PERSONAL INFORMATION PROTECTION ACT

Established by Act No. 10465, March 29, 2011
Amended by Act No. 11690, March 23, 2013
Amended by Act No. 11990, August 6, 2013
Amended by Act No. 12504, March 24, 2014
Amended by Act No. 12844, November 19, 2014
Amended by Act No. 13423, July 24, 2015

CHAPTER I. GENERAL PROVISIONS

Article 1 (Purpose)

The purpose of this Act is to provide for the processing and protection of the personal information for the purpose of enhancing the right and interest of individuals, and further realizing the dignity and value of the individuals. <*Amended Mar. 24, 2014*>

Article 2 (Definitions)

The terms used herein shall be defined as follows: <*Amended Mar. 24, 2014*>

1. "Personal information" shall mean the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information);
2. "Processing" shall mean the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, retrieval, correction, recovery, use, provision, disclosure and destruction of personal information and other similar activities;
3. "Data subject" shall mean the natural person who is identifiable by the information processed hereby to become the subject of such information;
4. "Personal information file" shall mean a set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy access to the personal information;
5. "Personal information controller"[1] shall mean a public institution, legal person, organization, individual, etc. that processes directly or indirectly personal information to operate personal information files for official or business purposes;
6. "Public institution" shall mean the institution stated in the following Items; and
   a. The administrative bodies of the National Assembly, the Court, the Constitutional Court and the National Election Commission, the central administrative departments or agencies (including those under the Presidential Office and the Prime Minister's Office)

1) The term "personal information processor" of the Act shall read as "personal information controller" in line with EU Directive, which differentiates the "data processor" from the "data controller".

and their affiliated bodies, and local governments; and

b. Other national institutions and public entities which are designated by the Presidential Decree.

7. "Visual data processing devices" shall mean the devices installed continuously at a certain place to take pictures of a person or image of things, or transmit such pictures via wired or wireless networks, which are designated by the Presidential Decree.

Article 3 (Personal Information Protection Principles)

(1) The personal information controller shall make the personal information processing purposes explicit and specified, and shall collect minimum personal information lawfully and fairly to the extent necessary for such purposes.

(2) The personal information controller shall process personal information compatibly to the extent necessary to attain the personal information processing purposes, and shall not use beyond such purposes.

(3) The personal information controller shall ensure the personal information accurate, complete and up to date to the extent necessary to attain the personal information processing purposes.

(4) The personal information controller shall manage personal information in a safe way according to the personal information processing methods, types, etc. in consideration of the possibility that the data subject rights are infringed upon and the degree of such risks.

(5) The personal information controller shall make public its privacy policy and other personal information processing matters, and shall guarantee the data subject rights including the right to access to his/her personal information.

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

(7) The personal information controller shall make efforts to process personal information in anonymity, if possible.

(8) The personal information controller shall make efforts to obtain trust of data subjects by observing and carrying out such duties and responsibilities as stated in this Act and other related laws and regulations

Article 4 (Rights of Data Subject)

The data subject shall, in relation to the processing of his/her own personal information, have the rights stated in the following subparagraphs:

1. The right to be informed of the processing of such personal information;
2. The right to consent or not, and to elect the scope of consent, to the processing of such personal information;
3. The right to confirm the processing of such personal information, and to demand access (including the issuance of certificate, hereinafter the same applies) to such personal

information;

4. The right to suspend processing of, and to make correction, deletion and destruction of such personal information; and
5. The right to appropriate redress for any damage arising out of the processing of such personal information in a prompt and fair procedure.

Article 5 (Obligations of the State, etc.)

(1) The state and local governments shall devise policies to prevent harmful consequences of beyond-purpose collection, abuse and misuse of personal information, indiscrete surveillance and pursuit, etc. and to enhance the dignity of human beings and individual privacy.

(2) The state and local governments shall work out policy measures, including the improvement of legislation, necessary to protect the rights of data subject as stated in Article 4.

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

(4) The state and local governments shall conform any enactment or amendment of laws, regulations or ordinances relating to the processing of personal information to the purpose of this Act.

