24 (1), a personal information controller shall not process any resident registration number, except in any of the following cases: *<Amended by Act No. 14107, Mar. 29, 2016; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

1. Where any Act, Presidential Decree, National Assembly Regulations, Supreme Court Regulations, Constitutional Court Regulations, National Election Commission Regulations or Board of Audit and Inspection Regulations specifically requires or permits the processing of resident registration numbers;
2. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party;
3. Where it is inevitable to process resident registration numbers in line with subparagraphs 1 and 2 in circumstances publicly notified by the Protection Commission.

(2) Notwithstanding Article 24 (3), a personal information controller shall retain resident registration numbers in a safe manner by means of encryption so that the resident registration numbers may not be lost, stolen, divulged, forged, altered, or damaged. In such cases, any necessary matters in relation to the scope of encryption objects and encryption timing by object, etc. shall be prescribed by Presidential Decree, taking into account the amount of personal information processed, data breach impact, etc. *<Newly Inserted by Act No. 12504, Mar. 24, 2014; Act No. 13423, Jul. 24, 2015>*

(3) A personal information controller shall provide data subjects with an alternative sign-up tool without using their resident registration numbers in the stage of being admitted to membership via the website while processing the resident registration numbers pursuant to paragraph (1).

(4) The Protection Commission may prepare and support such measures as legislative arrangements, policy-making, necessary facilities, and systems build-up in order to support the provision of the measures

provided for in paragraph (3). *<Amended by Act No. 12504, Mar. 24, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

Article 25 (Limitation to Installation and Operation of Visual Data Processing Devices)

(1) No one shall install and operate any visual data processing device at open places, except in any of the following circumstances:

1. Where specifically allowed by statutes;
2. Where it is necessary for the prevention and investigation of crimes;
3. Where it is necessary for the safety of facilities and prevention of fire;
4. Where it is necessary for regulatory control of traffic;
5. Where it is necessary for the collection, analysis, and provision of traffic information.

(2) No one shall install and operate any visual data processing device so as to look into the places which is likely to noticeably threaten individual privacy, such as a bathroom, restroom, sauna, and dressing room used by multiple unspecified persons: Provided, That the same shall not apply to the facilities prescribed by Presidential Decree, which detain or protect persons in accordance with statutes, such as correctional facilities and mental health care centers.

(3) The head of a public institution who intends to install and operate visual data processing devices pursuant to paragraph (1) and a person who intends to install and operate visual data processing devices pursuant to the proviso to paragraph (2) shall gather opinions of relevant specialist and interested persons through the formalities prescribed by Presidential Decree such as public hearings and information sessions.

(4) A person who installs and operates visual data processing devices pursuant to paragraph (1) (hereinafter referred to as “VDPD operator”) shall take necessary measures including posting on a signboard the following matters, so that data subjects may easily recognize such devices: Provided, That this shall not apply to military installations defined in subparagraph 2 of Article 2 of the Protection of Military Bases and Installations Act, important national facilities defined in subparagraph 13 of Article 2 of the United Defense Act, and other facilities prescribed by Presidential Decree: *<Amended by Act No. 14107, Mar. 29, 2016>*

1. The purpose and place of installation;
2. The scope and hours of photographing;
3. The name and contact information of the person in charge of its management;
4. Other matters prescribed by Presidential Decree.

(5) A VDPD operator shall not handle arbitrarily the visual data processing devices for other purposes than the initial one; direct the said devices toward different spots; nor use sound recording functions.

(6) Every VDPD operator shall take measures necessary to ensure safety pursuant to Article 29 so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged. *<Amended by Act No. 13423, Jul. 24, 2015>*

(7) Every VDPD operator shall establish an appropriate policy to operate and manage the visual data processing devices, as prescribed by Presidential Decree. In such cases, the VDPD operator may be exempted from adopting a Privacy Policy pursuant to Article 30.

(8) A VDPD operator may outsource the installation and operation of visual data processing devices to a third party: Provided, That the public institutions shall comply with the procedures and requirements prescribed by Presidential Decree when outsourcing the installation and operation of visual data processing devices to a third party.

Article 26 (Limitation to Personal Information Processing Subsequent to Outsourcing of Work)

(1) A personal information controller shall, when outsourcing personal information processing to a third party, effect such outsourcing through a document that states the following:

1. Prevention of personal information processing for other purposes than the outsourced purpose;
2. Technical and managerial safeguards of personal information;
3. Other matters prescribed by Presidential Decree to ensure safe management of personal information.

(2) A personal information controller that outsources personal information processing pursuant to paragraph (1) (hereinafter referred to as "outsourcer") shall disclose the details of the outsourced work and the entity that processes personal information (hereinafter referred to as “outsourcee”) under an outsourcing contract in the manner prescribed by Presidential Decree so that data subjects may recognize it with ease at any time.

(3) The outsourcer shall, in case of outsourcing the promotion of goods or services, or soliciting of sales thereof, notify data subjects of the outsourced work and the outsourcee in the manners prescribed by Presidential Decree. The same shall apply where the outsourced work or the outsourcee has been changed.

(4) The outsourcer shall educate the outsourcee so that personal information of data subjects may not be lost, stolen, leaked, forged, altered, or damaged owing to the outsourcing of work, and supervise how the outsourcee processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree. *<Amended by Act No. 13423, Jul. 24, 2015>*

(5) An outsourcee shall not use any personal information beyond the scope of the work outsourced by the personal information controller, nor provide personal information to a third party.

(6) With respect to the compensation of damage arising out of the processing of personal information outsourced to an outsourcee in violation of this Act, the outsourcee shall be deemed an employee of the personal information controller.

(7) Articles 15 through 25, 27 through 31, 33 through 38, and 59 shall apply mutatis mutandis to outsourcees.

Article 27 (Limitation to Transfer of Personal Information following Business Transfer, etc.)

(1) A personal information controller shall notify in advance the data subjects of the following matters in the manner prescribed by Presidential Decree in the case of transfer of personal information to a third party owing to the transfer of some or all of his or her business, a merger, etc.:

1. The fact that the personal information will be transferred;

2. The name (referring to the company name in case of a legal person), address, telephone number and other contact information of the recipient of the personal information (hereinafter referred to as "business transferee, etc.");

3. The method and procedure for withdrawing consent if the data subject does not wish his or her personal information to be transferred.

(2) Upon receiving personal information, the business transferee, etc. shall, without delay, notify data subjects of the fact in the manner prescribed by Presidential Decree: Provided, That this shall not apply where the personal information controller has already notified the data subjects of the fact of such transfer pursuant to paragraph (1).

(3) Upon receiving personal information owing to business transferee, etc., a merger, etc., the business transferee may use, or provide a third party with, the personal information only for the initial purposes dating to the time of the transfer. In such cases, the business transferee shall be deemed the personal information controller.

Article 28 (Supervision of Personal Information Handlers)

(1) While processing personal information, a personal information controller shall conduct appropriate control and supervision against the persons who process the personal information under his or her command and supervision, such as an officer or employee, temporary agency worker and part-time worker (hereinafter referred to as "personal information handler") to ensure the safe management of the personal information.

(2) A personal information controller shall provide personal information handlers with necessary educational programs on a regular basis in order to ensure the appropriate handling of personal information.

Article 28-2 (Processing of Pseudonymous Data)

(1) A personal information controller may process pseudonymized information without the consent of data subjects for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.

(2) A personal information controller shall not include information that may be used to identify a certain individual when providing pseudonymized information to a third party according to paragraph (1).

Article 28-3 (Restriction on Combination of Pseudonymous Data)

(1) Notwithstanding Article 28-2, the combination of pseudonymized information processed by different personal information controllers for statistical purposes, scientific research and preservation of records for public interest, etc. shall be conducted by a specialized institution designated by the Protection Commission or the head of the related central administrative agency.

(2) A personal information controller who intends to release the combined information outside the organization that combined the information shall obtain approval from the head of the specialized institution after processing the information into pseudonymized information or the form referred to in

Article 58-2.

(3) Necessary matters including the procedures and methods of combination pursuant to paragraph (1), standards and procedures to designate, or cancel the designation of, a specialized institution management and supervision, and standards and procedures of exporting and approval pursuant to paragraph (2) shall be prescribed by Presidential Decree.

Article 28-4 (Obligation to Take Safety Measures for Pseudonymous Data)

(1) When processing the pseudonymized information, a personal information controller shall take such technical, organizational and physical measures as separately storing and managing additional information needed for restoration to the original state, as may be necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged.

(2) A personal information controller who intends to process the pseudonymized information shall prepare and keep records relating to matters prescribed by the Presidential Decree including the purpose of processing the pseudonymized information, and a third party recipient when pseudonymized information is provided, to manage the processing of pseudonymized information.

Article 28-5 (Prohibited Acts for the Processing of the Pseudonymized Information)

(1) No one shall process the pseudonymized information for the purpose of identifying a certain individual.

(2) When information identifying a certain individual is generated while the pseudonymized information is processed, the personal information controller shall cease the processing of the information, and retrieve and destroy the information immediately.

Article 28-6 (Imposition of Administrative Surcharges for the Processing of the Pseudonymized Information)

(1) The Commission may impose a fine equivalent to less than three-hundredths of total sales on data controller who has processed data for the purpose of identifying a specific individual in violation of Article 28-5 (1): Provided, That in case where there is no sales or difficulty in calculating the sales revenues, the data controller may be subject to a fine of not more than 400 million won or three-hundredths of the capital amount, whichever is greater.

(2) Article 34-2 (3) through (5) shall apply mutatis mutandis to matters necessary to impose and collect administrative surcharges.

Article 28-7 (Scope of Application)

@Articles 20, 21, 27, 34 (1), 35 through 37, 39-3, 39-4, 39-6 through 39-8 shall not apply to the pseudonymized information.

Article 29 (Duty of Safeguards)

Every personal information controller shall take such technical, managerial, and physical measures as establishing an internal management plan and preserving access records, etc. that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen,

divulged, forged, altered, or damaged. *<Amended by Act No. 13423, Jul. 24, 2015>*

Article 30 (Establishment and Disclosure of Privacy Policy)

(1) Every personal information controller shall establish a personal information processing policy including the following matters (hereinafter referred to as "Privacy Policy"). In such cases, public institutions shall establish the Privacy Policy for the personal information files to be registered pursuant to Article 32: *<Amended by Act No. 14107, Mar. 29, 2016>*

1. The purposes for which personal information is processed;
2. The period for processing and retaining personal information;
3. Provision of personal information to a third party (if applicable);
3-2. Procedures and methods for destroying personal information (if personal information shall be preserved according to the proviso of Article 21 (1), this shall include the basis of preservation and particulars of personal information to be preserved);
4. Outsourcing personal information processing (if applicable);
5. The rights and obligations of data subjects and legal representatives, and how to exercise such rights;
6. Contact information, such as the name of a privacy officer designated under Article 31 or the name, telephone number, etc. of the department which performs the duties related to personal information protection and handles related grievances;
7. Installation and operation of an automatic collection tool for personal information, including internet access data files, and the denial thereof (if applicable);
8. Other matters prescribed by Presidential Decree regarding the processing of personal information.

