PERSONAL INFORMATION PROTECTION ACT

[Enforcement Date 15. Sep, 2023.] [Act No.19234, 14. Mar, 2023., Partial Amendment]

개인정보보호위원회 (심사총괄담당관 - 일반 법령해석)02-2100-3043

PERSONAL INFORMATION PROTECTION ACT

[Enforcement Date 15. Sep, 2023.] [Act No.19234, 14. Mar, 2023., Partial Amendment]

개인정보보호위원회 (심사총괄담당관 - 일반 법령해석) 02-2100-3043
개인정보보호위원회 (국제협력담당관 - 국외이전) 02-2100-2484, 2499
개인정보보호위원회 (개인정보보호정책과 - 법령 제・개정, 아동・청소년) 02-2100-3057, 3047
개인정보보호위원회 (신기술개인정보과 - 영상정보, 안전조치) 02-2100-3064, 3028
개인정보보호위원회 (데이터안전정책과 - 가명정보, 개인정보안심구역) 02-2100-3088, 3074, 3058, 3079
개인정보보호위원회 (자율보호정책과 - 보호책임자, 자율규제, 보호수준 평가, 처리방침, 영향평가) 02-2100-3083, 3089, 3087, 3096, 3086
개인정보보호위원회 (분쟁조정과 - 분쟁조정, 손해배상책임) 1833-6972, 02-2100-3142
개인정보보호위원회 (범정부마이데이터 추진단(전략기획팀 - 전송요구권(마이데이터)) 02-2100-3173

CHAPTER I GENERAL PROVISIONS

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 on Mar. 24, 2014>

Article 2 (Definitions) The terms used in this Act are defined as follows: <Amended on Mar. 24, 2014; Feb. 4, 2020; Mar. 14, 2023>

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, pictures, etc.;
   (b) Information which, even if it by itself does not uniquely identify an individual, may be easily combined with other information to uniquely identify an 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 uniquely identifying an 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 uniquely identify an individual without additional

information, by erasing 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 work;
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 "fixed visual data processing device" means a device prescribed by Presidential Decree, which is installed at a certain place to continuously or regularly takes pictures of persons or things, etc. or transmits such pictures via a wired or wireless network;

7-2. The term "mobile visual data processing device" means a device prescribed by Presidential Decree, which a person can wear or carry or which can be attached to or mounted on a movable object to take pictures of persons or things, etc. or to transmit such pictures through a wired or wireless network;

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 of Information Protection) (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 under Article 30 and other matters related to personal information processing, and shall guarantee the data subject's rights, such as the right to request access to his or her personal information. <Amended on Mar. 14, 2023>

(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 fulfill the purposes of collecting personal information by processing anonymized or pseudonymized personal information, the personal information controller shall endeavor to process personal information through anonymization, where anonymization is possible, or through pseudonymization, if it is impossible to fulfill the purposes of collecting personal information through anonymization. <Amended on Feb. 4, 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 or regulations.

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: <Amended on Mar. 14, 2023>

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 personal information is being processed and to request access (including the provision of copies; hereinafter the same applies) to and

transmission of such personal information;

4. The right to suspend the processing of, and to request correction, erasure, 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.
6. The right to refuse to accept a decision made through a fully automated processing of personal information or to request an explanation thereof.

Article 5 (Responsibilities of the State) (1) The State and local governments 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 to ensure the protection of individual privacy.

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

(3) The State and local governments shall formulate policies necessary for protecting the personal information of children under 14 years of age so that such children can clearly understand the effects of the processing of personal information and the rights of data subjects, etc. <Newly Inserted on Mar. 14, 2023>

(4) The State and local governments 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. <Amended on Mar. 14, 2023>

(5) When applying statutes or regulations or municipal ordinances regarding the processing of personal information, the State and local governments shall be in conformity with the principles of information protection to guarantee the rights of data subjects. <Amended on Mar. 14, 2023>

Article 6 (Relationship to Other Statutes) (1) Except as otherwise provided in other statutes, the processing and protection of personal information shall be governed by this Act. <Amended on Mar. 24, 2014; Mar. 14, 2023>

(2) An enactment of other statutes or amendment to existing statutes regarding the processing and protection of personal information shall be made fit for the purpose and principles of this Act. <Newly Inserted on Mar. 14, 2023>

CHAPTER II ESTABLISHMENT OF PERSONAL INFORMATION PROTECTION POLICIES

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 perform business affairs relating to the protection of personal information. <Amended on Feb. 4, 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 on Feb. 4, 2020>

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

(3) Deleted. <Feb. 4, 2020>

(4) Deleted. <Feb. 4, 2020>

(5) Deleted. <Feb. 4, 2020>

(6) Deleted. <Feb. 4, 2020>

(7) Deleted. <Feb. 4, 2020>

(8) Deleted. <Feb. 4, 2020>

(9) Deleted. <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 10 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 Article 2 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.

[This Article Newly Inserted on Feb. 4, 2020]

Article 7-3 (Chairperson) (1) The Chairperson shall represent the Protection Commission, preside over meetings of the Protection Commission, and oversee the related business affairs.

(2) If the Chairperson cannot perform his or 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 or 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 business affairs 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 business affairs under his or her jurisdiction.

[This Article Newly Inserted on Feb. 4, 2020]

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.

[This Article Newly Inserted on Feb. 4, 2020]

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 or 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 or her duties under this Act or any other Act.

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

[This Article Newly Inserted on Feb. 4, 2020]

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 work 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 work for profit set forth in paragraph (1) shall be prescribed by Presidential Decree.

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

[This Article Newly Inserted on Feb. 4, 2020]

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 party member 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 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.

[This Article Newly Inserted on Feb. 4, 2020]

Article 7-8 (Business Affairs under Jurisdiction of Protection Commission) The Protection Commission shall perform the following affairs: <Amended on Mar. 14, 2023>

1. Matters relating to the improvement of statutes or regulations relating to personal information protection;
2. Matters relating to the establishment or execution of policies, systems or plans relating to personal information protection;
3. Matters relating to 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 relating to the investigation and study, education and promotion of statutes or regulations, policies, systems and status relating to personal information protection;
7. Matters relating to support for and dissemination of technological development relating to personal information protection, the standardization of technologies, and nurturing of experts;

8. Matters provided in this Act and other statutes or regulations as affairs under the jurisdiction of the Protection Commission.

[This Article Newly Inserted on Feb. 4, 2020]

Article 7-9 (Matters to Be Deliberated and Resolved on by Protection Commission) (1) The Protection Commission shall deliberate and resolve on the following matters: <Amended on Mar. 14, 2023>

1. Matters relating to the assessment of personal information 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 relating to the improvement of policies, systems, and law relating to personal information protection;
4. Matters relating to the coordination of positions taken by public institutions with respect to the processing of personal information;
5. Matters relating to the interpretation and operation of statutes or regulations related to the protection of personal information;
6. Matters relating to the use and provision of personal information under Article 18 (2) 5;
6-2. Matters relating to orders to suspend cross-border transfers of personal information under Article 28-9;
7. Matters relating to the results of the privacy impact assessment under Article 33 (4);
8. Matters relating to the imposition of penalty surcharges under Article 64-2;
9. Matters relating to the presentation of opinions and recommendation for improvement under Article 61;
9-2. Matters concerning recommendations for correction pursuant to Article 63-2 (2);
10. Matters relating to corrective measures under Article 64;
11. Matters relating to accusation and recommendation for disciplinary actions under Article 65;
12. Matters relating to the publication of processing results and orders for publication under Article 66;
13. Matters relating to the imposition of administrative fines under Article 75;
14. Matters relating to the enactment, amendment and abolition of statutes or regulations 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 on which the Protection Commission deliberates or resolves pursuant to this Act or other statutes or regulations.

(2) The Protection Commission may take the following measures if necessary to deliberate and resolve matters provided 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 upon 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 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.

[This Article Newly Inserted on Feb. 4, 2020]

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.

[This Article Newly Inserted on Feb. 4, 2020]

Article 7-11 (Exclusion of, Challenge to, or Recusal of, Commissioner) (1) A Commissioner of the Protection Commission shall be excluded from deliberation and resolution on 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 obligor 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) Where the circumstances indicate that it would be impracticable to expect fair deliberations and resolutions by a Commissioner, any party may file a motion for challenge, and the Protection Commission shall make a decision by resolution.

(3) A Commissioner may recuse himself or herself from the case on the grounds provided in paragraph (1) or (2).

[This Article Newly Inserted on Feb. 4, 2020]

Article 7-12 (Sub-Commission) (1) The Protection Commission may have sub-commissions which will deliberate and resolve minor personal information breach 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.

[This Article Newly Inserted on Feb. 4, 2020]

Article 7-13 (Secretariat) The Protection Commission shall have a secretariat to perform business affairs, and matters that are not specified in this Act in relation to the organization of the Protection Commission shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Feb. 4, 2020]

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.

[This Article Newly Inserted on Feb. 4, 2020]

Article 8 Deleted. <Feb. 4, 2020>

Article 8-2 (Assessment of Personal Information Breach Incident Factors) (1) The head of a central administrative agency shall request the Protection Commission to assess the factors of personal information 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 or regulation by analyzing and reviewing the personal information breach incident factors of such statute or regulation.

(3) Matters necessary for the procedure and method to assess the personal information breach incident factors under paragraph (1) shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Jul. 24, 2015]

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 relevant central administrative agencies to ensure the protection of personal information and the rights and interests of data subjects: <Amended on Mar. 23, 2013; Nov. 19, 2014; 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 or regulations 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) (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 on Mar. 23, 2013; Nov. 19, 2014; 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 on Jul. 24, 2015; Jul. 26, 2017; Feb. 4, 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 on Jul. 24, 2015>

(4) Any person upon receipt of a request to furnish the materials under paragraphs (1) through (3) shall comply with the request unless there are extraordinary circumstances. <Amended on 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 on Jul. 24, 2015>

Article 11-2 (Assessment of Level of Personal Information Protection) (1) The Protection Commission shall conduct an annual assessment of central administrative agencies and

institutions affiliated with such agencies, local governments, or any other institutions prescribed by Presidential Decree for the performance of policies and work for the protection of personal information and the compliance of obligations under this Act (hereinafter referred to as "assessment of the level of personal information protection").

(2) The Protection Commission may require the head of a relevant public institution to submit relevant materials where necessary for the assessment of the level of personal information protection.

(3) The Protection Commission may disclose the results of the assessment of the level of personal information protection on its website, etc.

(4) The Protection Commission may grant awards to exemplary institutions and employees belonging thereto according to the results of the assessment of the level of personal information protection, and recommend improvement to the head of a relevant public institutions, if deemed necessary for the protection of personal information. In such cases, the head of the public institution shall make good faith efforts to comply with the recommendation, and notify the Protection Commission of the results of the measures taken.