Article 6 (Relation with Other Acts)

The data protection shall be governed by this Act, except as specifically provided in other laws.

CHAPTER II. ESTABLISHMENT OF DATA PROTECTION POLICIES, ETC.

Article 7 (Personal Information Protection Commission)

(1) The Personal Information Protection Commission (hereinafter referred to as the "Commission") shall be established under the Presidential Office to deliberate and resolve the matters regarding data protection. The Commission shall independently conduct the functions belonging to its authority

(2) The Commission shall consist of not more than 15 Commissioners, including one Chairperson and one Standing Commissioner, who shall be a public official in political service.

(3) The Chairperson shall be commissioned by the President from among non-public official Commissioners.

(4) The Commissioners shall be appointed or commissioned by the President from among the persons stated in any of the following subparagraphs. In this case, five Commissioners

shall be appointed or commissioned from among the candidates elected by the National Assembly, and other five Commissioners from among the candidates designated by the Chief Justice of the Supreme Court:

1. Persons recommended by privacy-related civic organizations or consumer groups;
2. Persons recommended by the trade associations composed of personal information controllers; and
3. Other persons who have ample academic knowledge and experiences related with personal information.

(5) The term of office for the Chairperson and Commissioners shall be three years, and their term of office may be only once extended.

(6) The meeting of the Commission shall be convened by the Chairperson when the Chairperson deems it necessary or more than one quarter of Commissioners demand it.

(7) The resolution of the meeting of the Commission shall be made by the affirmative votes of the majority of present Commissioners if more than half of the Commissioners are present at the meeting.

(8) A secretariat shall be established within the Commission to support the administration of the Commission.

(9) Other matters than those provided from paragraphs (1) through (8), necessary to the organization and operation of the Commission, shall be stated by the Presidential Decree.

Article 8 (Functions, etc. of the Commission)

(1) The Commission shall deliberate and resolve the following matters: *<Amended Jul. 24, 2015; Effective Jul. 25, 2016>*

1. Matters regarding the assessment of data breach incident factors under Article 8-2;

1-2. The Basic Plan under Article 9 and the Implementation Plan under Article 10;

2. Matters for the improvement of policies, systems and legislation related with data protection;
3. Matters for the coordination of positions taken by public institutions with respect to the processing of personal information;
4. Matters regarding the interpretation and operation of laws and regulations related with data protection;
5. Matters regarding the use and provision of personal information under Article 18(2)v;
6. Matters regarding the result of the Privacy Impact Assessment under Article 33(3);
7. Matters regarding the suggestion of opinion under Article 61(1);
8. Matters regarding the advice of measures under Article 64(4);
9. Matters regarding the disclosure of results under Article 66;
10. Matters regarding the making and submission of the Annual Report under Article 67(1);
11. Matters referred to the meeting by the President, the Chairperson of the Commission or more than two Commissioners with respect to data protection; and

12. Other matters to be deliberated and resolved by the Commission under this Act or other laws and regulations.

(2) The Commission may, if necessary for the deliberation and resolution of matters stated in paragraph (1), take measure of the following subparagraphs: *<Amended Jul. 24, 2015>*

1. Listening to the opinions of relevant public officials, specialists in data protection, civic organizations and related operators; and
2. Request of relevant materials from the authorities concerned or inquiry of facts.

(3) The authorities concerned which have been requested under paragraph (2) 2 shall respond to it except otherwise exempted by special circumstances. *<Newly Inserted Jul. 24, 2015>*

(4) The Commission may, in case of deliberation and resolution of matters subject to paragraph (1) 2, advise such improvement to the relevant organization. *<Newly Inserted Jul. 24, 2015>*

(5) The Commission may inspect whether its advice pursuant to paragraph (4) has been implemented or not. *<Newly Inserted Jul. 24, 2015>*

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

(1) The head of central administrative departments shall request the Commission to assess the data breach incident factors in case where the policy or system in need of personal information processing is adopted or changed by the enactment or amendment of the Act or subordinate statutes under its jurisdiction.