(2) Upon establishing or modifying the Privacy Policy, a personal information controller shall disclose the content so that data subjects may easily recognize it in such a way as prescribed by Presidential Decree.

(3) Where there exist discrepancies between the Privacy Policy and the agreement executed by and between the personal information controller and data subjects, the terms that are beneficial to the data subjects shall prevail.

(4) The Protection Commission may prepare the Privacy Policy Guidelines and encourage the personal information controllers to comply with such Guidelines. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

Article 31 (Designation of Privacy Officers)

(1) A personal information controller shall designate a privacy officer who comprehensively takes charge of personal information processing.

(2) Every privacy officer shall perform the following functions:

1. To establish and implement a personal information protection plan;
2. To conduct a regular survey of the status and practices of personal information processing, and to improve shortcomings;
3. To handle grievances and remedial compensation in relation to personal information processing;

4. To build the internal control system to prevent the divulgence, abuse, and misuse of personal information;

5. To prepare and implement an education program about personal information protection;

6. To protect, control, and manage the personal information files;

7. Other functions prescribed by Presidential Decree for the appropriate processing of personal information.

(3) In performing the functions provided for in paragraph (2), a privacy officer may inspect the status of personal information processing and systems frequently, if necessary, and may request a report thereon from the relevant parties.

(4) Where a privacy officer becomes aware of any violation of this Act or other relevant statutes in relation to the protection of personal information, the privacy officer shall take corrective measures immediately, and shall report such corrective measures to the head of the institution or organization to which he or she belongs, if necessary.

(5) A personal information controller shall not have the chief privacy officer impose or be subject to disadvantages without any justifiable ground while performing the functions provided for in paragraph (2).

(6) The requirements for designation as privacy officers, functions, qualifications, and other necessary matters, shall be prescribed by Presidential Decree.

Article 32 (Registration and Disclosure of Personal Information Files)

(1) Upon operating personal information files, the head of a public institution shall register the following matters with the Protection Commission. The same shall also apply where the registered matters are modified. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

1. The titles of the personal information files;

2. The grounds and purposes for the operation of the personal information files;

3. Particulars of personal information that are recorded in the personal information files;

4. The method of processing personal information;

5. The period for retaining personal information;

6. The recipient of personal information, if it is provided routinely or repetitively;

7. Other matters prescribed by Presidential Decree.

(2) Paragraph (1) shall not apply to any of the following personal information files:

1. Personal information files that record national security, diplomatic secrets, and other matters relating to grave national interests;

2. Personal information files that record the investigation of crimes, indictment and prosecution, punishment, and probation and custody, corrective orders, protective orders, security observation orders, and immigration;

3. Personal information files that record the investigations of violations of the Punishment of Tax Offenses Act and the Customs Act;

4. Personal information files exclusively used for internal job performance of public institutions;

5. Classified personal information files pursuant to other statutes.

(3) The Protection Commission may, if necessary, review the registration and content of the personal information files referred to in paragraph (1), and advise the head of the relevant public institution to make improvements. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(4) The Protection Commission shall make public the status of registered personal information files under paragraph (1) so that anyone may access them with ease. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(5) Necessary matters regarding the registration referred to in paragraph (1), the method, scope, and procedure of public disclosure referred to in paragraph (4), shall be prescribed by Presidential Decree.

(6) The registration and public disclosure of the personal information files retained by the National Assembly, the Court, the Constitutional Court and the National Election Commission (including their affiliated entities) shall be prescribed by the National Assembly Regulations, the Supreme Court Regulations, the Constitutional Court Regulations, and the National Election Commission Regulations.

Article 32-2 (Certification of Personal Information Protection)

(1) The Protection Commission may certify whether the data processing and other data protection-related action of a personal information controller abide by this Act, etc. *<Amended by Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(2) The certification provided for in paragraph (1) shall be effective for three years.

(3) In any of the following cases, the Protection Commission may revoke the certification granted under paragraph (1), as prescribed by Presidential Decree: Provided, That it shall be revoked in cases falling under subparagraph 1: *<Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

1. Where personal information protection has been certified by fraud or other unjust means;

2. Where follow-up management provided for in paragraph (4) has been denied or obstructed;

3. Where the certification criteria provided for in paragraph (8) have not been satisfied;

4. Where personal information protection-related statutes are breached seriously.

(4) The Protection Commission shall conduct follow-up management at least once annually to maintain the effectiveness of the certification of personal information protection. *<Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(5) The Protection Commission may authorize the specialized institutions prescribed by Presidential Decree to perform the duties related to certification under paragraph (1), revocation of certification under paragraph (3), follow-up management under paragraph (4), management of certification examiners under paragraph (7). *<Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(6) Any person who has obtained certification subject to paragraph (1) may indicate or promote the certification, as prescribed by Presidential Decree.

(7) Qualifications of certification examiners who conduct the certification examination subject to paragraph (1), criteria for disqualification, and other related matters shall be prescribed by Presidential Decree, taking into account specialty, career, and other necessary matters.

(8) Other necessary matters for the certification criteria, method, procedure, etc. subject to paragraph (1), including whether the personal information management system, guarantee of data subjects' rights, and measures to ensure safety are based on this Act, shall be prescribed by Presidential Decree.

Article 33 (Privacy Impact Assessment)

(1) In the case there is a risk of an infringement with respect to personal information of data subjects due to the operation of personal information files meeting the criteria prescribed by Presidential Decree, the head of a public institution shall conduct an assessment to analyze risk factors and improve them (hereinafter referred to as "privacy impact assessment"), and submit the results thereof to the Protection Commission. In such cases, the head of the public institution shall request the privacy impact assessment from any of the institutions designated by the Protection Commission (hereinafter referred to as "PIA institution"). *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(2) The privacy impact assessment shall cover the following matters:

1. The number of personal information being processed;
2. Whether the personal information is provided to a third party;
3. The probability to violate the rights of the data subjects and the degree of risks;
4. Other matters prescribed by Presidential Decree.

(3) The Protection Commission may provide its opinion on the results of the privacy impact assessment submitted under paragraph (1). *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(4) The head of a public institution shall register the personal information files in accordance with Article 32 (1), for which the privacy impact assessment has been conducted pursuant to paragraph (1), with the results of the privacy impact assessment attached thereto.

(5) The Protection Commission shall take necessary measures, such as fostering relevant specialists, and developing and disseminating criteria for the privacy impact assessment, to promote the privacy impact assessment. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(6) Necessary matters in relation to the privacy impact assessment, such as the criteria for designation as PIA institutions, revocation of designation, assessment criteria, method and procedure, etc. pursuant to paragraph (1), shall be prescribed by Presidential Decree.

(7) Matters regarding the privacy impact assessment conducted by the National Assembly, the Court, the Constitutional Court and the National Election Commission (including their affiliated entities) shall be prescribed by the National Assembly Regulations, the Supreme Court Regulations, the Constitutional Court Regulations, and the National Election Commission Regulations.

(8) A personal information controller other than public institutions shall proactively endeavor to conduct a privacy impact assessment, if there is a risk of an infringement with respect to personal information of data subjects in operating the personal information files.

Article 34 (Data Breach Notification)

(1) A personal information controller shall notify data subjects of the following matters without delay when the personal information controller becomes aware their personal information has been divulged:

1. Particulars of the personal information divulged;
2. When and how personal information has been divulged;
3. Any information about how the data subjects can minimize the risk of damage from divulgence, etc.;
4. Countermeasures taken by the personal information controller and remedial procedure;
5. Help desk and contact points for the data subjects to report damage.

(2) A personal information controller shall prepare countermeasures to minimize the risk of damage in the case of divulgence of personal information and take necessary measures.

(3) Where a breach of personal information above the scale prescribed by Presidential Decree takes place, the personal information controller shall, without delay, report the results of notification given under paragraph (1) and the results of measures taken under paragraph (2) to the Protection Commission or a specialized institution designated by Presidential Decree. In such cases, the Protection Commission and the specialized institution designated by Presidential Decree may provide technical assistance for the prevention and recovery of further damage, etc. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(4) Necessary matters in relation to the time, method, and procedure of data breach notification pursuant to paragraph (1), shall be prescribed by Presidential Decree.

Article 34-2 (Imposition, etc. of Penalty Surcharges)

(1) The Protection Commission may impose and collect a penalty surcharge not exceeding 500 million won where a personal information controller has failed to prevent any loss, theft, divulgence, forgery, alteration, or damage of resident registration numbers: Provided, That this shall not apply where the personal information controller has fully taken measures necessary to ensure safety under Article 24 (3) to prevent any loss, theft, divulgence, forgery, alteration, or damage of resident registration numbers. *<Amended by Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(2) The Protection Commission shall take into account the following when imposing the administrative surcharge pursuant to paragraph (1): *<Amended by Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

1. Scale of efforts taken to perform the measures necessary to ensure safety under Article 24 (3);
2. Status of the resident registration numbers which have been lost, stolen, divulged, forged, altered or damaged;

3. Fulfillment of subsequent measures to prevent further damage.

(3) The Protection Commission shall collect a late-payment penalty prescribed by Presidential Decree in an amount not exceeding 6/100 per annum of the unpaid administrative surcharge for the period beginning on the following day of the expiration of the payment deadline and ending on the day immediately preceding the day of payment of the administrative surcharge where a person liable to pay the administrative surcharge under paragraph (1) fails to pay the same by the payment deadline. In such cases, the late-payment penalty shall be collected for a maximum period of 60 months. *<Amended by Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(4) Where a person liable to pay the administrative surcharge under paragraph (1) fails to pay the same by the payment deadline, the Protection Commission shall give notice with the period of payment specified therein; and where the administrative surcharge and late-payment penalty are not paid within the specified period, the Protection Commission shall collect such administrative surcharge and late-payment penalty in the same manner as delinquent national taxes are collected. *<Amended by Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(5) Other matters necessary for imposing and collecting penalty surcharges shall be prescribed by Presidential Decree.

Article 35 (Access to Personal Information)

(1) A data subject may request access to his or her own personal information, which is processed by a personal information controller, from the personal information controller.

(2) Notwithstanding paragraph (1), where a data subject intends to request access to his or her own personal information from a public institution, the data subject may request such access directly from the said public institution, or indirectly via the Protection Commission, as prescribed by Presidential Decree. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>*

(3) Upon receipt of a request for access filed under paragraphs (1) and (2), a personal information controller shall grant the data subject access to his or her own personal information within the period prescribed by Presidential Decree. In such cases, if there is any justifiable ground not to permit access during such period, the personal information controller may postpone access after notifying the relevant data subject of the said ground. If the said ground ceases to exist, the data subject shall be permitted to access the personal information without delay.