(5) Other matters necessary for the criteria, methods, and procedures for the assessment of the level of personal information protection, the scope of data to be submitted under paragraph (2), etc. shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 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 13-2 (Personal Information Protection Day) (1) September 30 of each year shall be designated as the Personal Information Protection Day to raise awareness among citizens as to the importance of the protection and processing of personal information.

(2) The State and local governments may hold various events to spread the culture of personal information protection during the week in which the Personal Information Protection Day is included.

[This Article Newly Inserted on Mar. 14, 2023]

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 cross-border transfers of personal information.

CHAPTER III PROCESSING OF PERSONAL INFORMATION

SECTION 1 Collection, Use, and Provision 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 cases, and use it within the scope

of the purpose of collection: <Amended on Mar. 14, 2023>

1. Where consent is obtained from a data subject;
2. Where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations;
3. Where it is unavoidable for a public institution's performance of work under its jurisdiction as prescribed by statutes or regulations, etc.;
4. Where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract;
5. 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;
6. Where it is necessary to attain the legitimate interests 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 legitimate interests of the personal information controller and does not go beyond a reasonable scope.
7. Where it is urgently necessary for the public safety and security, public health, etc.

(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 to ensure safety such as encryption have been taken. <Newly Inserted on Feb. 4, 2020>

Article 16 (Restriction on 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 with consent of the data subject. <Newly Inserted on Aug. 6, 2013>

(3) A personal information controller shall not refuse to provide 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 on 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 cases: <Amended on Feb. 4, 2020; Mar. 14, 2023>

1. Where 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 through 7.

(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) Deleted. <Mar. 14, 2023>

(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 measures necessary to secure safety, such as encryption, have been

taken, etc. <Newly Inserted on Feb. 4, 2020>

Article 18 (Restriction on Repurposing Personal Information and Provision Thereof) (1) No personal information controller shall use personal information beyond the scope provided in Article 15 (1) or provide it to any third party beyond the scope provided in Articles 17 (1) and 28-8 (1). <Amended on Feb. 4, 2020; Mar. 14, 2023>

(2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may repurpose personal information or provide it to a third party, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That subparagraphs 5 through 9 shall be applied only to public institutions: <Amended on Feb. 4, 2020; Mar. 14, 2023>

1. Where separate consent is obtained from the data subject;
2. Where special provisions exist in other statutes;
3. 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;
4. Deleted; <Feb. 4, 2020>
5. Where it is impossible to perform the work under its jurisdiction as provided in other statutes, unless the personal information controller repurposes personal information 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, institution and maintenance of a prosecution;
8. Where it is necessary for a court to proceed with trial-related work;
9. Where it is necessary for the enforcement of punishment, probation and custody;
10. Where it is urgently necessary for the public safety and security, public health, etc.

(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 repurposes personal information or provides it to a third party under paragraph (2) 2 through 6 and 8 through 10, the public institution shall post matters necessary for the legal basis for such use or provision, purpose, scope, and the like on the Official Gazette or on its website, as prescribed by Notification of the Protection Commission.<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(5) Where a personal information controller provides personal information to a third party for another purpose in any case provided in any subparagraph of 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 upon receipt of such request shall take measures necessary to ensure the safety of the personal information.

[Title Amended on Aug. 6, 2013]

Article 19 (Restriction on 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 separate consent is obtained from the data subject;
2. Where special provisions exist in other statutes.

Article 20 (Notification of Sources of Personal Information Collected from Other Than Data Subjects) (1) When a personal information controller processes personal information collected from sources other than data subjects, the personal information controller shall immediately notify the data subject of the following matters at the request of such data subject: <Amended on Mar. 14, 2023>

1. The source of collected personal information;

2. The purpose of processing personal information;
3. The fact that the data subject is entitled to request suspension of processing of personal information or to withdraw consent, 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 on Mar. 29, 2016; Feb. 4, 2020>

(3) Matters necessary for the time, method, and procedure of giving notification to the data subject pursuant to the main clause of paragraph (2), shall be prescribed by Presidential Decree. <Newly Inserted on Mar. 29, 2016>

(4) Paragraph (1) and the main clause of paragraph (2) shall not apply to any of the following cases: Provided, That this shall be the case only where it is manifestly superior to the rights of data subjects under this Act: <Amended on Mar. 29, 2016; Mar. 14, 2023>

1. Where personal information, which is subject to a notification request, is included in the personal information files referred to in any subparagraph of Article 32 (2);
2. Where such notification is likely to cause harm to the life or body of any other person, or to unfairly damage the property and other interests of any other person.

[Title Amended on Mar. 14, 2023]

Article 20-2 (Notification of Details of Use and Provision of Personal Information) (1) A personal information controller who meets the criteria prescribed by Presidential Decree shall regularly notify data subjects of the details of the use and provision of personal information collected under this Act or the method of accessing the information system through which such details can be confirmed: Provided, That the notification may be omitted where personal information that enables notifications to the data subject, such as contact information, has not been collected or retained.

(2) Matters necessary for the scope of data subjects subject to notification, information to be notified, frequency, method, etc. of notification under paragraph (1) shall be prescribed

by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

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, the expiry of the processing period of pseudonymized information, etc.: Provided, That this shall not apply where the retention of such personal information is mandatory by other statutes or regulations. <Amended on Mar. 14, 2023>

(2) When a personal information controller destroys personal information pursuant to paragraph (1), measures necessary 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 of 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 Article 22-2 (1); hereafter in this Article the same shall apply) 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. In such cases, the personal information controller shall categorize the matters requiring consent falling under the following subparagraphs and obtain consent, respectively. <Amended on Apr. 18, 2017; Mar. 14, 2023>

1. Where consent shall be obtained under Article 15 (1) 1;
2. Where consent shall be obtained under Article 17 (1) 1;
3. Where consent shall be obtained under Article 18 (2) 1;
4. Where consent shall be obtained under subparagraph 1 of Article 19;
5. Where consent shall be obtained under Article 23 (1) 1;

6. Where consent shall be obtained under Article 24 (1) 1;
7. Where the personal information controller intends to obtain consent to the processing of personal information in order to promote goods or services or solicit purchase thereof;
8. Other cases prescribed by Presidential Decree where it is necessary to obtain consent by categorizing the matters requiring consent to protect a data subject.

(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 on Apr. 18, 2017; Jul. 26, 2017; Feb. 4, 2020>

(3) With respect to the personal information that can be processed without consent of the data subject, a personal information controller shall disclose the relevant items and legal basis for such processing under Article 30 (2) by separating such information from the personal information processed with consent of the data subject, or shall inform the data subject thereof by e-mail or any other means prescribed by Presidential Decree. In such cases, the burden of proof that personal information can be processed without consent shall be borne by the personal information controller. <Amended on Mar. 29, 2016; Apr. 18, 2017; Mar. 14, 2023>

(4) Deleted. <Mar. 14, 2023>

(5) A personal information controller shall not refuse to provide goods or services to a data subject on the grounds that the data subject would not consent to the matter eligible for selective consent, or would not consent pursuant to paragraph (1) 3 and 7. <Amended on Apr. 18, 2017; Mar. 14, 2023>

(6) Deleted. <Mar. 14, 2023>

(7) Except as provided in paragraphs (1) through (5), matters necessary for detailed methods to obtain the consent of data subjects shall be prescribed by Presidential Decree, in consideration of the collection media of personal information and other factors. <Amended on Apr. 18, 2017; Mar. 14, 2023>

Article 22-2 (Protection of Children's Personal Information) (1) When the consent of a child under 14 years of age is required to process the personal information of such child, a personal information controller shall obtain the consent of his or her legal representative and confirm whether the legal representative has granted consent.

(2) Notwithstanding paragraph (1), information prescribed by Presidential Decree as minimum information necessary for obtaining the consent of a legal representative may be collected directly from the relevant child without consent of the legal representative.

(3) A personal information controller shall, when notifying a child under 14 years of age of matters relating to the processing of personal information, use such a form and such a clear and plain language that the child can easily understand.

(4) Except as provided in paragraphs (1) through (3), matters necessary for the methods of obtaining consent and of obtaining confirmation of consent, etc., shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

SECTION 2 Restriction on Processing of Personal Information

Article 23 (Restriction on 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 on 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 or regulations 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 on Mar. 29, 2016>

(3) Where a personal information controller deems that there is a risk of privacy invasion because sensitive information of the data subject is included in the information disclosed in the course of the provision of goods or services, the personal information controller shall communicate to the data subject the possibility of disclosure of sensitive information and the method of selecting non-disclosure in an easily understandable manner before providing the goods or services. <Newly Inserted on Mar. 14, 2023>

Article 24 (Restriction on 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 or regulations (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 or regulations specifically require or permit the processing of unique identification information.

(2) Deleted. <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 on 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 on Mar. 29, 2016; Jul. 26, 2017; Feb. 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 on Mar. 29, 2016; Jul. 26, 2017; Feb. 4, 2020>

Article 24-2 (Restriction on 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 on Nov. 19, 2014; Mar. 29, 2016; Jul. 26, 2017; 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 cases prescribed by Notification of 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 on Mar. 24, 2014; 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). <Amended on Mar. 24, 2014>

(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 on Mar. 24, 2014; Jul. 26, 2017; Feb. 4, 2020>

[This Article Newly Inserted on Aug. 6, 2013]

Article 25 (Restriction on Installation and Operation of Fixed Visual Data Processing Devices) (1) No one shall install and operate any fixed visual data processing device at open places, except in any of the following cases: <Amended on Mar. 14, 2023>

1. Where specifically allowed by statutes or regulations;
2. Where it is necessary for the prevention and investigation of crimes;
3. Where a person with legitimate authority installs and operates such device for the safety and management of facilities and prevention of fire;
4. Where a person with legitimate authority installs and operates such device for traffic enforcement;
5. Where a person with legitimate authority installs and operates such device for the collection, analysis, and provision of traffic information;
6. Cases prescribed by Presidential Decree, where the photographed image information is not stored.