(2) When receiving the request pursuant to paragraph (1), the Commission may, upon the analysis and review of the data breach incident factors of the Act or subordinate statutes concerned, recommend the necessary matters for the improvement of such Act or subordinate statutes to the head of relevant departments concerned.

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

[*This Article Newly Inserted Jul. 24, 2015; Effective Jul. 25, 2016*]

Article 9 (Basic Plan)

(1) The Commission shall establish the Data Protection Basic Plan (hereinafter referred to as the "Basic Plan") every three years in consultation with the head of central administrative department or agency concerned to ensure the protection of personal information and the rights and interest of data subjects. *<Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015; Effective Jul. 25, 2016>*

(2) The Basic Plan shall include the followings:

1. The basic goals and intended directions of data protection;
2. The improvement of data protection systems and legislation;
3. Countermeasures to prevent privacy violation;
4. How to facilitate self-regulation for data protection;

5. How to activate education and public relations for data protection;
6. Training and fostering specialists in data protection; and
7. Other matters necessary for data protection.

(3) The National Assembly, the Court, the Constitutional Court and the National Election Commission may establish and implement its own basic plan for data protection of relevant institutions including affiliated entities.

Article 10 (Implementation Plan)

(1) The head of central administrative department or agency shall establish the implementation plan for data protection each year in accordance with the Basic Plan and submit it to the Commission, and shall carry out the implementation plan subject to the deliberation and resolution of the Commission.

(2) The matters necessary for the establishment and carrying out of the implementation plan shall be stated by the Presidential Decree.

Article 11 (Request, etc. for Materials)

(1) The Commission may, for the efficient establishment of the Basic Plan, request materials or suggestions regarding the actual state of regulatory compliance and personal information management, etc. by personal information controllers from personal information controllers, the head of central administrative department or agency concerned, the head of local governments and relevant organizations or associations, etc. *<Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015; Effective Jul. 25, 2016>*

(2) The Minister of Interior[2] may conduct a survey of the level of personal information protection and actual status toward personal information controllers, the head of central administrative department or agency concerned, the head of local governments and relevant organizations or associations, etc. if necessary for carrying out personal information protection policy and assessment of the outcome, etc. *<Newly Inserted Jul. 24, 2015>*

(3) The head of central administrative department or agency may, for the efficient establishment and carrying out of the implementation plan, request the materials stated in paragraph (1) from personal information controllers in the field under its jurisdiction. *<Amended Jul. 24, 2015>*

(4) Any person who has been requested to furnish the materials under paragraphs (1) through (3) shall do as requested except otherwise exempted by special circumstances. *<Amended Jul. 24, 2015>*

(5) Any necessary matters including the scope and method to furnish the materials under paragraphs (1) through (3) shall be stated by the Presidential Decree. *<Amended Jul. 24, 2015>*

---

2) Previously it was called the Minister of General Administration and Home Affairs (MOGAHA) or the Minister of Security and Public Administration (MOSPA).

Article 12 (Data Protection Guidelines)

(1) The Minister of Interior may establish the standard data protection guidelines (hereinafter referred to as the "Standard Guidelines") regarding the personal information processing standard, types of privacy violations and preventive measures, etc., and encourage personal information controllers to comply with it.

(2) The head of central administrative department or agency may establish the data protection guidelines regarding the personal information processing in the field under its jurisdiction, and encourage personal information controllers to comply with it.

(3) The National Assembly, the Court, the Constitutional Court and the National Election Commission may establish and implement its own data protection guidelines of relevant institutions including affiliated entities.

Article 13 (Promotion and Support of Self-Regulation)

The Minister of Interior shall work out the following policy measures necessary to promote and support the self-regulating data protection activities of personal information controllers:

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

Article 14 (International Cooperation)

(1) The government shall work out policy measures necessary to enhance the data protection standard in the international environment.

(2) The government shall work out relevant policy measures so that the rights of data subjects may not be infringed upon owing to cross border transfer of personal information.