(4) In any of the following cases, a personal information controller may limit or deny access after it notifies a data subject of the cause:

1. Where access is prohibited or limited by Acts;
2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person;
3. Where a public institution has grave difficulties in performing any of the following duties:

(a) Imposition, collection or refund of taxes;

(b) Evaluation of academic achievements or admission affairs at the schools of each level established under the Elementary and Secondary Education Act and the Higher Education Act, lifelong educational facilities established under the Lifelong Education Act, and other higher educational institutions established under other Acts;

(c) Testing and qualification examination regarding academic competence, technical capability and employment;

(d) Ongoing evaluation or decision-making in relation to compensation or grant assessment;

(e) Ongoing audit and examination under other Acts.

(5) Necessary matters in relation to the methods and procedures to file access requests, to limit access, to give notification, etc. pursuant to paragraphs (1) through (4) shall be prescribed by Presidential Decree.

Article 36 (Rectification or Erasure of Personal Information)

(1) A data subject who has accessed his or her personal information pursuant to Article 35 may request a correction or erasure of such personal information from the relevant personal information controller: Provided, That the erasure is not permitted where the said personal information shall be collected by other statutes.

(2) Upon receipt of a request by a data subject pursuant to paragraph (1), the personal information controller shall investigate the personal information in question without delay; shall take necessary measures to correct or erase as requested by the data subject unless otherwise specifically provided by other statutes in relation to correction or erasure; and shall notify such data subject of the result.

(3) The personal information controller shall take measures not to recover or revive the personal information in case of erasure pursuant to paragraph (2).

(4) Where the request of a data subject falls under the proviso to paragraph (1), a personal information controller shall notify the data subject of the details thereof without delay.

(5) While investigating the personal information in question pursuant to paragraph (2), the personal information controller may, if necessary, request from the relevant data subject the evidence necessary to confirm a correction or erasure of the personal information.

(6) Necessary matters in relation to the request of correction and erasure, notification method and procedure, etc. pursuant to paragraphs (1), (2) and (4) shall be prescribed by Presidential Decree.

Article 37 (Suspension of Processing of Personal Information)

(1) A data subject may request the relevant personal information controller to suspend the processing of his or her personal information. In such cases, if the personal information controller is a public institution, the data subject may request the suspension of processing of only the personal information contained in the personal information files to be registered pursuant to Article 32.

(2) Upon receipt of the request under paragraph (1), the personal information controller shall, without delay, suspend processing of some or all of the personal information as requested by the data subject: Provided, That, where any of the following is applicable, the personal information controller may deny the

request of such data subject:

1. Where special provisions exist in other laws or it is inevitable to observe legal obligations;
2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person;
3. Where the public institution cannot perform its work as prescribed by any Act without processing the personal information in question;
4. Where it is impracticable to perform a contract such as the provision of services as agreed upon with the said data subject without processing the personal information in question, and the data subject has not clearly expressed the desire to terminate the agreement.

(3) When denying the request pursuant to the proviso to paragraph (2), the personal information controller shall notify the data subject of the reason without delay.

(4) The personal information controller shall, without delay, take necessary measures including destruction of the relevant personal information when suspending the processing of personal information as requested by data subjects.

(5) Necessary matters in relation to the methods and procedures to request the suspension of processing, to deny such request, and to give notification, etc. pursuant to paragraphs (1) through (3) shall be prescribed by Presidential Decree.

Article 38 (Methods and Procedures for Exercise of Rights)

(1) A data subject may authorize his or her representative to file requests for access pursuant to Article 35, correction or erasure pursuant to Article 36, suspension of processing pursuant to Article 37, and withdrawal of consent pursuant to Article 39-7 (hereinafter referred to as “request for access, etc.”) by the methods and procedure prescribed by Presidential Decree, such as written documents. *<Amended by Act No 16930, February. 4, 2020>*

(2) The legal representative of a child under 14 years of age may file a request for access, etc. to the personal information of the child with a personal information controller.

(3) A personal information controller may demand a fee and postage (only in case of a request to mail the copies), as prescribed by Presidential Decree, from a person who files a request for access, etc.

(4) A personal information controller shall prepare the detailed method and procedure to enable data subjects to file requests for access, etc., and publicly announce such method and procedure so that the data subjects may become aware of them.

(5) A personal information controller shall prepare and provide necessary procedures for data subjects to raise objections regarding the denial of a request for access, etc. from such data subjects.

Article 39 (Responsibility for Compensation)

(1) A data subject who suffers damage by reason of a violation of this Act by a personal information controller is entitled to claim compensation from the personal information controller for such damage. In such cases, the said personal information controller may not be released from responsibility for compensation if it fails to prove the non-existence of wrongful intent or negligence.

(2) Deleted. *<by Act No. 13423, Jul. 24, 2015>*

(3) Where a data subject suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his or her own personal information, caused by wrongful intent or negligence of a personal information controller, the Court may determine the amount of compensation for damage not exceeding three times such damage: Provided, That the same shall not apply to the personal information controller who has proved non-existence of his or her wrongful intent or negligence. *<Newly Inserted by Act No. 13423, Jul. 24, 2015>*

(4) The Court shall take into account the following when determining the amount of compensation for damage pursuant to paragraph (3): *<Newly Inserted by Act No. 13423, Jul. 24, 2015>*

1. The degree of wrongful intent or expectation of damage;
2. The amount of loss caused by the violation;
3. Economic benefits the personal information controller gained in relation to the violation;
4. A fine and a penalty surcharge to be levied subject to the violation;
5. The duration, frequency, etc. of violations;
6. The property of the personal information controller;
7. The personal information controller's efforts to retrieve the affected personal information after the loss, theft, or divulgence of personal information;
8. The personal information controller's efforts to remedy damage suffered by the data subject.

Article 39-2 (Claims for Statutory Compensation)

(1) Notwithstanding Article 39 (1), a data subject, who suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his or her own personal information, caused by wrongful intent or negligence of a personal information controller, may claim a reasonable amount of damages not exceeding three million won. In such cases, the said personal information controller may not be released from the responsibility for compensation if it fails to prove non-existence of his or her wrongful intent or negligence.

(2) In the case of a claim made under paragraph (1), the Court may determine a reasonable amount of damages not exceeding the amount provided for in paragraph (1) taking into account all arguments in the proceedings and the results of examining evidence.

(3) A data subject who has claimed compensation pursuant to Article 39 may change such claim to the claim provided for in paragraph (1) until the closure of fact-finding proceedings.

Article 39-3 (Special Provisions on Consent to the Collection and Use of Personal Information)

(1) Notwithstanding Article 15 (1), an information and communications service provider who intends to collect and use personal information of users shall notify users of the following matters and obtain consent therefor. The same shall apply when changes are made for the following matters:

1. The purpose of the collection and use of personal information;
2. Particulars of personal information to be collected;

3. The period for retaining and using personal information.

(2) An information and communications service provider may collect and use personal information of users without their consent under paragraph (1) in any of the following cases:

1. Where the information is necessary in implementing a contract for provision of information and communications services (referring to the information and communications services defined in Article 2 (1) 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection; hereinafter the same shall apply), but it is clearly difficult to obtain ordinary consent for economic and technical reasons;

2. Where the information is necessary to calculate fees for the provision of information and communications services;

3. Where special provisions exist in other laws.

(3) No information and communications service provider shall reject the provision of services for the reason that a user does not provide his/her personal information beyond the minimum personal information required. The minimum personal information refers to information that is necessary for the performance of the fundamental functions of the services.

(4) An information and communications provider who intends to obtain consent from children aged under 14 for the collection, use and provision of personal information shall obtain such consent from his/her legal representative and confirm whether the legal representative has granted consent as prescribed by the Presidential Decree.

(5) An information and communications provider shall, when notifying children aged under 14 of matters relating to the processing of personal information, use understandable forms and plain and readily comprehensible language.

(6) The Protection Commission shall take measures to protect the personal information of children aged under 14 who may not clearly understand matters such as the risks and results of personal information processing and users' rights.

Article 39-4 (Special Cases on the Notification and Reporting on the Divulgence of Personal Information)

(1) Notwithstanding Article 34 (1) and (3), information and communications service provider and a person who receives personal information of users therefrom pursuant to Article 17 (1) (hereinafter referred to as "information and communications service provider, etc.") shall notify the relevant users of the following matters without delay upon becoming aware that their personal information has been lost, stolen or divulged (hereinafter referred to as "divulgence, etc."), report such case to a specialized institution prescribed by the Protection Commission or Presidential Decree, and shall notify the users or report that matter not later than 24 hours since he or she became aware of such fact, without a justifiable reason: Provided, That if there is a justifiable reason such as users' contact number being unknown, other measures may be taken in lieu of notification as prescribed by Presidential Decree:

1. Particulars of the personal information divulged, etc.;
2. The time when the personal information has been divulged, etc.;
3. Any measure that users can take;
4. Countermeasures to be taken by of the information and communications service provider, etc.;
5. Department and contact points to which the user can apply for consultation.

(2) A specialized institution prescribed by Presidential Decree which receives a report pursuant to paragraph (1) shall notify the Protection Commission of the case without delay.

(3) An information and communications service provider, etc. shall explain any justifiable reason pursuant to paragraph (1) to the Protection Commission.

(4) Necessary matters in relation to the methods and procedures of notification and reporting under paragraph (1) shall be prescribed by the Presidential Decree.

Article 39-5 (Special Cases on Safeguards for Personal Information)

Information and communications service provider, etc. shall limit the number of persons who process users' personal information to the minimum extent.

Article 39-6 (Special Cases on the Destruction of Personal Information)

(1) Information and communications service provider, etc. shall take necessary measures as prescribed by Presidential Decree such as destruction to protect the personal information of users who have not used information and communications services for one year: Provided, That, if the period is designated otherwise by other statutes or at the request of the user, the designated period shall apply.

(2) Information and communications service provider, etc. shall notify users of 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 by a method prescribed by Presidential Decree such as e-mail, at least 30 days prior to the expiration of the above designated period.

Article 39-7 (Special Cases on Users' Rights)

(1) Users may withdraw consent to the collection, use and provision of personal information at any time from information and communications service provider, etc.

(2) Information and communications service providers, etc. must make it easier for users to request to withdraw their consent under paragrah (1), to access their information under Article 35, and to rectify under Article 36 than to give consent to the collection of their personal information.

(3) Once a user withdraws his or her consent pursuant to paragraph (1), the information and communications service provider, etc. shall take necessary measures without delay such as destroying the information to such an extent that it is not recoverable or revivable.