(2) No one shall install and operate any fixed visual data processing device to look into the places which are likely to noticeably threaten individual privacy, such as a bathroom, restroom, sauna, and dressing room used by many unspecified persons: Provided, That this shall not apply to the facilities prescribed by Presidential Decree, which are used to detain or protect persons in accordance with statutes or regulations, such as correctional institutions and mental health care centers. <Amended on Mar. 14, 2023>

(3) The head of a public institution who intends to install and operate fixed visual data processing devices pursuant to the subparagraphs of paragraph (1) and a person who intends to install and operate fixed visual data processing devices pursuant to the proviso of paragraph (2) shall gather opinions of relevant specialist and interested persons through the procedures prescribed by Presidential Decree such as public hearings and information sessions. <Amended on Mar. 14, 2023>

(4) A person who installs and operates fixed visual data processing devices pursuant to the subparagraphs of paragraph (1) (hereinafter referred to as "fixed visual data processing device 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 on Mar. 29, 2016; Mar. 14, 2023>

1. The purpose and place of installation;

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

(5) A fixed visual data processing device operator shall neither arbitrarily manipulate a fixed visual data processing device for purposes other than those for which the device was installed, nor direct the device toward different spots, nor use sound recording functions. <Amended on Mar. 14, 2023>

(6) A fixed visual data processing device operator shall take measures necessary to ensure safety pursuant to Article 29 to prevent personal information from being lost, stolen, divulged, forged, altered, or damaged. <Amended on Jul. 24, 2015; Mar. 14, 2023>

(7) A fixed visual data processing device operator shall establish an appropriate policy to operate and manage the fixed visual data processing devices, as prescribed by Presidential Decree: Provided, That the fixed visual data processing device operator need not formulate a policy to operate and manage the fixed visual data processing devices if he or she has included matters regarding the operation and management of fixed visual data processing devices when formulating the Privacy Policy under Article 30. <Amended on Mar. 14, 2023>

(8) A fixed visual data processing device operator may entrust the business affairs regarding the installation and operation of fixed visual data processing devices to a third party: Provided, That public institutions shall comply with the procedures and requirements prescribed by Presidential Decree when entrusting the business affairs regarding the installation and operation of fixed visual data processing devices to a third party. <Amended on Mar. 14, 2023>

[Title Amended on Mar. 14, 2023]

Article 25-2 (Restriction on Operation of Mobile Visual Data Processing Devices) (1) A person who intends to operate a mobile visual data processing device for work purposes shall not take photographs (limited to cases falling within the scope of personal information; hereinafter the same shall apply) of a person or things related to such person at public places, except in the following cases:

1. In any of the cases falling under any subparagraph of Article 15 (1);
2. Where the data subject fails to express his or her intention to refuse to be photographed, although the fact of photographing is clearly stated to inform the data

subject; in such cases, it shall be limited to cases where it is unlikely to unduly infringe upon the right of a data subject and where it does not exceed reasonable limits;

3. Other cases prescribed by Presidential Decree, corresponding to those referred to in subparagraphs 1 and 2.

(2) No one shall take photographs of a person or things related to such person through a mobile visual data processing device at a place used by many unspecified persons where an individual's privacy could be significantly compromised, such as a bathroom, toilet, sauna, and changing room: Provided, That this shall not apply to cases prescribed by Presidential Decree, where it is necessary for lifesaving and first-aid services.

(3) Where a person or thing related to such person is photographed with a portable visual data processing device in cases falling under the subparagraphs of paragraph (1), the fact of photographing shall be indicated and notified as prescribed by Presidential Decree, by such means as light, sound, and signboard.

(4) Except as provided in paragraphs (1) through (3), Article 25 (6) through (8) shall apply mutatis mutandis to the operation of mobile visual data processing devices.

[This Article Newly Inserted on Mar. 14, 2023]

Article 26 (Restriction on Personal Information Processing Subsequent to Entrustment of Work) (1) A personal information controller shall, when entrusting the processing of personal information to a third party, do so in a document that states the following: <Amended on Mar. 14, 2023>

1. Prevention of personal information processing for other purposes than performing the entrusted work;
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 who entrusts the processing of personal information pursuant to paragraph (1) (hereinafter referred to as "person entrusting") shall disclose the details of the entrusted affairs and the entity that processes personal information (including a third party re-entrusted from a person entrusted with the processing of personal information; hereinafter referred to as "person entrusted") in the manner prescribed by Presidential Decree so as to be easily recognizable by data subjects at any time. <Amended on Mar. 14, 2023>

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

(4) The person entrusting shall educate the person entrusted so that personal information of data subjects may not be lost, stolen, divulged, forged, altered, or damaged owing to the outsourcing of work, and supervise how the person entrusted processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree. <Amended on Jul. 24, 2015>

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

(6) A person entrusted shall, when he or she intends to re-entrust the processing of entrusted personal information to a third party, obtain consent from the person entrusting. <Newly Inserted on Mar. 14, 2023>

(7) With respect to liability for damages arising out of the processing of personal information entrusted to an person entrusted in violation of this Act, the person entrusted shall be deemed an employee of the personal information controller. <Amended on Mar. 14, 2023>

(8) Articles 15 through 18, 21, 22, 22-2, 23, 24, 24-2, 25, 25-2, 27, 28, 28-2 through 28-5, 28-7 through 28-11, 29, 30, 30-2, 31, 33, 34, 34-2, 35, 35-2, 36, 37, 37-2, 38, 59, 63, 63-2, and 64-2 shall apply mutatis mutandis to outsourcees. In such cases, "personal information controller" shall be construed as "person entrusted". <Amended on Mar. 14, 2023>

Article 27 (Restriction on Transfer of Personal Information following Business Transfer) (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) In processing personal information, a personal information controller shall limit the scope of persons who process the personal information under his or her command and supervision, such as an executive officer or employee, temporary agency worker, and part-time worker (hereinafter referred to as "personal information handler") to a minimum extent and shall appropriately manage and supervise such personal information handlers. <Amended on Mar. 14, 2023>

(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.

SECTION 3 Special Cases concerning Pseudonymized Information

Article 28-2 (Processing of Pseudonymized Information) (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 uniquely identify an individual when providing pseudonymized information to a third party according to paragraph (1).

[This Article Newly Inserted on Feb. 4, 2020]

Article 28-3 (Restriction on Combination of Pseudonymized Information) (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 transfer 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 revoke the designation of, a specialized institution management and supervision, and standards and procedures of transfer and approval pursuant to paragraph (2) shall be prescribed by Presidential Decree. [This Article Newly Inserted on Feb. 4, 2020]

Article 28-4 (Obligation to Take Safety Measures for Pseudonymized Information) (1) In processing pseudonymized information under Article 28-2 or 28-3, a personal information controller shall take such technical, administrative, and physical measures as separately storing and managing additional information needed for restoration to the original state, which are necessary to ensure safety as prescribed by Presidential Decree to prevent personal information from being lost, stolen, divulged, forged, altered, or damaged. <Amended on Mar. 14, 2023>

(2) In processing pseudonymized information in accordance with Article 28-2 or 28-3, a personal information controller may separately determine the processing period of the pseudonymized information in consideration of the processing purpose, etc. <Newly Inserted on Mar. 14, 2023>

(3) A personal information controller who intends to process pseudonymized information under Article 28-2 or 28-3 shall prepare and retain records relating to matters prescribed by Presidential Decree including the purpose of processing the pseudonymized information, a recipient in cases pseudonymized information is provided to a third party, the processing period of pseudonymized information, etc. (limited to cases where the processing period is separately determined under paragraph (2)) to manage the details of

the processing of pseudonymized information, and shall retain the records for at least three years from the date of destruction in the event of destruction of pseudonymized information. <Amended on Mar. 14, 2023>
[This Article Newly Inserted on Feb. 4, 2020]

Article 28-5 (Prohibited Acts in Processing Pseudonymized Information) (1) No person who processes pseudonymized information under Article 28-2 or 28-3 shall process such information for the purpose of uniquely identifying an individual. <Amended on Mar. 14, 2023>

(2) When information that can uniquely identify an individual is generated in the process of processing pseudonymized information under Article 28-2 or 28-3, a personal information controller shall immediately cease the processing of the relevant information, and shall retrieve and destroy the information without delay. <Amended on Mar. 14, 2023>
[This Article Newly Inserted on Feb. 4, 2020]

Article 28-6 Deleted. <Mar. 14, 2023>

Article 28-7 (Scope of Application) @Articles 20, 20-2, 27, 34 (1), 35, 35-2, 36, and 37 shall not apply to pseudonymized information processed under Article 28-2 or 28-3. <Amended on Mar. 14, 2023>
[This Article Newly Inserted on Feb. 4, 2020]

SECTION 4 Cross-Border Transfer of Personal Information

Article 28-8 (Cross-Border Transfer of Personal Information) (1) No cross-border provision (including inquiry), entrusted processing, or storage (hereafter in this Section referred to as "transfer") of personal information shall be allowed by a personal information controller: Provided, That in any of the following cases, the cross-border transfer of personal information may be allowed:

1. Where separate consent is obtained from the data subject;
2. Where there are special provisions regarding the cross-border transfer of personal information in a statute, a treaty to which the Republic of Korea is a party, or other international conventions;

3. In any of the following cases where it is necessary to entrust the processing of personal information and to retain such personal information in order to conclude and perform a contract with the data subject:
   (a) Where the matters set forth in the subparagraphs of paragraph (2) are disclosed in the Privacy Policy provided in Article 30;
   (b) Where the matters provided in the subparagraphs of paragraph (2) are communicated to the data subject by means prescribed by Presidential Decree, such as electronic mail;
4. Where the recipient of personal information obtains certification determined and publicly notified by the Protection Commission, such as the certification of personal information protection under Article 32-2, and takes all of the following measures:
   (a) Safety measures necessary for protecting personal information and measures necessary for guaranteeing the rights of data subjects;
   (b) Measures necessary for implementing certified matters in the country to which personal information is to be transferred;
5. Where the Protection Commission recognizes that the personal information protection system of the country or international organization to which the personal information is to be transferred, the scope of guarantee of the rights of the data subject, and the procedures for damage relief, etc. are substantially equal to the level of personal information protection under this Act.

(2) A personal information controller shall inform data subjects of the following matters in advance when obtaining consent under paragraph (1) 1:

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 recipient of personal information (referring to the name of a corporation and the contact information of the corporation, if the recipient is a corporation);
4. The purpose of using personal information by the recipient of personal information and the period of retention and use of personal information;
5. The method and procedure for refusing the transfer of personal information and the effect of such refusal.

(3) A personal information controller that intends to change the matters provided in any subparagraph of paragraph (2) shall inform a data subject of such change and obtain the

data subject's consent thereto.

(4) A personal information controller shall comply with other provisions of this Act and Articles 17 through 19 and Chapter V of this Act, which are related to the cross-border transfer of personal information, and shall take protective measures prescribed by Presidential Decree, where it makes cross-border transfers of personal information pursuant to the proviso, with the exception of the subparagraphs, of paragraph (1).

(5) A personal information controller shall not enter into a contract for cross-border transfers of personal information containing terms and conditions that are in violation of this Act.

(6) Except as provided in paragraphs (1) through (5), matters necessary for the criteria and procedures for the cross-border transfer of personal information, etc. shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

Article 28-9 (Orders to Suspend Cross-Border Transfers of Personal Information) (1) The Protection Commission may order a personal information controller to suspend cross-border transfers of personal information in any of the following cases where the cross-border transfer of personal information is ongoing or where any further cross-border transfer is expected:

1. Cases in violation of Article 28-8 (1), (4), or (5);
2. Where the recipient of personal information or the State or international organization to which the personal information is transferred fails to properly protect the personal information when compared to the level of personal information protection under this Act, and thus the data subject suffers damage or is highly likely to suffer damage.

(2) Upon receipt of an order to suspend cross-border transfers of personal information under paragraph (1), a personal information controller may file an objection with the Protection Commission within seven days after receipt of such order.

(3) Matters necessary for the standards for orders to suspend cross-border transfers of personal information under paragraph (1), the procedures for filing an objection under paragraph (2), etc. shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

Article 28-10 (Reciprocity) Notwithstanding Article 28-8, personal information controllers in a country that restricts cross-border transfers of personal information may be subject to restrictions at a level equivalent to those imposed by the country: Provided, That this shall not apply where cross-border transfers are necessary to implement a treaty or other international conventions.
[This Article Newly Inserted on Mar. 14, 2023]

Article 28-11 (Provisions Applicable Mutatis Mutandis)

CHAPTER IV SAFEGUARD OF PERSONAL 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 on Jul. 24, 2015>

Article 30 (Establishment and Disclosure of Privacy Policy) (1) A 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 on Mar. 29, 2016; Feb. 4, 2020; Mar. 14, 2023>

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);
3-3. The possibility of disclosure of sensitive information and the method of selecting non-disclosure under Article 23 (3) (if applicable);
4. Entrusting personal information processing (if applicable);
4-2. Matters relating to processing, etc. of pseudonymized information under Articles 28-2 and 28-3 (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 work 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020>

Article 30-2 (Evaluation of Privacy Policy and Recommendations for Improvements) (1) The Protection Commission shall evaluate the following with respect to the Privacy Policy and may recommend that the relevant personal information controller improve the policy pursuant to Article 61 (2), if it is deemed necessary to improve the policy based on the evaluation results:

1. Whether the matters that shall be included in the Privacy Policy pursuant to this Act are appropriately determined;
2. Whether the Privacy Policy has been prepared in an easily understandable manner;
3. Whether the Privacy Policy is disclosed in such a way that the data subject can easily confirm.

(2) Matters necessary for those subject to the evaluation of the Privacy Policy, criteria and procedures therefor, etc. shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

Article 31 (Designation of Privacy Officers) (1) A personal information controller shall designate a privacy officer who shall have general supervision and control of the work regarding personal information processing: Provided, That a personal information controller whose number of employees, turnover, etc. meet the criteria prescribed by Presidential Decree need not designate a privacy officer. <Amended on Mar. 14, 2023>

(2) Where a privacy officer is not designated under the proviso of paragraph (1), the business owner or representative of the personal information controller shall become the privacy officer. <Newly Inserted on Mar. 14, 2023>

(3) A privacy officer shall perform the following work: <Amended on Mar. 14, 2023>

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 work prescribed by Presidential Decree for the appropriate processing of personal information.

(4) In performing the work provided in the subparagraphs of paragraph (3), a privacy officer may occasionally inspect the current status of personal information processing, processing systems, etc. if necessary, and may request a report thereon from the relevant parties. <Amended on Mar. 14, 2023>

(5) Where a privacy officer becomes aware of any violation of this Act or other relevant statutes or regulations in relation to the protection of personal information, he or she 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. <Amended on Mar. 14, 2023>

(6) A personal information controller shall not allow the privacy officer to give or be subject to disadvantages without good cause while performing the affairs provided in the

subparagraphs of paragraph (3), and shall guarantee the independent performance of work by the privacy officer. <Amended on Mar. 14, 2023>

(7) A personal information controller may organize and operate a council of privacy officers comprised of the privacy officers provided in paragraph (1) so as to safely process and protect personal information, exchange information, and conduct other joint projects prescribed by Presidential Decree. <Newly Inserted on Mar. 14, 2023>

(8) The Protection Commission may provide support necessary for the activities of the council of privacy officers under paragraph (7). <Newly Inserted on Mar. 14, 2023>

(9) Matters necessary for the qualification requirements for a privacy officer under paragraph (1), the work under paragraph (3), the guarantee of independence under paragraph (6), and other relevant matters, shall be prescribed by Presidential Decree, taking into consideration sales, the scale of personal information retained, etc. <Amended on Mar. 14, 2023>

[Title Amended on Mar. 14, 2023]

Article 31-2 (Designation of Domestic Agents) (1) A personal information controller with no address or place of business in the Republic of Korea who is prescribed by Presidential Decree in consideration of the sales, the scale of personal information retained, and other factors shall designate a person who acts as an agent for the following (hereinafter referred to as "domestic agent"). In such cases, the domestic agent shall be designated in writing: <Amended on Mar. 14, 2023>

1. Work of a privacy officer under Article 31 (3);
2. Notification and reporting of the personal data under Article 34 (1) and (3);
3. Submission of materials such as articles and documents under Article 63 (1).

(2) A domestic agent shall have an address or business office in Korea. <Amended on Mar. 14, 2023>

(3) The personal information controller shall include the following in the Privacy Policy if he or she designates a domestic agent pursuant to paragraph (1): <Amended on Mar. 14, 2023>

1. Name of the domestic agent (in cases of a corporation, referring to its name and the name of its representative);
2. Address (in cases of a corporation, referring to the location of a business office), telephone number, and e-mail address of the domestic agent.

(4) If a domestic agent violates this Act in relation to the subparagraphs of paragraph (1), the personal information controller shall be deemed to have committed such a violation. <Amended on Mar. 14, 2023>

[This Article Newly Inserted on Feb. 4, 2020]

[Moved from Article 39-11 <Mar. 14, 2023>]

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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 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: <Amended on Mar. 14, 2023>

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, institution and maintenance of a 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 prescribed by Presidential Decree, which are recognized as having little need for continuous management, such as ephemeral files;
5. Classified personal information files pursuant to other statutes or regulations.

(3) The Protection Commission may, if necessary, review where personal information files are registered and the content thereof under paragraph (1), and may recommend that the head of a relevant public institution make improvements.<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(4) If necessary to guarantee the rights of data subjects, 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(5) Matters necessary for 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 on Jul. 26, 2017; Feb. 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 on Jul. 26, 2017; Feb. 4, 2020>

1. Where personal information protection has been certified by fraud or other improper 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 or regulations are breached, and the grounds for the violation are material.

(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 on Jul. 26, 2017; Feb. 4, 2020>

(5) The Protection Commission may authorize the specialized institutions prescribed by Presidential Decree to perform the work 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 on Jul. 26, 2017; Feb. 4, 2020>

(6) Any person who has obtained certification under paragraph (1) may indicate or promote the details of 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 matters necessary 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.

[This Article Newly Inserted on Jul. 24, 2015]

Article 33 (Privacy Impact Assessment) (1) Where there is a risk of a personal information breach 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 to improve them (hereinafter referred to as "privacy impact assessment"), and submit the results thereof to the Protection Commission.
<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(2) The Protection Commission may designate a person who satisfies the requirements prescribed by Presidential Decree such as human resources and facilities as an institution that performs a privacy impact assessment (hereinafter referred to as "assessment institution"), and the head of a public institution shall request the assessment institution to conduct the privacy impact assessment. <Newly Inserted on Mar. 14, 2023>

(3) Privacy impact assessments shall take into account the following: <Amended on Mar. 14, 2023>

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.

(4) The Protection Commission may provide its opinion on the privacy impact assessment results submitted under paragraph (1).<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(5) 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. <Amended on Mar. 14, 2023>

(6) 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(7) The Protection Commission may revoke the designation of an assessment institution that has obtained designation under paragraph (2) in any of the following cases: Provided, That it shall revoke the designation in cases falling under subparagraph 1 or 2: <Newly Inserted on Mar. 14, 2023>

1. Where the designated assessment institution has obtained its designation by fraud or other improper means;
2. Where the designated assessment institution wants revocation of such designation or has closed its business;
3. Where the designated assessment institution ceases to meet the requirements for designation provided in paragraph (2);
4. Where the designated assessment institution has poorly performed its work either by intention or gross negligence, and is deemed incapable of duly performing its affairs;
5. Other cases that fall under any ground prescribed by Presidential Decree.

(8) Where the Protection Commission revokes designation pursuant to paragraph (7), it shall hold a hearing in accordance with the Administrative Procedures Act. <Newly Inserted on Mar. 14, 2023>

(9) Matters necessary for the criteria, methods, procedures, etc. for privacy impact assessments under paragraph (1) shall be prescribed by Presidential Decree. <Amended on Mar. 14, 2023>

(10) 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. <Amended on Mar. 14, 2023>

(11) A personal information controller other than public institutions shall proactively endeavor to conduct a privacy impact assessment, if there is a risk of a personal information beach of data subjects in operating the personal information files. <Amended on Mar. 14, 2023>

Article 34 (Notification and Reporting of Divulgence of Personal Information) (1) A personal information controller shall notify data subjects of the following matters without delay when the personal information controller becomes aware of loss, theft, or divulgence (hereafter in this Article referred to as "divulgence, etc.") of personma information: Provided, That if the contact information of the data subject is unknown or if any other good cause exists, a measure may be taken in lieu of giving notice, as prescribed by Presidential Decree: <Amended on Mar. 14, 2023>

1. Particulars of divulgence, etc. of personal information;
2. When and how divulgence, etc. of personal is made;
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, etc. of personal information and take necessary measures. <Amended on Mar. 14, 2023>

(3) Upon becoming aware of divulgence, etc. of personal information, the personal information controller shall, without delay, file a report with the Protection Commission or a specialized institution designated by Presidential Decree with respect to the matters provided in the subparagraphs of paragraph (1), as prescribed by Presidential Decree in consideration of the types of personal information, the process and scale of divulgence, etc., and other factors. In such cases, the Protection Commission and the specialized institution designated by Presidential Decree may provide technical assistance for the

prevention of the spread of damage, recovery from damage, and other purposes.<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(4) Matters necessary for notifying divulgence, etc. under paragraph (1) and timing, methods, and procedures for reporting breach, etc. under paragraph (3) shall be prescribed by Presidential Decree. <Amended on Mar. 14, 2023>

[Title Amended on Mar. 14, 2023]

Article 34-2 (Erasure and Blocking of Exposed Personal Information) (1) A personal information processor shall make sure to prevent personal information such as personally identifiable information, account information, and credit card information from being exposed to the public through information and communications networks. <Amended on Mar. 14, 2023>

(2) With respect to personal information exposed to the public, if requested by the Protection Commission or a specialized institution designated by Presidential Decree, the personal information controller shall take necessary measures such as erasing or blocking the relevant information. <Amended on Mar. 14, 2023>

[This Article Newly Inserted on Feb. 4, 2020]

[Moved from Article 39-10; previous Article 34-2 Deleted]

CHAPTER V GUARANTEE OF RIGHTS OF DATA SUBJECTS

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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 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 good cause for not permitting access during such period, the personal information

controller may postpone access after notifying the relevant data subject of the said ground and 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 statutes;
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 work:
   (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 statutes;
   (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 statutes.