Article 39-8 (Notification of the Use History of Personal Information)

(1) Information and communications service provider, etc. meeting standards prescribed by President Decree shall notify users of the use history of their personal information collected pursuant to Articles 23 and 39-3 (including provision pursuant to Article 17) on a regular basis: Provided, That this shall not apply where the collected information does not include a contact number, etc. that enables notification to

users,

(2) The type of information to be notified to users under paragraph (1), the types of information to be notified, the frequency and method of notification, and other matters necessary for the notification of the details shall be determined by Presidential Decree.

Article 39-9 (Indemnity for Losses)

(1) Information and communications service providers, etc. shall take necessary measures such as purchasing insurance or deduction plans or accumulating reserves to fulfil its liabilities for compensation pursuant to Articles 39 and 39-2.

(2) Necessary matters including the scope of personal information controllers subject to the obligation pursuant to paragraph (1) and relevant standards shall be prescribed by Presidential Decree.

Article 39-10 (Deletion and Blocking of Exposed Personal Information)

(1) Information and communications service provider, etc. shall ensure that users' personal information including resident registration number, bank account information and credit card information is not exposed to the public through information and communications networks.

(2) Notwithstanding paragraph (1), at the request of the Protection Commission or specialized institutions designated by Presidential Decree in relation to personal information exposed to the public, information and communications service provider, etc. shall take necessary measures such as deleting and blocking.

Article 39-11 (Designation of Domestic Agents)

(1) Information and communications service provider, etc. with no address or business office in Korea meeting the criteria prescribed by Presidential Decree in consideration of the number of users and revenues shall designate an agent to act on his or her behalf with respect to the following (hereinafter referred to as "domestic agent") in writing:

1. Duties of a privacy officer under Article 31;
2. Notification and reporting under Article 39-4;
3. Submission of related articles, documents, etc. under Article 63 (1).

(2) A domestic agent shall have an address or business office in Korea.

(3) When a domestic agent is designated pursuant to paragraph (1), the following matters shall all be included in the Privacy Policy pursuant to Article 30:

1. Name of the domestic agent (for a corporation, the title and name of the representative);
2. Address of the domestic agent (for a corporation, location of a business office), telephone number, e-mail address.

(4) If the domestic agent violates this Act in relation to each item of paragraph (1), the information and communications service provider, etc. shall be deemed to have committed such a violation.

Article 39-12 (Protection of Information Transferred Overseas)

(1) The information and communications service provider, etc. shall not execute an international contract in violation of this Act in relation to users' personal information.

(2) Notwithstanding Article 17 (3), information and communications service provider, etc. shall obtain users' consent if intending to provide (including accessing), outsource the processing of, or store (hereinafter referred to as "transfer" in this Article) users' personal information overseas: Provided, That if all items of paragraph (3) below are made public pursuant to Article 30 (2) or notified to users by a method prescribed by the Presidential Decree such as e-mail, the information and communications service provider, etc. may opt not to obtain users' consent to outsourcing the processing of, or storing, personal information.

(3) The information and communications service provider, etc. shall notify users of the following matters in advance if intending to obtain consent under paragraph (2):

1. Particulars of the personal information to be transferred;
2. The country to which the personal information is transferred, transfer date and method;
3. Name of the entity to which the personal information is transferred (referring to the name of a corporation and the contact information of the person responsible for the management of information, if the person is a corporation);
4. The purpose of using personal information by the entity to which the information is transferred and the period of retaining and using personal information.

(4) The information and communications service provider, etc. shall implement safeguards as prescribed by Presidential Decree if intending to transfer personal information overseas with consent obtained pursuant to paragraph (2).

(5) where a person who receives personal information of the users transfers it to a third country, he or she shall comply with paragraphs (1) through (4). In such cases, "information and communications service providers, etc." shall be regarded as "personal information recipient," and "personal information recipient" shall be regarded as "a person who receives personal information from a third country.

Article 39-13 (Reciprocity)

Notwithstanding Article 39-12, information and communications service providers, etc. in a country that restricts cross-border transfer may face an equivalent level of restrictions in another country: Provided, That this shall not apply where cross-border transfer is necessary to implement a pact or other international arrangements.

Article 39-14 (Special Cases for Broadcasting Service Providers)

If entities falling under subparagraphs 3 (a) through (e), 6, 9, 12 and 14 of Article 2 of the Broadcasting Act (hereinafter referred to as "broadcasting service provider, etc.") process the personal information of viewers, the broadcasting service provider, etc. shall observe regulations applicable to an information and communications service provider, etc. In such cases, "broadcasting service provider, etc." shall be deemed to be "information and communications service provider, etc." and "viewers" to be "users."

Article 39-15 (Special Cases for the Imposition of Administrative Surcharges)

(1) Upon information and communications service provider, etc. conducting any of the following acts, the Protection Commission may impose administrative surcharges not exceeding 3/100 of the total revenues

relating to the concerned violation:

1. Using or providing personal information in violation of Articles 17 (1), 17 (2), 18 (1), 18 (2), and 19 (including applicable cases pursuant to Article 39-14);
2. Collecting personal information of a child aged under 14 without his/her legal representative's consent in violation of Article 22 (6) (including applicable cases pursuant to Article 39-14);
3. Collecting sensitive information without the user's consent in violation of Article 23 (1) 1 (including applicable cases pursuant to Article 39-14);
4. Where it neglects its control, supervision, or education under Article 26 (4) (including where the aforesaid provisions apply mutatis mutandis pursuant to Article 39-14), thereby causing an outsourcee subject to special cases to violate this Act;
5. Losing, stealing, divulging, forging, altering, or damaging users' personal information and failing to take measures (excluding matters on the establishment of internal management plan) set forth in Article 29 (including applicable cases pursuant to Article 39-14);
6. Collecting users' personal information without their consent in violation of Article 39-3 (1) (including applicable cases pursuant to Article 39-14);
7. Providing users' personal information overseas without their consent in violation of the main clause of Article 39-12 (2) (including applicable cases pursuant to paragraph (5) of the same Article).

(2) When administrative surcharges are imposed in accordance to paragraph (1), but the information and communications service provider, etc. either refuses to submit basic materials for revenue calculation or submits false documents, their revenues may be estimated based on the accounting documents, such as financial statements, and operational status, such as the number of subscribers and usage fees, of similar-sized information and communications service providers, etc.: Provided, That up to 400 won million may be imposed as administrative surcharges on an information and communications service provider, etc. having no revenues or revenues difficult to calculate as prescribed by Presidential Decree.

(3) The Protection Commission shall consider the following matters to impose administrative surcharges under paragraph (1):

1. Details and degree of the violation;
2. Period and number of the violation;
3. Size of profits gained from the violation.

(4) Administrative surcharges under paragraph (1) shall be calculated in consideration of paragraph (3), but the detailed calculation standards and procedures shall be prescribed by Presidential Decree.

(5) The Protection Commission shall collect a late-payment penalty in the amount not exceeding 6/100 per annum of the unpaid administrative surcharges for the period beginning on the following day of the expiration of the payment deadline.

(6) Where a person liable to pay the administrative surcharges under paragraph (1) fails to pay it by the payment deadline, the Protection Commission shall give notice with the period of payment specified in it; and where the administrative surcharges and late-payment penalty under paragraph (5) are not paid within

the specified period, the Protection Commission shall collect such administrative surcharges and late-payment penalty in the same manner as delinquent national taxes are collected.

(7) When the administrative surcharges imposed according to paragraph (1) are refunded for such reasons as a court's decision, the Protection Commission shall make additional payments in the amount calculated based on the interest rate prescribed by Presidential Decree considering the deposit interest rates of financial companies, etc., for the period beginning on the following day of the payment of administrative surcharges and ending on the day of the refund.

(8) Notwithstanding paragraph (7), when a disposition of imposing administrative surcharges is revoked due to a court's decision and new administrative surcharges are imposed based on the reasoning of the decision, additional payments shall be calculated and paid with respect to the amount that remains after the newly imposed administrative surcharges are deducted from the already paid administrative surcharges.

Article 40 (Establishment and Composition)

(1) There shall be established a Personal Information Dispute Mediation Committee (hereinafter referred to as the "Dispute Mediation Committee") to mediate disputes over personal information.

(2) The Dispute Mediation Committee shall be comprised of not more than 20 members, including one chairperson, and the members shall be ex officio members and commissioned members. *<Amended by Act No. 13423, Jul. 24, 2015>*

(3) The commissioned members shall be commissioned by the Chairperson of the Protection Commission from among the following persons, and public officials of the national agencies prescribed by Presidential Decree shall be ex officio members: *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015>*

1. Persons who previously served as members of the Senior Executive Service of the central administrative agencies in charge of personal information protection, or persons who presently work or have worked at equivalent positions in the public sector and related organizations, and have job experience in personal information protection;
2. Persons who presently serve or have served as associate professors or higher positions in universities or in publicly recognized research institutes;
3. Persons who presently serve or have served as judges, public prosecutors, or attorneys-at-law;
4. Persons recommended by data protection-related civic organizations or consumer groups;
5. Persons who presently work or have worked as senior officers for the trade associations comprised of personal information controllers.

(4) The chairperson shall be commissioned by the Chairperson of the Protection Commission from among Committee members who are not public officials. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015>*

(5) The term of office for the chairperson and commissioned members shall be two years, and their term may be renewable for one further term. *<Amended by Act No. 13423, Jul. 24, 2015>*

(6) In order to conduct dispute settlement efficiently, the Dispute Mediation Committee may, if necessary, establish a mediation panel that is comprised of not more than five Committee members in each sector of mediation cases, as prescribed by Presidential Decree. In this case, the resolution of the mediation panel delegated by the Dispute Mediation Committee shall be construed as that of the Dispute Mediation Committee.

(7) The quorum for holding a Dispute Mediation Committee or a mediation panel shall be the presence of a majority of its members, and any resolution shall require the affirmative votes of a majority of the members present.

(8) The Protection Commission may deal with the administrative affairs necessary for dispute mediation, such as receiving dispute mediation cases and fact-finding. *<Amended by Act No. 13423, Jul. 24, 2015>*

(9) Except as otherwise expressly provided for in this Act, matters necessary to operate the Dispute Mediation Committee shall be prescribed by Presidential Decree.

Article 41 (Guarantee of Members' Status)

None of the Committee members shall be dismissed or de-commissioned against his or her will except when he or she is sentenced to the suspension of qualification or a heavier punishment, or unable to perform his or her duties due to mental or physical incompetence.

Article 42 (Exclusion, Recusal, and Refrainment of Members)

(1) A member of the Dispute Mediation Committee shall be excluded from participating in the deliberation and resolution of a case requested for dispute mediation pursuant to Article 43 (1) (hereafter in this Article referred to as "case") if:

1. The member or his/her current or former spouse is a party to the case or is a joint right holder or a joint obligator with respect to the case;
2. The member is or was a relative of a party to the case;
3. The member has given any testimony, expert opinion, or legal advice with respect to the case;
4. The member is or was involved in the case as an agent or representative of a party to the case.