(5) Matters necessary for 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 35-2 (Request for Transmission of Personal Information) (1) A data subject may request the personal information controller satisfying the criteria prescribed by Presidential Decree in consideration of the ability to process personal information, etc. to transmit to him or her personal information that satisfies all of the following requirements:

1. The personal information, the transmission of which is requested by the data subject, shall be any of the following personal information on himself or herself:
   (a) Personal information processed with consent under Article 15 (1) 1, 23 (1) 1, or 24 (1) 1;
   (b) Personal information processed to take measures at the request of a data subject in the course of performing or concluding a contract under Article 15 (1) 4;

(c) Among the personal information processed pursuant to Article 15 (1) 2 and 3, Article 23 (1) 2, or Article 24 (1) 2, the personal information designated as being subject to request for transmission by deliberation and resolution by the Protection Commission at the request of the head of a relevant central administrative agency for the interest of a data subject or public interest of a data subject;

2. Personal information, the transmission of which is requested, shall not be information separately generated by analyzing and processing the personal information collected by a personal information controller;
3. The personal information, the transmission of which is requested, shall be the personal information processed by a computer or any other information processing device.

(2) A data subject may request a personal information controller satisfying the criteria prescribed by Presidential Decree in consideration of the sales, the scale of personal information retained, the capability of personal information processing, industrial characteristics, and other relevant factors, to transmit his or her personal information requested under paragraph (1) to the following persons, to the extent it is technically feasible and reasonable:

1. Institutions specializing in managing personal information under Article 35-3 (1);
2. A person who fulfills his or her duty of safeguards under Article 29 and meets the standards for facilities and technology prescribed by Presidential Decree.

(3) Upon receipt of a request for transmission under paragraphs (1) and (2), the personal information controller shall transmit the relevant information in a form processable through a computer or other information processing device to the extent reasonable in terms of time, expenses, and technology.

(4) Upon receipt of a request for transmission under paragraphs (1) and (2), a personal information controller shall transmit the personal information of the data subject, notwithstanding the relevant provisions of any of the following statutes:

1. Article 81-13 of the Framework Act on National Taxes;
2. Article 86 of the Framework Act on Local Taxes;
3. Provisions of statutes prescribed by Presidential Decree, which are similar to those provided in subparagraphs 1 and 2.

(5) A data subject may withdraw his or her request for transmission under paragraphs (1) and (2).

(6) A personal information controller may refuse the request for transmission under paragraph (1) or (2) or suspend the transmission in cases prescribed by Presidential Decree, such as where it is impossible to verify whether a data subject is the person in question.
(7) No data subject shall infringe upon another person's rights or legitimate interests on the grounds of a request for transmission under paragraphs (1) and (2).
(8) Except as provided in paragraphs (1) through (7), necessary matters, such as the scope of information subject to a request for transmission, methods of requesting transmission, deadlines and methods for transmission, methods of withdrawing requests for transmission, rejection of requests for transmission, and methods of suspending transmission, shall be prescribed by Presidential Decree.
[This Article Newly Inserted on Mar. 14, 2023]

Article 35-3 (Institutions Specializing in Managing Personal Information) (1) A person who intends to perform any of the following work shall be designated by the Protection Commission or the head of a relevant central administrative agency as an institution specializing in managing personal Information:

1. Support for the exercise of the right to request the transmission of personal information under Article 35-2;
2. Establishing and standardizing a personal information transmission system to support the exercise of the rights of data subjects;
3. Managing and analyzing personal information to support the exercise of rights of data subjects;
4. Other affairs prescribed by Presidential Decree to effectively support the exercise of the rights of data subjects.

(2) Requirements for designation as an institution specializing in managing personal information under paragraph (1) shall be as follows:

1. The applicant shall have the technical level and expertise to transmit, manage, and analyze personal information;
2. The applicant shall be equipped with a level of measures to ensure safety for safely managing personal information;
3. The applicant shall have the financial capability necessary for the stable operation of an institution specializing in managing personal Information.

(3) No institution specializing in managing personal information shall engage in any of the following acts:

1. Forcing a data subject to request the transmission of his or her personal information, or unfairly inducing it;
2. Any other act prescribed by Presidential Decree, which is likely to infringe on personal information or restrict the rights of a data subject.

(4) If an institution specializing in managing personal information falls under any of the following, the head of the Protection Commission or of a relevant central administrative agency may revoke the designation of the institution specializing in managing personal information: Provided, that he or she shall revoke such designation in cases falling under subparagraph 1:

1. Where the institution has obtained the designation by fraud or other improper means;
2. Where the institution ceases to meet the requirements for designation under paragraph (2).

(5) If the Protection Commission or the head of a relevant central administrative agency intends to revoke the designation under paragraph (4), he or she shall hold hearings under the Administrative Procedures Act.

(6) The Protection Commission and the head of a relevant central administrative agency may provide an institution specializing in managing personal information support necessary for performing its work.

(7) In performing affairs under the subparagraphs of paragraph (1) at the request of a data subject, an institution specializing in managing personal information may collect from the data subject expenses incurred in performing such work.

(8) Matters necessary for the procedures for the designation of an institution specializing in managing personal information under paragraph (1), the detailed requirements for designation under paragraph (2), the procedures for revocation of designation under paragraph (4), etc. shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

Article 35-4 (Management of Transmitting Personal Information and Support Therefor) (1) The Protection Commission shall systematically manage and supervise the current status of personal information controllers provided in Articles 35-2 (1) and (2) and institutions specializing in managing personal information provided in Article 35-3 (1), the details of

use, the actual status of management, etc.

(2) The Protection Commission may build and operate a personal information transmission support platform to ensure the safe and efficient transmission of personal information, including the following:

1. The current status of institutions specializing in managing personal information and a list of personal information items that can be transmitted;
2. Details of a data subject's request for transmission and withdrawal of such request;
3. Support functions such as managing the history of transmission of personal information;
4. Other matters necessary to transmit personal information.

(3) The Protection Commission may interlink or integrate the transmission systems built and operated by institutions specializing in managing personal information for the efficient operation of personal information transmission support platforms under paragraph (2). In such cases, it shall have a prior consultation with the head of a relevant central administrative agency and the relevant institution specializing in managing personal information.

(5) Matters necessary for management and supervision and the establishment and operation of a personal information transmission support system under paragraphs (1) through (3) shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

Article 36 (Correction 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 or regulations.

(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 measures necessary to correct or erase as requested by the data subject unless otherwise specifically provided by other statutes or regulations 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 of 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) Matters necessary for 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 or may withdraw his or her consent to personal information processing. In such cases, if the personal information controller is a public institution, the data subject may request the institution to suspend the processing of his or her personal information contained in the personal information files to be registered pursuant to Article 32 or may withdraw his or her consent to personal information processing. <Amended on Mar. 14, 2023>
(2) Upon receipt of the request for suspension of processing 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: <Amended on Mar. 14, 2023>

1. Where special provisions exist in other statutes or it is unavoidable to observe obligations under statutes or regulations;
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) A personal information controller shall, when a data subject withdraws his or her consent pursuant to paragraph (1), take necessary measures without delay, such as destroying collected personal information to prevent recovery and reproduction thereof: Provided, That in cases falling under any subparagraph of paragraph (2), a personal information controller need not take measures following the withdrawal of consent. <Newly Inserted on Mar. 14, 2023>

(4) When rejecting a request for suspension of processing pursuant to the proviso of paragraph (2) or failing to take measures following the withdrawal of consent pursuant to the proviso of paragraph (3), the personal information controller shall notify the data subject of the reason without delay. <Amended on Mar. 14, 2023>

(5) 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. <Amended on Mar. 14, 2023>

(6) Matters necessary for the methods and procedures to request the suspension of processing, to withdraw consent, to reject such request, and to give notification, etc. pursuant to paragraphs (1) through (5) shall be prescribed by Presidential Decree. <Amended on Mar. 14, 2023>

Article 37-2 (Rights of Data Subjects for Automated Decision) (1) If a decision (excluding an automatic disposition by an administrative authority under Article 20 of the Framework Act on Administration; hereafter in this Article referred to as "automated decision") made by processing personal information with a completely automated system (including a system to which artificial intelligence technologies are applied) has a significant effect on his or her right or duty, a data subject shall have the right to file with the relevant personal information controller an objection against the relevant decision: Provided, That this shall not apply to cases where automated decisions are made pursuant to Article 15 (1) 1, 2, and 4.

(2) A data subject may, if the personal information controller has made an automated decision, request explanation, etc. thereof.

(3) Where a data subject refuses to accept an automated decision or requests a personal information controller to provide explanations, etc. thereof pursuant to paragraph (1) or (2), the personal information controller shall not apply the automated decision unless there is a compelling reason not to do so, or shall take necessary measures, such as re-

processing through human involvement and providing explanations.

(4) A personal information controller shall disclose the criteria and procedures for making automated decisions and the methods, etc. of processing personal information so that data subjects can easily confirm them.

(5) Except as provided in paragraphs (1) through (4), matters necessary for the procedures and methods for refusing to accept automated decisions, requesting explanations, etc. thereof, necessary measures in response to refusal, a request for explanations, etc., the criteria and procedures for making automated decisions, the disclosure of the method in which personal information is processed, etc. shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Mar. 14, 2023]

Article 38 (Methods and Procedures for Exercise of Rights) (1) A data subject may authorize his or her representative to file requests for access under Article 35, transmission under Article 35-2, rectification or erasure under Article 36, suspension of processing and withdrawal of consent under Article 37, and refusal and requests for explanation, etc. under Article 37-2 (hereinafter referred to as "request for access, etc.") by the methods and procedures prescribed by Presidential Decree, such as written documents. <Amended on Feb. 4, 2020; Mar. 14, 2023>

(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 charge a person who files a request for access, etc. a fee and postage (only in cases of a request to mail the copies), as prescribed by Presidential Decree: Provided, That in cases of a request for transmission under Article 35-2 (2), the personal information controller may assess a fee, taking into account additional facilities necessary for transmission and other factors as well. <Amended on Mar. 14, 2023>

(4) A personal information controller shall prepare detailed methods and procedures to enable data subjects to file requests for access, etc., and disclose such methods and procedures so that the data subjects may become aware of them. In such cases, the methods and procedures for filing requests for access, etc. shall be no more difficult than the methods and procedures for the collection of the relevant personal information. <Amended on Mar. 14, 2023>

(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 (Liability for Damages) (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 absence of intention or negligence.

(2) Deleted. <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 intention or negligence of a personal information controller, the Court may determine the amount of compensation for damage not exceeding five times such damage: Provided, That the same shall not apply to the personal information controller who has proved the absence of intention or negligence. <Newly Inserted on Jul. 24, 2015; Mar. 14, 2023>

(4) The Court shall take into account the following when determining the amount of compensation for damage under paragraph (3): <Newly Inserted on Jul. 24, 2015>

1. The degree of intention 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 intention 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 the absence of intention 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.

[This Article Newly Inserted on Jul. 24, 2015]

CHAPTER VI Deleted

Article 39-3 (Submission of Data) (1) In a lawsuit seeking damages resulting from an act in violation of this Act, the court may, upon a request of a party, order the other party to prove the damage or to submit data necessary for the calculation of the amount of damages: Provided, That this shall not apply if the person upon receipt of an order to submit data has good cause for refusing to do so.

(2) Where a person upon receipt of an order to submit data under paragraph (1) asserts that there is good cause for refusing to do so, the court may order the presentation of data in order to determine propriety of such assertion. In such cases, the court shall not allow others to view the data.

(3) Even if the data to be submitted under paragraph (1) are trade secrets under subparagraph 2 of Article 2 of the Unfair Competition Prevention and Trade Secret Protection Act (hereinafter referred to as "trade secrets"), if the data are absolutely necessary in proving damage or calculating the amount of damages, it shall not be deemed that there is good cause under the proviso of paragraph (1). In such cases, the court shall determine the scope of access or persons allowed access within the purpose of the submission order.

(4) Where the party upon receipt of an order to submit data under paragraph (1) fails to comply with the order without good cause, the court may recognize that the claim of the

applicant on the description of data is true.

(5) In cases falling under paragraph (4), where the applicant who has requested the submission of data is in a considerably difficult situation to make a detailed assertion on the description of data and where it is also impractical to expect that other evidence would verify the facts to be proved by the data, the court may recognize that the claim of the applicant on the facts which he or she intends to verify through the description of the data is true.

[This Article Wholly Amended on Mar. 14, 2023]

Article 39-4 (Confidentiality Order) (1) In a lawsuit seeking damages resulting from an act in violation of this Act, the court may order the following persons not to use the trade secrets held by the party for any purpose other than proceeding with the relevant lawsuit, by a decision upon the request of a party, or not to disclose to persons other than those who have received an order under this paragraph: Provided, That this shall not apply where the following persons have already acquired the trade secrets by means other than the perusal to briefs or the examination of evidence as of the time the application is filed:

1. The other party (referring to the representative in the case of a corporation);
2. A person who represents the party in the relevant lawsuit;
3. Any other person who has become aware of the trade secrets through the lawsuit.

(2) A person who applies for an order under paragraph (1) (hereinafter referred to as "confidentiality order") shall account for all of the following points:

1. The trade secret is contained in briefs already submitted or to be submitted, evidence already examined or to be examined, or data submitted or to be submitted pursuant to Article 39-3 (1);
2. The trade secrets referred to in subparagraph 1, if used or disclosed for purposes other than for conducting said litigation, are likely to impede the business operation of the relevant party, so that it is required to place a restriction on the use or disclosure of such trade secrets in order to prevent the impediment.

(3) An application for a confidentiality order shall be made in writing stating the following:

1. A person who will be subject to the confidentiality order;
2. The facts sufficient to specify the trade secrets to be protected by the confidentiality order;

3. Facts falling under the subparagraphs of paragraph (2).

(4) Where a decision is made to issue a confidentiality order, the court shall serve the written decision on the person to whom the confidentiality order is to be issued.

(5) A confidentiality order shall take effect when the written decision referred to in paragraph (4) is served on the person subject to the confidentiality order.

(6) An immediate appeal may be filed against a judgment that dismisses, with or without prejudice, an application for a confidentiality order.

[This Article Wholly Amended on Mar. 14, 2023]

Article 39-5 (Revocation of Confidentiality Order) (1) Where there are facts or circumstances that do not correspond to the points in the subparagraphs of Article 39-4 (2), the person who has applied for a confidentiality order or the person who has received a confidentiality order may request the court that keeps the litigation records (if there is no court keeping the records, it refers to the court that issued the confidentiality order) to revoke the confidentiality order.

(2) When a court makes a decision on a request to revoke a confidentiality order, it shall serve a written decision on the applicant for request and the other party.

(3) An immediate complaint may be raised against a decision on revocation of a confidentiality order.

(4) A decision to revoke a confidentiality order shall take effect when it becomes final and conclusive.

(5) When a court decides to revoke a confidentiality order, it shall immediately notify a person to whom a confidentiality order of the relevant trade secret was issued, if any, of the fact that a decision is made to revoke the confidentiality order, in addition to the applicant for request to revoke the confidentiality order and the other party.

[This Article Wholly Amended on Mar. 14, 2023]

Article 39-6 (Notification of Request for Perusal of Litigation Records) (1) Where a decision under Article 163 (1) of the Civil Procedure Act has been rendered for litigation records regarding lawsuit proceedings for which a confidentiality order had been issued (excluding lawsuit proceedings for which any and all confidentiality orders have been revoked), and the party has made a request for perusal, etc. of confidential records prescribed in that paragraph but the procedures for such request have been followed by a person not

subject to a confidentiality order in the lawsuit at issue; a court official of Grade IV, V, VI, or VII (hereafter in this Article referred to as "court official of Grade V, etc.") shall notify the party who has made a request under that paragraph (excluding a person who has made the aforementioned request for perusal, etc.; hereafter in paragraph (3), the same shall apply) of the fact that the request for perusal, etc. was made immediately after the request.

(2) No court official of Grade V, etc. shall allow a person who has followed the procedures for the request for perusal, etc. to peruse the confidential records under paragraph (1) until two weeks have elapsed from the date the request under paragraph (1) was made (referring to the time when a judgment on the request becomes final and conclusive, if a request for issuing a confidentiality order to a person who has followed the request procedures is made within the period).

(3) Paragraph (2) shall not apply where all the parties who have filed a request under Article 163 (1) of the Civil Procedure Act give their consent to permitting a person who has made a request for perusal, etc. under paragraph (1) to peruse, etc. the confidential records under paragraph (1).

[This Article Wholly Amended on Mar. 14, 2023]

Article 39-7 (Coverage of Liabilities for Damages) (1) A personal information controller that meets the criteria prescribed by Presidential Decree in consideration of sales and the scale of personal information retained shall take necessary measures such as purchasing insurance or joining a mutual aid organization or accumulating reserves to meet its liabilities for damages under Articles 39 and 39-2. <Amended on Mar. 14, 2023>

(2) Notwithstanding paragraph (1), any of the following need not take measures provided in paragraph (1): <Amended on Mar. 14, 2023>

1. A public institution, non-profit corporation, or organization prescribed by Presidential Decree;
2. A person who entrusts the processing of personal information to a person prescribed by Presidential Decree, who is a micro enterprise defined in Article 2 (1) of the Framework Act on Micro Enterprises;
3. A personal information controller that has purchased insurance or joined a mutual aid organization, or accumulated reserves pursuant to other statutes to cover liabilities for damages under Articles 39 and 39-2.

(3) Matters necessary for the criteria for meeting liabilities for damages, etc. under paragraphs (1) and (2) shall be prescribed by Presidential Decree. <Newly Inserted on Mar. 14, 2023>

[This Article Newly Inserted on Feb. 4, 2020]

[Moved from Article 39-9; previous Article 39-7 deleted <Mar. 14, 2023>]

CHAPTER VII PERSONAL INFORMATION DISPUTE MEDIATION COMMITTEE

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 composed of up to 30 members, including one chairperson, and the members shall be ex officio members and commissioned members. <Amended on Jul. 24, 2015; Mar. 14, 2023>

(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 on Mar. 23, 2013; Nov. 19, 2014; 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 on Mar.

23, 2013; Nov. 19, 2014; 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 on 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 such cases, 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 business affairs necessary for dispute mediation, such as receiving dispute mediation cases and fact-finding. <Amended on Jul. 24, 2015>

(9) Except as provided 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 of, Challenge to, or Recusal, of Members) (1) A member of the Dispute Mediation Committee shall be excluded from deliberation and resolution on 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 or her current or former spouse is a party to the case or is a joint right holder or a joint obligor 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 the circumstances indicate that it would be impracticable to expect fair deliberations and resolution by a Committee member, any party may file a motion for challenge to the chairperson. In such cases, the chairperson shall determine whether or not to accept the motion without referring the motion to the Dispute Mediation Committee for resolution.

(3) Where any committee member falls under the case of paragraph (1) or (2), he or she may recuse himself or herself from deliberation and resolution on the case in question.

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 personal information controller is notified of dispute mediation under paragraph (2), he or she shall respond to it unless there is a compelling reason not to do so. <Amended on Mar. 14, 2023>

Article 44 (Time Limitation of Mediation Proceedings) (1) The Dispute Mediation Committee shall examine the case and prepare a proposal of mediation 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 of 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 (Requests for Materials and Fact-Finding Investigation) (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 in the absence of good cause.

(2) Where it is necessary to verify facts for the mediation of a dispute, the Dispute Mediation Committee may require members of the Dispute Mediation Committee or public

officials belonging to the secretariat prescribed by Presidential Decree to enter the place related to the case and to investigate or inspect relevant data. In such cases, where any party to the relevant dispute has good cause for refusing the relevant investigation or inspection, he or she may refuse the investigation or access by explaining such grounds therefor. <Newly Inserted on Mar. 14, 2023>

(3) A public official who performs his or her duties pursuant to Article 2 shall carry identification verifying his or her authority and present it to relevant persons. <Newly Inserted on Mar. 14, 2023>

(4) If deemed necessary to mediate a dispute, the Dispute Mediation Committee may request relevant agencies, etc. to provide necessary cooperation, such as the submission of materials or opinions. <Newly Inserted on Mar. 14, 2023>

(5) The Dispute Mediation Committee may summon disputing parties or relevant witnesses to appear before the Committee to hear their opinions, if deemed necessary. <Amended on Mar. 14, 2023>

[Title Amended on Mar. 14, 2023]

Article 45-2 (Restriction on Invoking Statements) Opinions and statements made in mediation proceedings shall not be invoked in a lawsuit (excluding quasi-retrial of the relevant conciliation).

[This Article Newly Inserted on Mar. 14, 2023]

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 proposal of mediation 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 proposal of mediation pursuant to paragraph (1), the Dispute Mediation Committee shall present the proposal of mediation to each party without delay.

(3) If a party presented with the proposal of mediation prepared under paragraph (2) fails to notify the Dispute Mediation Committee of his or her acceptance or denial of the

proposal of mediation within 15 days from the date of receipt of such decision, he or she shall be deemed to have accepted the decision. <Amended on Mar. 14, 2023>

(4) If the parties accept the draft mediation decision (including deemed acceptance under paragraph (3)), the Dispute Mediation Committee shall prepare a written mediation decision and deliver the original copies thereof to each party or his or her agents after the chairperson of the Dispute Mediation Committee and the parties affix their names and seals thereto: Provided, That in cases of deemed acceptance under paragraph (3), the names, seals, and signatures of each party may be omitted. <Amended on Mar. 14, 2023>

(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 improper 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 provided 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 provided 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 50-2 (Notification of Opinion for Improvement) The Dispute Mediation Committee may notify the Protection Commission and the heads of relevant central administrative agencies of its opinions for the improvement of the protection of personal information and the protection of the rights of data subjects in connection with the performance of the work under its jurisdiction.