(2) Where any party finds it impracticable to expect a fair deliberation and resolution from a Committee member, such party may file an application for recusal with the chairperson. In such cases, the chairperson shall determine with respect to such application for recusal without any resolution of the Dispute Mediation Committee.

(3) Where any committee member falls under the case of paragraph (1) or (2), he/she may refrain from the deliberation and resolution of the case.

Article 43 (Application for Mediation)

(1) Any person who wishes a dispute over personal information mediated may apply for mediation of the dispute to the Dispute Mediation Committee.

(2) Upon receipt of an application for dispute mediation from a party to the case, the Dispute Mediation Committee shall notify the counterparty of the application for mediation.

(3) Where a public institution is notified of dispute mediation under paragraph (2), the public institution shall respond to it unless there are extraordinary circumstances.

Article 44 (Time Limitation of Mediation Proceedings)

(1) The Dispute Mediation Committee shall examine the case and prepare a draft mediation decision within 60 days from the date of receiving an application pursuant to Article 43 (1): Provided, That the Dispute Mediation Committee may pass a resolution to extend such period by reason of inevitable circumstances.

(2) Where the period is extended pursuant to the proviso to paragraph (1), the Dispute Mediation Committee shall inform the applicant of the reasons for extending the period and other matters concerning the extension of such period.

Article 45 (Request for Materials)

(1) Upon receipt of an application for dispute mediation pursuant to Article 43 (1), the Dispute Mediation Committee may request disputing parties to provide materials necessary to mediate the dispute. In such cases, such parties shall comply with the request unless any justifiable ground exists.

(2) The Dispute Mediation Committee may require disputing parties or relevant witnesses to appear before the Committee to hear their opinions, if deemed necessary.

Article 46 (Settlement Advice before Mediation)

Upon receipt of an application for dispute mediation pursuant to Article 43 (1), the Dispute Mediation Committee may present a draft settlement to the disputing parties and recommend a settlement before mediation.

Article 47 (Dispute Mediation)

(1) The Dispute Mediation Committee may prepare a draft mediation decision including the following matters:

1. Suspension of the violation to be investigated;
2. Restitution, compensation and other necessary remedies;
3. Any measure necessary to prevent recurrence of the identical or similar violations.

(2) Upon preparing a draft mediation pursuant to paragraph (1), the Dispute Mediation Committee shall present the draft mediation to each party without delay.

(3) Each party presented with the draft mediation decision prepared under paragraph (1) shall notify the Dispute Mediation Committee of his/her acceptance or denial of the draft mediation decision within 15 days from the date of receipt of such draft mediation decision, without which such mediation shall be deemed rejected.

(4) If the parties accept the draft mediation decision, the Dispute Mediation Committee shall prepare a written mediation decision, and the chairperson of the Dispute Mediation Committee and the parties shall have their names and seals affixed thereon.

(5) The mediation agreed upon pursuant to paragraph (4) shall have the same effect as a settlement before the court.

Article 48 (Rejection and Suspension of Mediation)

(1) Where the Dispute Mediation Committee deems that it is inappropriate to mediate any dispute in view of its nature, or that an application for mediation of any dispute is filed for an unfair purpose, it may reject the mediation. In this case, the reasons for rejecting the mediation shall be notified to the applicant.

(2) If one of the parties files a lawsuit while mediation proceedings are pending, the Dispute Mediation Committee shall suspend the dispute mediation and notify the parties thereof.

Article 49 (Collective Dispute Mediation)

(1) The State, a local government, a data protection organization or institution, a data subject, and a personal information controller may request or apply for a collective dispute mediation (hereinafter referred to as "collective dispute mediation") to the Dispute Mediation Committee where damages or infringement on rights occur to multiple data subjects in an identical or similar manner, and such incident is such as prescribed by Presidential Decree.

(2) Upon receipt of a request or an application for collective dispute mediation under paragraph (1), the Dispute Mediation Committee may commence, by its resolution, collective dispute mediation proceedings pursuant to paragraphs (3) through (7). In such cases, the Dispute Mediation Committee shall publicly announce the commencement of such proceedings for a period prescribed by Presidential Decree.

(3) The Dispute Mediation Committee may accept an application from any data subject or personal information controller other than the parties to the collective dispute mediation to participate in the collective dispute mediation additionally as a party.

(4) The Dispute Mediation Committee may, by its resolution, select one or a few persons as a representative party, who most appropriately represents the common interest among the parties to the collective dispute mediation pursuant to paragraphs (1) and (3).

(5) When the personal information controller accepts a collective dispute mediation award presented by the Dispute Mediation Committee, the Dispute Mediation Committee may advise the personal information controller to prepare and submit a compensation plan for the benefit of the non-party data subjects suffered from the same incident.

(6) Notwithstanding Article 48 (2), if a group of data subjects among a multitude of data subject parties to the collective dispute mediation files a lawsuit before the court, the Dispute Mediation Committee shall not suspend the proceedings but exclude the relevant data subjects, who have filed the lawsuit, from the proceedings.

(7) The period for collective dispute mediation shall not exceed 60 days from the following day when public announcement referred to in paragraph (2) ends: Provided, That the period can be extended by the resolution of the Dispute Mediation Committee in extenuating circumstances.

(8) Other necessary matters, such as the procedures for collective dispute mediation, shall be prescribed by Presidential Decree.

Article 50 (Mediation Procedures)

(1) Except as otherwise expressly provided for in Articles 43 through 49, the method and procedures to mediate disputes and matters necessary to deal with such dispute mediation shall be prescribed by Presidential Decree.

(2) Except as otherwise expressly provided for in this Act, the Judicial Conciliation of Civil Disputes Act shall apply mutatis mutandis to the operation of the Dispute Mediation Committee and dispute mediation proceedings.

Article 51 (Parties to Class Action Lawsuit)

Any of the following organizations may file a lawsuit (hereinafter referred to as "class action lawsuit") with the court to prevent or suspend an infringement with respect to personal information if a personal information controller rejects or would not accept the collective dispute mediation under Article 49:

1. A consumer group registered with the Fair Trade Commission pursuant to Article 29 of the Framework Act on Consumers that meets all of the following criteria:

(a) Its by-laws shall constantly state the purpose to augment the rights and interests of data subjects;

(b) The number of full members shall exceed 1000;

(c) Three years shall have passed since the registration under Article 29 of the Framework Act on Consumers;

2. A non-profit, non-governmental organization referred to in Article 2 of the Assistance for Non-Profit, Non-Governmental Organizations Act that meets all of the following criteria:

(a) At least 100 data subjects, who experienced the same infringement as a matter of law or fact, shall submit a request to file a class action lawsuit;

(b) Its by-laws shall state the purpose of data protection and it has conducted such activities for the most recent 3 years;

(c) The number of regular members shall be at least 5000;

(d) It shall be registered with any central administrative agency.

Article 52 (Exclusive Jurisdictions)

(1) A class action lawsuit shall be subject to the exclusive jurisdiction of the competent district court (panel of judges) at the place of business or main office, or at the address of the business manager in the case of no business establishment, of the defendant.

(2) Where paragraph (1) applies to a foreign business entity, the same shall be determined by the place of business or main office, or the address of the business manager located in the Republic of Korea.

Article 53 (Retention of Litigation Attorney)

The plaintiff of a class-action lawsuit shall retain an attorney-at-law as a litigation attorney.

Article 54 (Application for Permission of Lawsuit)

(1) An organization that intends to file a class action shall submit to the court an application for permission of lawsuit describing the following in addition to the complaint:

1. Plaintiff and his or her litigation attorney;

2. Defendant;

3. Detailed violation of the rights of data subjects.

(2) An application for certification of lawsuit filed under paragraph (1) shall be accompanied by the following materials:

1. Materials that prove that the organization which has filed a lawsuit meets all criteria provided for in Article 51;

2. Documentary evidence that proves that the personal information controller has rejected the dispute mediation or would not accept the mediation award.

Article 55 (Requirements for Permission of Lawsuit)

(1) The court shall permit a class action only when all of the following requirements are satisfied:

1. That the personal information controller has rejected the dispute mediation or would not accept the mediation award;

2. That none of the descriptions in the application for permission of lawsuit filed under Article 54 is defective.

(2) The court decision that permits, or refuses to permit, a class action may be challenged through immediate appeal.

Article 56 (Effect of Conclusive Judgment)

When a judgment dismissing a plaintiff's complaint becomes conclusive, any other organizations provided for in Article 51 cannot file a class-action lawsuit regarding the identical case: Provided, That this shall not apply in any of the following circumstances:

1. Where, after the judgment became conclusive, new evidence has been found by the State, a local government, or a State or local government-invested institution regarding the said case;

2. Where the judgment dismissing the lawsuit proves to have been caused intentionally by the plaintiff.

Article 57 (Application of Civil Procedure Act)

(1) Except as otherwise expressly provided for in this Act, the Civil Procedure Act shall apply to a class action.

(2) When a decision to permit a class action lawsuit is made under Article 55, a preservation order provided for in PART IV of the Civil Execution Act may be issued.

(3) Matters necessary for class action lawsuit proceedings shall be provided by the Supreme Court Regulations.

Article 58 (Partial Exclusion of Application)

(1) Chapter III through VII shall not apply to any of the following personal information:

1. Personal information collected pursuant to the Statistics Act for processing by public institutions;

2. Personal information collected or requested to be provided for the analysis of information related to national security;

3. Personal information processed temporarily where it is urgently necessary for the public safety and security, public health, etc.;

4. Personal information collected or used for its own purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties, respectively.

(2) Articles 15, 22, 27 (1) and (2), 34, and 37 shall not apply to any personal information that is processed by means of the visual data processing devices installed and operated at open places pursuant to Article 25 (1).

(3) Articles 15, 30 and 31 shall not apply to any personal information that is processed by a personal information controller to operate a group or association for friendship, such as an alumni association and a hobby club.

(4) In the case of processing personal information pursuant to paragraph (1), a personal information controller shall process the personal information to the minimum extent necessary to attain the intended purpose for the minimum period; and shall also make necessary arrangements, such as technical, managerial and physical safeguards, individual grievance handling and other necessary measures for the safe management and appropriate processing of such personal information.

Article 58-2 (Exemption from Application)

This Act shall not apply to information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc.

Article 59 (Prohibited Activities)

Anyone who processes or has processed personal information shall be prohibited from undertaking any of the following activities:

1. To acquire personal information or to obtain consent to personal information processing by fraud, improper or unjust means;
2. To divulge personal information acquired in the course of business, or to provide it for any third party's use without authority;
3. To damage, destroy, alter, forge, or divulge other's personal information without legal authority or beyond proper authority.