[This Article Newly Inserted on Mar. 14, 2023]

CHAPTER VIII CLASS-ACTION LAWSUIT OVER DATA INFRINGEMENT

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 1,000;
   (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 three years;
   (c) The number of regular members shall be at least 5,000;
   (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 by intention 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.

CHAPTER IX SUPPLEMENTARY PROVISIONS

Article 58 (Partial Exclusion from Application) (1) Chapter III through VIII shall not apply to any of the following personal information: <Amended on Mar. 14, 2023>

1. Deleted; <Mar. 14, 2023>
2. Personal information collected or requested to be provided for the analysis of information related to national security;
3. Deleted; <Mar. 14, 2023>
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, 22-2, 27 (1) and (2), 34, and 37 shall not apply to any personal information that is processed by means of the fixed visual data processing devices installed and operated at open places pursuant to the subparagraphs of Article 25 (1). <Amended on Mar. 14, 2023>

(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.
[This Article Newly Inserted on Feb. 4, 2020]

Article 59 (Prohibited Activities) Anyone who processes or has processed personal information shall be prohibited from engaging in any of the following activities: <Amended on Mar. 14, 2023>

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

Article 60 (Confidentiality) Any person who performs or has performed the following work 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, this shall not apply except as provided in other statutes: <Amended on Feb. 4, 2020; Mar. 14, 2023>

1. Work of the Protection Commission provided in Article 8;
2. Work of designating specialized institutions and duties of specialized institutions under Article 28-3;
3. Certification of personal information protection provided in Article 32-2;
4. Privacy impact assessments provided in Article 33;
5. Work of designating institutions specializing in managing personal information and affairs of such institutions under Article 35-3;
6. Dispute mediation of the Dispute Mediation Committee under Article 40.

[Enforcement Date: Mar. 15, 2024] Subparagraph 5 of Article 60

Article 61 (Presentation of Opinions and Recommendations for Improvement) (1) The Protection Commission may present its opinion to any relevant agency through deliberation and resolution where it is deemed necessary with respect to the statutes or regulations or municipal ordinances containing provisions that are likely to affect the

protection of personal information. <Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; 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 center (hereinafter referred to as the "Privacy Call Center").<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020>

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

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. Work incidental to those under 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; 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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; 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 identification verifying his or her authority and show it to relevant persons.<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015; Jul. 26, 2017; Feb. 4, 2020>

(3) The Protection Commission may request the heads of the following relevant institutions to cooperate in taking prompt and effective measures where any serious personal information breach occurs due to a violation of laws related to the protection of personal information, such as this Act: <Amended on Mar. 14, 2023>

1. Central administrative agencies;

2. A local government;

3. Other public institutions having, delegated or entrusted with, administrative authority pursuant to statutes and regulations or municipal ordinances and rules.

(4) The head of a relevant institution who receives a request for cooperation under paragraph (3) shall comply with such request in the absence of special circumstances. <Amended on Mar. 14, 2023>

(5) Matters necessary for requests for the submission of materials, procedures and methods for inspection, etc. under paragraphs (1) and (2) may be determined and publicly notified by the Protection Commission. <Amended on Mar. 14, 2023>

(6) The Protection Commission shall neither 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 provided in this Act. <Newly Inserted on Feb. 4, 2020; Mar. 14, 2023>

(7) Upon receiving materials via information and communications networks, or digitalizing the collected materials, etc., the Protection Commission shall take systematic and technical supplementary measures to prevent the divulgence of personal information, trade secrets, etc. <Newly Inserted on Feb. 4, 2020; Mar. 14, 2023>

Article 63-2 (Preliminary Fact-Finding Inspections) (1) In cases not falling under the subparagraphs of Article 63 (1), the Protection Commission may inspect the status of protection of personal information of a personal information controller that is highly susceptible to a personal information breach incident and deemed to need a preliminary inspection of vulnerabilities in the protection of personal information.

(2) The Protection Commission may, if it finds any violation of this Act through a fact-finding inspection under paragraph (1), formulate a correction scheme and recommend that the relevant personal information controller comply with it.

(3) Upon receipt of the recommendation for correction under paragraph (2), a personal information controller shall notify the Protection Commission as to whether it accepts the recommendation within 10 days from the date of receipt of the recommendation, and inform the Protection Commission of the results of the implementation thereof, as prescribed by Notification of the Protection Commission.

(4) When any person upon receipt of the recommendation for correction under paragraph (2) accepts the relevant recommendation, he or she shall be deemed to have received an order for corrective measures (referring to a recommendation under Article 64 (3) in cases of central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) under Article 64 (1).

(5) If a person upon receipt of the recommendation for correction under paragraph (2) refuses to accept or fails to comply with the relevant recommendation, the Protection Commission may conduct an inspection under Article 63 (2).

(6) The Protection Commission may inspect the status of personal information protection under paragraph (1) jointly with the head of a relevant central administrative agency. [This Article Newly Inserted on Mar. 14, 2023]

Article 64 (Corrective Measures) (1) The Protection Commission may order a person who violates this Act (excluding central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) to take the following measures: <Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

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

(2) 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 the measures provided in the subparagraphs of paragraph (1). <Amended on Mar. 14, 2023>

(3) 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 that the head of the relevant agency take any of the measures provided in the subparagraphs of paragraph (1). In such cases, upon receiving the recommendation, the agency shall comply therewith unless there is a compelling reason not to do so. <Amended on Mar. 14, 2023>

Article 64-2 (Imposition of Penalty Surcharges) (1) The Protection Commission may impose a penalty surcharge on the relevant personal information controller within the scope not exceeding 3/100 of the total sales, in any of the following cases: Provided, That a penalty surcharge not exceeding two billion won may be imposed in cases prescribed by Presidential Decree where no sales have been made or where it is impracticable to calculate the sales:

1. Where the personal information controller processes personal information, in violation of Article 15 (1), 17 (1), 18 (1) and (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8)), or 19;

2. Where the personal information controller processes personal information of a child under 14 years of age without his or her legal representative's consent, in violation of Article 22-2 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
3. Where the personal information controller processes sensitive information without the data subject's consent, in violation of Article 23 (1) 1 (including where it is applied mutatis mutandis pursuant to Article 26 (8));
4. Where the personal information controller processes personally identifiable information or resident registration numbers, in violation of Articles 24 (1) and 24-2 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
5. Where the personal information controller neglects its management, supervision, or education under Article 26 (4), thereby causing the person entrusted to violate this Act;
6. Where the personal information controller processes information to uniquely identify an individual (including where it is applied mutatis mutandis pursuant to Article 26 (8)) in violation of Article 28-5 (1);
7. Where the personal information controller makes cross-border transfers of personal information, in violation of Article 28-8 (1) (including where it is applied mutatis mutandis pursuant to Articles 26 (8) and 28-11);
8. Failing to comply with an order to suspend a cross-border transfer, in violation of Article 28-9 (1) (including where it is applied mutatis mutandis pursuant to Articles 26 (8) and 28-11);
9. Where the personal information processed by the personal information controller is lost, stolen, divulged, forged, altered, or damaged; Provided, That this shall not apply where a personal information controller has taken all measures necessary to ensure safety under Article 29 (including where it is applied mutatis mutandis pursuant to Article 26 (8)) to prevent personal information from being lost, stolen, divulged, forged, altered, or damaged.

(2) Where the Protection Commission intends to impose a penalty surcharge under paragraph (1), it shall calculate the penalty surcharge based on the gross sales net of the sales unrelated to the violation.

(3) Where the Protection Committee intends to impose a penalty surcharge pursuant to paragraph (1), it may calculate the sales based on the gross sales of the personal information controller if the personal information controller refuses to submit sales

calculation data or submits false data without good case: Provided, That it may presume sales based on the scale of personal information retained, accounting data such as financial statements, prices of products and services, and other data regarding the business state of a personal information controller with a size similar to that of the relevant personal information controller.

(4) The Protection Commission shall, where it imposes a penalty surcharge under paragraph (1), take into account the following matters to ensure that the penalty surcharge shall be proportional to the violation and be effective in preventing breach:

1. The details and degree of a violation;
2. The duration and frequency of violations;
3. Scale of profits derived from a violation;
4. Efforts to take measures to ensure safety, such as encryption;
5. Where the personal information is lost, stolen, divulged, forged, altered, or damaged, the relation to the violation and the scale of loss, theft, divulgence, forgery, alteration, or damage;
6. Whether measures for recovering from damage and preventing the spread of damage have been taken;
7. The type and volume of work of the personal information controller;
8. Types of personal information processed by a personal information controller and the impact on data subjects;
9. The amount of damage caused by the violation;
10. Efforts for the protection of personal information, including the certification of personal information protection and autonomous protection activities;
11. Whether measures have been taken to rectify violations, including cooperation with the Protection Commission.

(5) The Protection Commission need not impose a penalty surcharge in any of the following cases:

1. Where the person subject to the penalty surcharge is objectively deemed unable to pay the penalty surcharge due to insolvency, suspension of payment, capital impairment, etc.;
2. Where there is good cause for the person subject to the penalty surcharge to mistakenly believe that his or her conduct is not illegal;

3. Where the details and degree of the violation are minor or where the assessed penalty surcharge is small;
4. Where any ground prescribed by Presidential Decree exists, on which the data subject has suffered no or minor damage.

(6) Penalty surcharges under paragraph (1) shall be calculated in consideration of paragraphs (2) through (5), but the detailed calculation criteria and procedures shall be prescribed by Presidential Decree.

(7) If the person subject to the penalty surcharge under paragraph (1) fails to pay it by the payment deadline, the Protection Commission shall collect the additional charge equivalent to 6/100 per annum of the unpaid penalty surcharge from the date following the payment deadline. In such cases, the period for collecting of the additional charge shall not exceed 60 months.

(8) Where a person liable to pay a penalty surcharge under paragraph (1) fails to pay it by the payment deadline, the Protection Commission shall demand payment thereof within a specified period; and where the penalty surcharges and additional charges under paragraph (7) are not paid within the specified period, the Protection Commission shall collect such penalty surcharges in the same manner as national taxes are compulsorily collected.

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

(10) Notwithstanding paragraph (9), when a disposition to impose penalty surcharges is revoked due to a court's decision and new penalty surcharges are imposed based on the reasoning of the decision, additional refunds shall be calculated and paid only with respect to the amount that remains after the newly imposed penalty surcharges are deducted from the penalty surcharges already paid.