Article 60 (Confidentiality)

Any person who performs or has performed the following affairs shall not divulge any confidential information acquired in the course of performing his or her duties to any other person, nor use such information for any purpose other than for his or her duties: Provided, That, the same shall not apply where special provisions exist in other laws: *<Amended by Act No. 16930, Feb. 4, 2020>*

1. Affairs of the Protection Commission provided for in Article 8;

1-2. Certification of personal information protection provided for in Article 32-2;

2. Impact assessments provided for in Article 33;
3. Dispute mediation of the Dispute Mediation Committee establish11ed under Article 40.

Article 61 (Suggestions and Recommendations for Improvements)

(1) The Protection Commission may provide its opinion to any relevant agency through deliberation and resolution where it is deemed necessary with respect to the statutes or municipal ordinances containing

provisions that are likely to affect the protection of personal information. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, February. 4, 2020>*

(2) The Protection Commission may advise a personal information controller to improve the status of personal information processing where doing so is deemed necessary to protect personal information. In such cases, upon receiving the advice, the personal information controller shall make sincere efforts to comply with the advice, and shall inform the Protection Commission of the results. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(3) The head of a related central administrative agency may recommend that a personal information controller improve the status of personal information processing pursuant to the statutes under the related central administrative agency's jurisdiction where doing so is deemed necessary to protect personal information. In such cases, upon receiving the recommendation, the personal information controller shall make sincere efforts to comply with the recommendation, and shall inform the head of the related central administrative agency of the results.

(4) Central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission may provide their opinions, or provide guidance or inspection with respect to the protection of personal information to their affiliated entities and the public institutions under their jurisdiction.

Article 62 (Reporting on Infringements)

(1) Anyone who suffers infringement of rights or interests relating to his or her personal information in the course of personal information processing by a personal information controller may report such infringement to the Protection Commission. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(2) The Protection Commission may designate a specialized institution in order to efficiently receive and handle the claim reports pursuant to paragraph (1), as prescribed by Presidential Decree. In such cases, such specialized institution shall establish and operate a personal information infringement call centre (hereinafter referred to as the "Privacy Call Center"). *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(3) The Privacy Call Center shall perform the following duties:

1. To receive claim reports and provide consultation in relation to personal information processing;
2. To investigate and confirm incidents and hear opinions of related parties;
3. Duties incidental to subparagraphs 1 and 2.

(4) The Protection Commission may, if necessary, dispatch its public official to the specialized institution designated under paragraph (2) pursuant to Article 32-4 of the State Public Officials Act in order to efficiently investigate and confirm the incidents pursuant to paragraph (3) 2. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

Article 63 (Requests for Materials and Inspections)

(1) The Protection Commission may request relevant materials, such as articles and documents, from a personal information controller in any of the following cases: *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

1. Where any violation of this Act is found or suspected;
2. Where any violation of this Act is reported or a civil complaint thereon is received;
3. In cases prescribed by Presidential Decree where it is necessary to protect the personal information of data subjects.

(2) Where a personal information controller fails to furnish materials pursuant to paragraph (1) or is regarded as having violated this Act, the Protection Commission may require its public official to enter the offices or places of business of the personal information controller and other persons related to such violation to inspect the status of business operations, ledgers, documents, etc. In such cases, the public official who conducts the inspection shall carry a certificate indicating his/her authority and show it to the related persons. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(3) The head of a related central administrative agency may, in accordance with statutes under the related central administrative agency's jurisdiction, request materials from a personal information controller pursuant to paragraph (1), or may inspect the personal information controller and other persons related to the relevant violation of such statutes pursuant to paragraph (2). *<Amended by Act No. 13423, Jul. 24, 2015>*

(4) Upon discovering any violation of this Act or becoming aware of any suspected violation of this Act, the Protection Commission may demand that the head of the related central administrative agency (if there is a corporation authorized to conduct inspection in accordance with the direction and supervision of the head of the related central administrative agency, this refers to the corporation) investigate the personal information controller after setting a specific scope, and if necessary, request a public official under the Protection Commission to jointly engage in the investigation. In such cases, upon receiving such demand, the head of the related central administrative agency shall comply therewith unless there are extraordinary circumstances. *<Amended by Act No. 16930, Feb. 4, 2020>*

(5) The Protection Commission may request the head of the related central administrative agency (if there is a corporation authorized to conduct inspection in accordance with the direction and supervision of the head of the related central administrative agency, this refers to the corporation) to take corrective measures on the relevant personal information processer with regard to the result of the inspection conducted pursuant to paragraph (4) or provide opinions on dispositions, etc. *<Amended by Act No. 16930, Feb. 4, 2020>*

(6) Matters concerning the methods, procedures, etc. for paragraphs (4) and (5) shall be prescribed by Presidential Decree. *<Amended by Act No. 16930, Feb. 4, 2020>*

(7) The Protection Commission may inspect the status of personal information protection jointly with the head of a related central administrative agency for the prevention of personal information breach incidents and efficient response. *<Newly Inserted by Act No. 13423, Jul. 24, 2015; Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(8) The Protection Commission and the head of the related central administrative agency shall not provide any third party with the documents, materials, etc. furnished or collected pursuant to paragraphs (1) and (2), nor disclose them to the general public, except as otherwise required by this Act. *<Newly Inserted by Act No. 16930, Feb. 4, 2020>*

(9) Where receiving materials via information and communications networks, or digitalizing the collected materials, etc., the Protection Commission and the head of the related central administrative agency shall take systematic and technical security measures to prevent the breach of personal information, trade secrets, etc. *<Newly Inserted by Act No. 16930, Feb. 4, 2020>*

Article 64 (Corrective Measures)

(1) Where the Protection Commission deems that there is substantial ground to deem that there has been infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy, it may order the violator of this Act (excluding central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) to take any of the following measures: *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

1. To suspend infringement with respect to personal information;
2. To temporarily suspend personal information processing;
3. Other measures necessary to protect personal information and to prevent personal information infringement.

(2) Where the head of a related central administrative agency deems that there is substantial ground to deem that there has been an infringement of personal information, and failure to take action is likely to cause damage that is difficult to remedy, he or she may order a personal information controller to take any of the measures provided for in paragraph (1) pursuant to the statutes under such related central administrative agency's jurisdiction.

(3) A local government, the National Assembly, the Court, the Constitutional Court, or the National Election Commission may order their affiliated entities and public institutions, which are found to have violated this Act, to take any of the measures provided for in paragraph (1).

(4) When a central administrative agency, a local government, the National Assembly, the Court, the Constitutional Court, or the National Election Commission violates this Act, the Protection Commission may recommend the head of the relevant agency to take any of the measures provided for in paragraph (1). In such cases, upon receiving the recommendation, the agency shall comply therewith unless there are extraordinary circumstances.

Article 65 (Accusation and Recommendation for Disciplinary Action)

(1) When there is deemed substantial ground for suspecting a criminal violation of this Act or other data protection-related statutes, the Protection Commission may make an accusation to the competent investigative agency. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(2) When there is deemed substantial ground for deeming that there has been a violation of this Act or other data protection-related statutes, the Protection Commission may recommend the relevant personal information controller to take disciplinary action against the person responsible for such violation (including the representative and the executive officer in charge). In such cases, upon receiving the recommendation, the relevant personal information controller shall comply therewith, and notify the Protection Commission of the results. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 11990, Aug. 6, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(3) The head of a related central administrative agency may file a criminal complaint against a personal information controller pursuant to paragraph (1), or recommend that the head of an affiliated agency, organization, etc. take disciplinary action pursuant to paragraph (2), in accordance with the statutes under the central administrative agency's jurisdiction. In such cases, upon receiving the recommendation under paragraph (2), the head of an affiliated agency, organization, etc. shall comply therewith, and notify the head of the related central administrative agency of the results.

Article 66 (Disclosure of Results)

(1) The Protection Commission may disclose the recommendation for improvement pursuant to Article 61; the order to take corrective measures pursuant to Article 64; the accusation or recommendation to take disciplinary action pursuant to Article 65; and the imposition of administrative fines pursuant to Article 75 and the results thereof. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(2) The head of a related central administrative agency may disclose the matters provided for in paragraph (1) in accordance with the statutes under the central administrative agency's jurisdiction.

(3) The method, criteria, procedure, etc. for disclosure pursuant to paragraphs (1) and (2) shall be prescribed by Presidential Decree.

Article 67 (Annual Reports)

(1) The Protection Commission shall prepare a report each year, based on necessary materials furnished by related agencies, etc., in relation to the establishment and implementation of personal information protection policy measures, and submit (including transmission via an information and communications networks) it to the National Assembly before the opening of the regular session.

(2) The annual report referred to in paragraph (1) shall contain the following matters: *<Amended by Act No. 14107, Mar. 29, 2016>*

1. Infringement on the rights of data subjects and the status of remedies thereof;
2. Results of the survey in relation to the status of personal information processing;
3. Status of implementation of the personal information protection policy measures and achievements;
4. Global legislative and policy trends regarding personal information;
5. Status of the enactment and amendment of Acts, Presidential Decrees, the National Assembly Regulations, the Supreme Court Regulations, the Constitutional Court Regulations, the National Election Commission Regulations, and the Board of Audit and Inspection Regulations, in relation to

processing of resident registration numbers;

6. Other matters to be disclosed or reported in relation to the personal information protection policy.

Article 68 (Delegation and Entrustment of Authority)

(1) The authority of the Protection Commission or the head of a related central administrative agency under this Act may in part be delegated or entrusted, as prescribed by Presidential Decree, to the Special Metropolitan City Mayor, Metropolitan City Mayors, Do Governors, Special Self-Governing Province Governors, or the specialized institutions prescribed by Presidential Decree. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, February. 4, 2020>*

(2) The agencies to which the authority of the Protection Commission or the head of a related central administrative agency has been partially delegated or entrusted pursuant to paragraph (1) shall notify the Protection Commission or the head of the related central administrative agency of the results of performing the affairs delegated or entrusted. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

(3) Where delegating or entrusting a part of the authority to a specialized institution pursuant to paragraph (1), the Protection Commission may provide a contribution to the special institution to cover expenses incurred in performing the affairs. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

Article 69 (Persons Deemed to be Public Officials for Purposes of Penalty Provisions)

(1) Among the Commissioners of the Protection Commission, Commissioners other than public officials and employees other than public officials shall be deemed a public official for the purposes of applying penalty under the Criminal Act or other statutes. *<Newly Inserted by Act No. 16930, Feb. 4, 2020>*

(2) Any executive or employee of a relevant agency that performs the affairs entrusted by the Protection Commission or the head of a related central administrative agency shall be deemed a public official for the purposes of Articles 129 through 132 of the Criminal Act. *<Newly Inserted by Act No. 16930, Feb. 4, 2020>*

Article 70 (Penalty Provisions)

Any of the following persons shall be punished by imprisonment with labor for not more than 10 years, or by a fine not exceeding 100 million won: *<Amended by Act No. 13423, Jul. 24, 2015>*

1. A person who causes the suspension, paralysis or other severe hardship of work of a public institution by altering or erasing the personal information processed by the public institution for the purpose of disturbing the personal information processing of such public institution;

2. A person who obtains any personal information processed by third parties by fraud or other unjust means or methods and provides it to a third party for a profit-making or unjust purpose, and a person who abets or arranges such conduct.