[This Article Newly Inserted on Mar. 14, 2023]

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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; 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 on Mar. 23, 2013; Aug. 6, 2013; Nov. 19, 2014; Jul. 26, 2017; 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 (Publication of Results) (1) The Protection Commission may publish the recommendation for improvement under Article 61; the order to take corrective measures under Article 64; the imposition of penalty surcharges under Article 64-2; the accusation or recommendation for a disciplinary action under Article 65; and the imposition of administrative fines under Article 75 and the results thereof. <Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>

(2) Where the Protection Commission makes dispositions such as a recommendation for improvement under Article 61, an order to take corrective measures under Article 64, the imposition of a penalty surcharge under Article 64-2, an accusation or recommendation for a disciplinary action under Article 65, or a disposition to impose an administrative fine under Article 75, it may order the person who has received such disposition to publish the fact of receiving such disposition. <Amended on Mar. 14, 2023>

(3) The method, criteria, procedure, etc. for publishing the fact of receiving a recommendation for improvement, etc. and issuing orders for publication under paragraphs (1) and (2) shall be prescribed by Presidential Decree. <Amended on Mar. 14,

2023>

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 on Mar. 29, 2016; Mar. 14, 2023>

1. Infringement on the rights of data subjects and the status of remedies thereof;
2. Results of fact-finding surveys on personal information processing and the assessments of the level of personal information protection;
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 statutes, 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 measures.

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 on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 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 work delegated or entrusted.
<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; 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 work.<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020>

Article 69 (Persons Deemed to be Public Officials for Purposes of Applying 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 on Feb. 4, 2020>

(2) Any executive or employee of a relevant agency that performs the works entrusted by the Protection Commission or the head of a related central administrative agency shall be deemed a public official for the purposes of applying Articles 129 through 132 of the Criminal Act. <Newly Inserted on Feb. 4, 2020>

CHAPTER X PENALTY PROVISIONS

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 on 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 improper 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 labor for not more than five years, or by a fine not exceeding 50 million won:<Amended on Mar. 29, 2016; Feb. 4, 2020; Mar. 14, 2023>

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 (including where it is applied mutatis

mutandis pursuant to Article 26 (8)) 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 Article 18 (1) and (2), 27 (3), 28-2 (including where it is applied mutatis mutandis pursuant to Article 26 (8)), 19, or 26 (5) and a person who knowingly receives such personal information for a profit-making or improper purposes;
3. A person who collects personal information of a child under 14 years of age without his or her legal representative's consent, in violation of Article 22-2 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
4. A person who processes sensitive information, in violation of Article 23 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
5. A person who processes personally identifiable information, in violation of Article 24 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
6. A person who consolidates pseudonymized information without having been designated as a specialized institution by the Protection Commission or the head of a relevant central administrative agency, in violation of Article 28-3 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
7. A person who transfers combined information to outside the institution that has performed the combination without obtaining approval therefor from the head of the specialized institution, or provides a third party with such information, in violation of Article 28-3 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8)), or a person who knowingly receives such combined information for profit-making or improper purposes;
8. A person who processes pseudonymized information for the purpose of uniquely identifying an individual, in violation of Article 28-5 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
9. A person who divulges personal information acquired in the course of performing his or her work 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 improper purposes;
10. A person who uses, damages, destroys, alters, forges, or divulges any other person'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 three years, or by a fine not exceeding 30 million won: <Amended on Mar. 14, 2023>

1. A person who arbitrarily manipulates a fixed visual data processing device for purposes other than those for which the device was installed, directs such device toward different spots, or uses sound recording functions, in violation of Article 25 (5) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
2. A person who acquires personal information or obtains consent to personal information processing by fraud or other improper means in violation of subparagraph 1 of Article 59, and a person who knowingly receives such personal information for a profit-making or improper 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 or her duties in violation of Article 60.

Article 73 (Penalty Provisions) (1) Any of the following persons shall be punished by imprisonment with labor for not more than two years or by a fine not exceeding 20 million won:

1. A person who fails to take necessary measures, such as correction and erasure, in violation of Article 36 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8)), and keeps on using the personal information or provides it to a third party;
2. A person who fails to suspend the processing of personal information, in violation of Article 37 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8)), and keeps on using the personal information or provides it to a third party;
3. Any person who fails to comply with a confidentiality order under Article 39-4 in or outside Korea without good cause;
4. A person who refuses to submit materials or submits false materials in response to a request for the submission of materials under Article 63 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8)) for the purpose of concealing or understating violations of the Act;
5. A person who refuses, obstructs, or evades an investigation by concealing, discarding, or refusing access to, materials, or by forging or falsifying, etc. materials during an entry

and inspection conducted pursuant to Article 63 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8)).

(2) No prosecution against a crime under paragraph (1) 3 shall be instituted without a criminal complaint is filed by a person who has requested a confidentiality order.

[This Article Wholly Amended on Mar. 14, 2023]

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 this shall not apply where such corporation or individual has not been negligent in taking due care and supervisory activities concerning the relevant 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 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.

[This Article Newly Inserted on Jul. 24, 2015]

Article 75 (Administrative Fines) (1) Any of the following persons shall be subject to an administrative fine not exceeding 50 million won:

1. A person who installs and operates a fixed visual data processing device, in violation of Article 25 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
2. A person who takes photographs of a person or thing related to such person with a mobile visual processing device, in violation of Article 25-2 (2) (including where it is

applied mutatis mutandis pursuant to Article 26 (8)).

(2) Any of the following persons shall be subject to an administrative fine not exceeding 30 million won:

1. A person who refuses to provide goods or services, in violation of Article 16 (3) or 22 (5) (including where it is applied mutatis mutandis pursuant to 26 (8));
2. A person who fails to notify a data subject of the facts provided in the subparagraphs of Article 20 (1), in violation of paragraphs (1) or (2) of that Article;
3. A person who fails to notify a data subject of the details of the use and provision of personal information or the method of accessing the information system through which such details can be confirmed, in violation of Article 20-2 (1);
4. A person who fails to take necessary measures, such as destroying personal information, in violation of Article 21 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
5. A person who fails to take measures necessary to ensure safety, in violation of Article 23 (2), 24 (3), or 25 (6) (including where it is applied mutatis mutandis pursuant to Article 25-2 (4)), or Article 28-4 (1), or 29 (including where it is applied mutatis mutandis pursuant to Article 26 (8));
6. A person who fails to communicate to the data subject the possibility of disclosure of sensitive information and the method of selecting non-disclosure, in violation of Article 23 (3) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
7. A person who processes resident registration numbers, in violation of Article 24-2 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
8. A person who fails to take encryption measures, in violation of Article 24-2 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
9. A person who fails to provide data subjects with an alternative sign-up tool without using their resident registration numbers, in violation of Article 24-2 (3) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
10. A person who installs and operates a fixed visual data processing device, in violation of Article 25 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
11. A person who takes photographs of a person or a thing related to such person, in violation of Article 25-2 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));

12. A person who fails to notify a data subject of the matters he or she is required to notify, in violation of Article 26 (3);
13. A person who fails to cease the use of, to retrieve or to destroy, information even if information that can uniquely identify an individual has been generated, in violation of Article 28-5 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
14. A person who fails to take protective measures, in violation of Article 28-8 (4) (including where it is applied mutatis mutandis pursuant to Articles 26 (8) and 28-11);
15. A person who indicates or promotes the details of certification despite a failure to obtain such certification, in violation of Article 32-2 (6);
16. A person who fails to conduct a privacy impact assessment or to submit the results thereof to the Protection Commission, in violation of Article 33 (1);
17. A person who fails to notify a data subject of the facts provided in the subparagraphs of Article 34 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8)), in violation of that paragraph;
18. A person who fails to file a report with the Protection Commission or a specialized institution prescribed by Presidential Decree, in violation of Article 34 (3) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
19. A person who limits or denies access, in violation of Article 35 (3) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
20. A person who performs work under Article 35-3 (1) 2 without obtaining designation under that paragraph;
21. A person who violates Article 35-3 (3);
22. A person who fails to take necessary measures, such as correction or erasure, in violation of Article 36 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
23. A person who fails to take necessary measures, such as destruction, in violation of Article 37 (3) or (5) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
24. A person who fails to comply with a request by a data subject without good cause, in violation of Article 37-2 (3) (including where it is applied mutatis mutandis pursuant to Article 26 (8));

25. Any person who fails to submit or falsely submits materials, including articles and documents related thereto under Article 63 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
26. A person who refuses, obstructs, or evades an entry and inspection, in violation of Article 63 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
27. A person who fails to comply with an order to take corrective measures under Article 64 (1).

(3) Any of the following persons shall be subject to an administrative fine not exceeding 20 million won:

1. A person who re-entrusts a third party with entrusted work without consent of the person entrusting, in violation of Article 26 (6);
2. A person who fails to designate a domestic agent, in violation of Article 31-2 (1).

(4) Any of the following persons shall be subject to an administrative fine not exceeding 10 million won:

1. A person who fails to submit materials without good cause or who submits false materials, in violation of Article 11-2 (2);
2. A person who fails to separately store and manage personal information, in violation of Article 21 (3) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
3. A person who obtains consent, in violation of Article 22 (1) through (3) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
4. A person who, when entrusting work, fails to do so in a document stating the matters provided in Article 26 (1), in violation of that paragraph;
5. A person who fails to disclose the entrusted work and the person entrusted in violation of Article 26 (2);
6. A person who fails to notify the data subject of the fact of transfer of personal information, in violation of Article 27 (1) or (2) (including where it is applied mutatis mutandis pursuant to 26 (8));
7. A person who fails to prepare and retain relevant records, in violation of Article 28-4 (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
8. A person who fails to establish or disclose, the Privacy Policy, in violation of Article 30 (1) or (2) (including where it is applied mutatis mutandis pursuant to Article 26 (8));

9. A person who fails to designate a privacy officer, in violation of Article 31 (1) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
10. A person who fails to notify a data subject of the matters he or she is required to notify, in violation of Article 35 (3) and (4), 36 (2) and (4), or 37 (4) (including where it is applied mutatis mutandis pursuant to Article 26 (8));
11. A person who fails to submit materials provided in Article 45 (1) without good cause or who submits false materials;
12. A person who refuses, obstructs, or evades an entry, inspection, or access under Article 45 (2), without good cause.

(5) The Protection Commission shall impose and collect administrative fines under paragraphs (1) through (4), as prescribed by Presidential Decree. In such cases, the Protection Commission may reduce or exempt administrative fines based on the degree of, motives for, and consequences of the violation, the size of the personal information controller, etc.

[This Article Wholly Amended on Mar. 14, 2023]

[Enforcement Date: Mar. 15, 2024] Article 75 (2) 16, 20, 21, and 24, and Article 75 (4) 1 and 9

Article 76 (Special Exemption to Application of Provisions on Administrative Fines) For the purposes of applying the provisions governing administrative fines provided in Article 75, no additional administrative fine shall be imposed for any act subject to penalty surcharges pursuant to Article 64-2. <Amended on Mar. 14, 2023>

[This Article Newly Inserted on Aug. 6, 2013]