Article 71 (Penalty Provisions)

Any of the following persons shall be punished by imprisonment with labour for not more than 5 years, or by a fine not exceeding 50 million won: *<Amended by Act No. 14107, Mar. 29, 2016; Act No. 16930, Feb. 4, 2020>*

1. A person who provides personal information to a third party without the consent of a data subject in violation of Article 17 (1) 1 even through Article 17 (1) 2 is not applicable, and a person who knowingly receives such personal information;

2. A person who uses personal information or provides personal information to a third party in violation of Articles 18 (1) and (2) (including where the aforesaid provisions apply mutatis mutandis pursuant to Article 39-14), 19, 26 (5), 27 (3), or 28-2 and a person who knowingly receives such personal information for a profit-making or unfair purpose;

3. A person who processes sensitive information in violation of Article 23 (1);

4. A person who processes personally identifiable information in violation of Article 24 (1);

4-2. A person who processes or provides a third party with pseudonymised information in violation of Article 28-3, and a person who knowingly receives such pseudonymised information for profit-making or unfair purposes;

4-3. A person who processes pseudonymised information for the purpose of identifying a certain individual in violation of Article 28-5 (1);

4-4. An information and communications service provider who uses or provides a third party with personal information without taking necessary measures for correction or deletion requests (including necessary measures to be taken in accordance with a request for access, etc. provided for in Article 38 (2)) pursuant to Article 36 (2) (including a person to whom personal information has been transferred from information and communications service provider, etc. pursuant to Article 27 and applicable cases pursuant to Article 39-14);

4-5. A person who collects personal information without users' consent in violation of Article 39-3 (1) (including where the aforesaid provisions apply mutatis mutandis pursuant to Article 39-14);

4-6. A person who collects the personal information of children aged under 14 without his or her legal representative's consent or without confirming whether the legal representative has given consent or not in violation of Article 39-3 (4) (including applicable cases pursuant to Article 39-14);

5. A person who divulges personal information acquired in the course of business or provides it for any other person's use without authority in violation of subparagraph 2 of Article 59, and a person who knowingly receives such personal information for a profit-making or unfair purposes;

6. A person who damages, destroys, alters, forges, or divulges any third party's personal information in violation of subparagraph 3 of Article 59.

Article 72 (Penalty Provisions)

Any of the following persons shall be punished by imprisonment with labor for not more than 3 years, or by a fine not exceeding 30 million won:

1. A person who arbitrarily handles visual data processing devices for any purpose other than the purpose for which the device was installed, directs such devices toward different spots, or uses a sound recording function in violation of Article 25 (5);

2. A person who acquires personal information or obtains consent to personal information processing by fraud or other unjust means in violation of subparagraph 1 of Article 59, and a person who knowingly receives such personal information for a profit-making or unfair purpose;

3. A person who divulges confidential information acquired while performing his or her duties, or uses such information for purposes other than for the purpose of discharging his/her duties in violation of Article 60.

Article 73 (Penalty Provisions)

Any of the following persons shall be punished by imprisonment with labor for not more than 2 years, or by a fine not exceeding 20 million won: *<Amended by Act No. 13423, Jul. 24, 2015; Act No. 14107, Mar. 29, 2016; Act No. 16930, Feb. 4, 2020>*

1. A person who fails to take necessary measures to ensure safety in violation of Article 23 (2), 24 (3), 25 (6), 28-4 (1), or 29 and causes personal information to be lost, stolen, divulged, forged, altered, or damaged;

1-2. Information and communications service provider, etc. who fails to destroy personal information in violation of Article 21 (1) (including applicable cases pursuant to Article 39-14);

2. A person who fails to take necessary measures to rectify or erase personal information in violation of Article 36 (2), and continuously uses, or provides a third party with, the personal information;

3. A person who fails to suspend processing of personal information in violation of Article 37 (2), and continuously uses, or provides a third party with, the personal information.

Article 74 (Joint Penalty Provisions)

(1) If the representative of a corporation, or an agent or employee of, or any other person employed by, a corporation or an individual commits any of the offenses provided for in Article 70 in connection with the business affairs of the corporation or individual, not only shall such offender be punished, but also the corporation or individual shall be punished by a fine not exceeding 70 million won: Provided, That the same shall not apply where such corporation or individual has not been negligent in taking due care and supervisory activities concerning the relevant business affairs to prevent such offense.

(2) If the representative of a corporation, or an agent or employee of, or any other person employed by, a corporation or an individual commits any of the offenses provided for in Articles 71 through 73 in connection with the business affairs of the corporation or individual, not only shall such offender be punished, but also the corporation or individual shall be punished by a fine prescribed in the relevant Article: Provided, That the same shall not apply where such corporation or individual has not been negligent in taking due care and supervisory activities concerning the relevant business affairs to prevent such offense.

Article 74-2 (Confiscation and Collection)

Any money or goods or other profits acquired by a person who has violated Articles 70 through 73 in relation to such violation may be confiscated, or, if confiscation is impossible, the value thereof may be collected. In such cases, such confiscation or collection may be levied in addition to other penalty

provisions.

Article 75 (Administrative Fines)

(1) Any of the following persons shall be subject to an administrative fine not exceeding 50 million won: *<Amended by Act No. 14765, Apr. 18, 2017>*

1. A person who collects personal information in violation of Article 15 (1);
2. A person who fails to obtain the consent of a legal representative in violation of Article 22 (6);
3. A person who installs and operates visual data processing devices in violation of Article 25 (2).

(2) Any of the following persons shall be subject to an administrative fine not exceeding 30 million won: *<Amended by Act No. 11990, Aug. 6, 2013; Act No. 12504, Mar. 24, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14107, Mar. 29, 2016; Act No. 14765, Apr. 18, 2017; Act No. 16930, Feb. 4, 2020>*

1. A person who fails to notify a data subject of necessary information in violation of Article 15 (2), 17 (2), 18 (3), or 26 (3);
2. A person who denies the provision of goods or services to a data subject in violation of Article 16 (3) or 22 (5);
3. A person who fails to notify a data subject of the matters provided for in Article 20 (1) or (2) in violation of Article 20 (1) or (2);
4. A person who fails to take necessary measures, such as destroying personal information, in violation of Article 21 (1) or Article 39-6 (including applicable cases pursuant to Article 39-14);

4-2. A person who processes resident registration numbers in violation of Article 24-2 (1);

4-3. A person who fails to adopt encryption measures in violation of Article 24-2 (2);

5. A person who fails to provide a data subject with an alternative method without using his or her resident registration number in violation of Article 24-2 (3);
6. A person who fails to take measures necessary to ensure safety in violation of Article 23 (2), 24 (3), 25 (6), 28-4 (1), or 29;
7. A person who installs and operates visual data processing devices in violation of Article 25 (1);

7-2. A person who fails to cease the use of, collect or destroy, information which has been generated to identify a certain individual, in violation of Article 28-5 (2);

7-3. A person who indicates and promotes the certification by fraud despite a failure to obtain such certification, in violation of Article 32-2 (6);

8. A person who fails to notify a data subject of the facts provided for in Article 34 (1) in violation of same paragraph;
9. A person who fails to report the results of measures taken, in violation of Article 34 (3);
10. A person who limits or denies access to personal information in violation of Article 35 (3);
11. A person who fails to take necessary measures to correct or erase personal information, in violation of Article 36 (2);
12. A person who fails to take necessary measures, such as destruction of the personal information whose processing has been suspended, in violation of Article 37 (4);

12-2. A person who refuses to provide services in violation of Article 39-3 (3) (including applicable cases pursuant to Article 39-14);

12-3. A person who fails to notify or report the relevant users, the Protection Commission or a specialized institution or notifies or reports after the lapse of 24 hours without any just cause, in violation of Article 39-4 (1) (including applicable cases pursuant to Article 39-14);

12-4. A person who fails to explain or falsely explains just cause, in violation of Article 39-4 (3);

12-5. A person who fails to provide methods of withdrawing consent, and accessing to, or correcting, personal information, in violation of Article 39-7 (2) (including applicable cases pursuant to Article 39-14);

12-6. Information and communications service provider, etc. who fails to take necessary measures in violation of Article 39-7 (3) (including applicable cases pursuant to Article 39-14 and any person to whom personal information has been transferred from information and communications service provider, etc. pursuant to Article 27);

12-7. A person who fails to notify users of the use history of their personal information in violation of the main clause of Article 39-8 (1) (including applicable cases pursuant to Article 39-14);

12-8. A person who fails to take protective measures, in violation of Article 39-12 (4) (including applicable cases pursuant to paragraph (5) of the same Article);

13. A person who fails to comply with corrective orders taken under Article 64 (1).

(3) Any of the following persons shall be subject to an administrative fine not exceeding 20 million won: *<Newly Inserted by Act No. 16930, Feb. 4, 2020>*

1. A person who fails to take necessary measures such as purchasing an insurance, joining a mutual aid organization, or accumulating reserves, in violation of Article 39-9 (1);

2. A person who fails to designate a domestic agent, in violation of Article 39-11 (1);

3. A person who outsources the processing of, or stores, users' personal information overseas without disclosing or informing all matters provided for in Article 39-12 (3) or notifying users in violation of the proviso of Article 39-12 (2).

(4) Any of the following persons shall be subject to an administrative fine not exceeding 10 million won: *<Amended by Act No. 14765, Apr. 18, 2017; Act No. 16930, Feb. 4, 2020>*

1. A person who fails to store and manage personal information separately in violation of Article 21 (3);

2. A person who obtains consent in violation of Article 22 (1) through (4);

3. A person who fails to take necessary measures including posting a signboard in violation of Article 25 (4);

4. A person who fails to execute a document stating the matters provided for in Article 26 (1) when outsourcing the work in violation of the same paragraph;

5. A person who fails to disclose the outsourced work and the outsourcee in violation of Article 26 (2);

6. A person who fails to notify a data subject of the transfer of his or her personal information in violation of Article 27 (1) or (2);

6-2. A person who fails to prepare and keep a record of relevant matters in violation of Article 28-4 (2);

7. A person who fails to establish, or disclose, the Privacy Policy in violation of Article 30 (1) or (2);

8. A person who fails to designate a privacy officer in violation of Article 31 (1);

9. A person who fails to notify a data subject of necessary information in violation of Article 35 (3) and (4), 36 (2) and (4), or 37 (3);

10. A person who fails to furnish materials, such as articles and documents pursuant to Article 63 (1), or who submits false materials;

11. A person who refuses, interferes with, or evades access or an inspection pursuant to Article 63 (2).

(5) Administrative fines provided for in paragraphs (1) through (4) shall be imposed and collected by the Protection Commission and the head of a related central administrative agency, as prescribed by Presidential Decree. In such cases, the head of a related central administrative agency shall impose and collect administrative fines from the personal information controllers in the field under his or her jurisdiction. *<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>*

Article 76 (Special Exemption to Application of Provisions on Administrative Fines)

For the purposes of the provisions on administrative fines provided for in Article 75, no additional administrative fine shall be imposed on any act subject to penalty surcharges pursuant to Article 34-2.

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force six months after the date of its promulgation: Provided, That Articles 24 (2) and 75 (2) 5 shall enter into force one year after the date of its promulgation.

Article 2 (Repeal of other Acts)

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

Article 3 (Transitional Measures concerning Personal Information Dispute Mediation Committee)

An act performed by or against the Personal Information Dispute Mediation Committee under the previous Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. as at the time this Act enters into force shall be deemed an act performed by or against the Personal Information Dispute Mediation Committee corresponding thereto under this Act.

Article 4 (Transitional Measures concerning Personal Information being Processed)

Any personal information legitimately processed under other Acts before this Act enters into force shall be deemed to have been processed under this Act.

Article 5 (Transitional Measures concerning Application of Penalty Provisions)

(1) The application of the penalty provisions to a violation of the previous Act on the Protection of Personal Information Maintained by Public Institutions before this Act enters into force shall be governed by the previous Act on the Protection of Personal Information Maintained by Public Institutions.

(2) The application of the penalty provisions to a violation of the previous Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. before this Act enters into force shall be governed by the previous Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

Article 6 Omitted.

Article 7 (Relationship to other Acts)

Where the previous Act on the Protection of Personal Information Maintained by Public Institutions or the provisions thereof are cited in other statutes at the time this Act enters into force, and any provision corresponding thereto exists in this Act, this Act or the corresponding provision of this Act shall be deemed cited in lieu of the previous provision.

ADDENDA *<Act No. 11690, Mar. 23, 2013>*

Article 1 (Enforcement Date)

(1) This Act shall enter into force on the date of its promulgation.

(2) Omitted.

Articles 2 through 7 Omitted.

ADDENDA *<Act No. 11990, Aug. 6, 2013>*

Article 1 (Enforcement Date)

This Act shall enter into force one year after the date of its promulgation.

Article 2 (Transitional Measures concerning Limitation to Processing of Resident Registration Numbers)

(1) A person who processes resident registration numbers as at the time this Act enters into force shall destroy the resident registration numbers possessed, within two years after this Act enters into force: Provided, That any of the cases falling under the amended subparagraphs of Article 24-2 (1) shall be excluded from the destruction.

(2) Where resident registration numbers are not destroyed within the period referred to in paragraph (1), the amended provisions of Article 24-2 (1) shall be deemed to have been violated.

ADDENDUM *<Act No. 12504, Mar. 24, 2014>*

This Act shall enter into force on the date of its promulgation: Provided, That the amended provisions of Articles 24-2 and 75 (2) 5 of the Personal Information Protection Act (Act No. 11990) shall enter into force on January 1, 2016.

ADDENDA *<Act No. 12844, Nov. 19, 2014>*

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation. (Proviso Omitted.)

Articles 2 through 7 Omitted.

ADDENDA *<Act No. 13423, Jul. 24, 2015>*

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation: Provided, That the amended provisions of Articles 8 (1), 8-2, 9, 11 (1), 32-2, 39 (3) and (4), 39-2, 40, and 75 (2) 7-2 shall enter into force one year after the date of its promulgation, and the amended provisions of the former part of Article 24-2 (2) and Article 75 (2) 4-3 of the Personal Information Protection Act (Act No. 12504) shall enter into force on January 1, 2016, respectively.

Article 2 (Applicability to Compensation)

The amended provisions of Articles 39 (3) and (4) and 39-2 shall apply, beginning with the first claim for compensation for personal information suffering loss, theft, divulgence, forgery, alteration, or damage after this Act enters into force.

Article 3 (Transitional Measures concerning Personal Information Protection Certification)

Any person who has obtained the personal information protection certification from the Minister of the Interior before this Act enters into force shall be deemed obtained the personal information protection certification under the amended provisions of Article 32-2.

Article 4 (Transitional Measures concerning Qualifications for Certification Examiners of Personal Information Protection)

Any person qualified as a certification examiner of personal information protection before this Act enters into force shall be deemed qualified under this Act.

Article 5 (Transitional Measures concerning Terms of Office of Members of Personal Information Dispute Mediation Committee)

Members of the Dispute Mediation Committee appointed or commissioned by the Minister of the Interior before this Act enters into force shall be deemed members of the Dispute Mediation Committee commissioned by the Protection Commission under the amended provisions of Article 40.

Article 6 (Transitional Measures concerning Penalty Provisions, etc.)

The former provisions shall apply to the application of penalty provisions or imposition of administrative fines for offenses committed before this Act enters into force.

ADDENDA *<Act No. 14107, Mar. 29, 2016>*

Article 1 (Enforcement Date)

This Act shall enter into force six months after the date of its promulgation: Provided, That the amended provisions of Articles 24-2 (1) 1 and 67 (2) 5 shall enter into force one year after the date of its promulgation.

Article 2 (Applicability to Notification of Other Sources, etc. of Personal Information than Data Subjects)

The amended provisions of Article 20 (2) and (3) shall apply, beginning with the first case where any personal information is collected from a person other than the data subjects after this Act enters into force.

Article 3 (Transitional Measures concerning Privacy Policy)

(1) The Privacy Policy established under the former provisions as at the time this Act enters into force shall be deemed the Privacy Policy established under the amended provisions of Article 30 (1).

(2) Each personal information controller shall amend the Privacy Policy referred to in paragraph (1) to meet the purport of amending Article 30 (1) within six months after this Act enters into force.

ADDENDUM *<Act No. 14765, Apr. 18, 2017>*

This Act shall enter into force six months after the date of its promulgation.

ADDENDA *<Act No. 14839, Jul. 26, 2017>*

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation: Provided, That any amendment to the Acts made pursuant to Article 5 of this Addenda, promulgated before this Act enters into force, which have not yet entered into force, shall enter into force on the date the corresponding Act takes effect.

Articles 2 through 6 Omitted.

ADDENDA *<Act No. 16930, Feb. 4, 2020>*

Article 1 (Enforcement Date)

This Act shall enter into force six months after the date of its promulgation.

Article 2 (Transitional Measures concerning Terms of Office of Commissioners)

The term of office of the Commissioners of the Protection Commission appointed under the previous provisions as at the time this Act enters into force, shall be deemed expired on the date preceding the enforcement date of this Act.

Article 3 (Transitional Measures concerning Duties Following Adjustment of Functions)

(1) Among the duties of the Korea Communications Commission under Article 11 (1) of the Act on the Establishment and Operation of Korea Communications Commission as at the time this Act enters into force, those relating to personal information protection shall be transferred to the Protection Commission.

(2) Among the duties of the Minister of the Interior and Safety as at the time this Act enters into force, those pursuant to the amended provisions in Article 7-8 shall be assumed by the Protection Commission.

(3) Among the notifications, administrative dispositions and other acts of the Minister of the Interior and Safety, and acts conducted with respect to the Minister of the Interior and Safety such as filing of an application or report before this Act enters into force, those relating to matters for which competent authority is transferred from the Minister of the Interior and Safety to the Protection Commission shall be deemed to be the acts of, or acts conducted with respect to, the Protection Commission.

(4) Among the notifications, administrative dispositions and other acts of the Korea Communications Commission, and acts conducted with respect to the Korea Communications Commission such as filing of a report before this Act enters into force, those relating to matters for which competent authority is transferred from the Korea Communications Commission to the Protection Commission shall be deemed to be the acts of, or acts conducted with respect to, the Protection Commission pursuant to this Act.

(5) Among the public officials of the Ministry of the Interior and Safety or the Korea Communications Commission as at the time this Act enters into force, those prescribed by Presidential Decree shall be deemed to be the public officials of the Protection Commission pursuant to this Act.

Article 4 (Transitional Measures concerning the Protection Commission)

(1) The acts of, or acts conducted with respect to, the Protection Commission pursuant to the previous provisions as at the time this Act enters into force shall be deemed to be the acts of, or acts conducted with respect to, the Protection Commission pursuant to this Act.

Article 5 (Transitional Measures concerning Certifying Organizations for Personal Information Protection Management System)

(1) Entities designated as a certifying or examining organization pursuant to Article 47-3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. (hereinafter referred to as the “Network Act”) as at the time this Act enters into force, shall be deemed to have been designated as a specialized organization in accordance with Article 32-2 of this Act.

(2) Entities certified for personal information protection management system or qualified as a certification examiner pursuant to Article 47-3 of the Network Act as of the effective date of this Act shall be deemed to have been certified for personal information protection management system or qualified as a certification examiner pursuant to Article 32-2 of this Act.

Article 6 (Transitional Measures concerning Delegation or Entrustment of Authority)

The Special Metropolitan City Mayor, a Metropolitan City Mayor, a Do Governor, the Special Self-Governing Province Governor, the Special Self-Governing City Mayor or specialized institutions who have been delegated or entrusted with part of the authority of the Minister of the Interior and Safety pursuant to the previous provisions as of the effective date of this Act shall be deemed to have been delegated or entrusted with part of the authority of the Protection Commission pursuant to this Act.

Article 7 (Transitional Measures concerning Penalty Provisions and Administrative Fines)

Application of penalty and administrative fines on acts that were committed before this Act enters into force shall be governed by the previous provisions.

Article 8 (Transitional Measures concerning Imposition of Administrative Surcharges)

Imposition of administrative surcharges on acts that were committed before this Act enters into force shall be governed by the previous provisions.

Article 9 Omitted.

Article 10 (Relationship to Other Statutes)

(1) When other statutes (including statutes that were promulgated before this Act enters into force but the enforcement date of which has not arrived yet) state the “Korea Communications Commission” or “Chairperson of the Korea Communications Commission” in relation to the work of the Korea Communications Commission and the Ministry of the Interior and Safety that is transferred to the Protection Commission according to this Act as at the time this Act enters into force, such terms are regarded as the “Protection Commission” or “Chairperson of the Protection Commission” as applicable; “public officials of the Korea Communications Commission” as “public officials of the Protection Commission;” “Ministry of the Interior and Safety” or “Minister of the Interior and Safety” as “Protection Commission” or “Chairperson of the Protection Commission” as applicable; and “public officials of the Ministry of the Interior and Safety” as “public officials of the Protection Commission”.

(2) If other statutes quote the previous Network Act or provisions therein as at the time this Act enters into force, and if there is any corresponding provision in this Act, such statutes or the provisions therein are regarded as this Act or provisions of this Act.

Last updated : 2021-03-31