CHAPTER III. PROCESSING OF PERSONAL INFORMATION

Section 1 Collection, Use, Provision, etc. of Personal Information

Article 15 (Collection and Use of Personal Information)

(1) The personal information controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes:

1. Where the consent is obtained from data subjects;

2. Where special provisions exist in laws or it is unavoidable so as to observe legal obligations;
3. Where it is unavoidable so that the public institution may carry out such work under its jurisdiction as prescribed by laws and regulations;
4. Where it is unavoidably necessary so as to execute and perform a contract with data subjects;
5. Where it deems necessary explicitly for the protection, from impending danger, of life, body or economic profits of the data subject or a third party in case that the data subject or his/her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses; or
6. Where it is necessary to attain the justifiable interest of personal information controller, which is explicitly superior to that of data subjects. In this case, it is allowed only when substantial relation exists with the justifiable interest of personal information controller and it does not go beyond the reasonable scope.

(2) The personal information controller shall inform data subjects of the followings when it obtains the consent under subparagraph 1 of paragraph (1). The same shall apply when any of the followings is modified:

1. The purpose of collection and use of personal information;
2. Particulars of personal information to be collected;
3. The period when personal information is retained and used; and
4. The fact which data subjects are entitled to deny consent, and disadvantage affected resultantly from the denial of consent.

Article 16 (Limitation to Collection of Personal Information)

(1) The personal information controller shall collect the minimum personal information necessary to attain the purpose in the case applicable to any subparagraph of Article 15(1). In this case, the burden of proof that the minimum personal information is collected shall be borne by the personal information controller.

(2) The personal information controller shall collect the personal information by informing the data subject of the fact concretely that he/she may deny the consent to the collection of other personal information than the minimum information necessary in case of collecting the personal information by the consent of the data subject. *<Newly Inserted Aug. 6, 2013>*

(3) The personal information controller shall not deny the provision of goods or services to the data subjects on ground that they would not consent to the collection of personal information exceeding minimum requirement.

Article 17 (Provision of Personal Information)

(1) The personal information controller may provide (or share, hereinafter the same applies)

the personal information of data subjects to a third party in the case applicable to any of the following subparagraphs:

1. Where the consent is obtained from data subjects; or
2. Where personal information is provided within the scope of purposes for which personal information is collected under subparagraphs 2, 3 and 5 of Article 15(1);

(2) The personal information controller shall inform data subjects of the followings when it obtains the consent under subparagraph 1 of paragraph (1). The same shall apply when any of the followings is modified:

1. The recipient of personal information;
2. The purpose of use of personal information of the said recipient;
3. Particulars of personal information to be provided;
4. The period when personal information is retained and used by the said recipient; and
5. The fact which data subjects are entitled to deny consent, and disadvantage affected resultantly from the denial of consent.

(3) When the personal information controller provides personal information to a third party overseas, it shall inform data subjects of any of subparagraphs of paragraph (2), and obtain consent from data subjects. The personal information controller shall not enter into a contract for the cross-border transfer of personal information in violation of this Act.

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

(1) The personal information controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3).

(2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, the personal information controller may use personal information for other purpose than the intended one, or provide it to a third party, unless it likely infringes upon unfairly the interest of data subjects or a third party; *provided, however*, that subparagraphs 5 through 9 are applicable only to the public institutions.

1. Where additional consent is obtained from data subjects;
2. Where special provisions exist in laws;
3. Where it deems necessary explicitly for the protection, from impending danger, of life, body or economic profits of the data subject or a third party in case that the data subject or his/her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses;
4. Where personal information is provided in a manner keeping individuals unidentifiable necessarily for the purposes of statistics and academic research, etc.;
5. Where it is impossible to carry out the work under its jurisdiction as stated in other laws unless personal information controller uses personal information for other purpose

than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution of the Commission;

6. Where it is necessary to provide personal information to a foreign government or international organization so as to perform a treaty or other international convention;
7. Where it is necessary for the investigation of crimes, indictment and prosecution;
8. Where it is necessary for the court to proceed the case; or
9. Where it is necessary for punishment, and enforcement of care and custody.

(3) The personal information controller shall inform data subjects of the followings when it obtains the consent under subparagraph 1 of paragraph (2). The same shall apply when any of the followings is modified:

1. The recipient of personal information;
2. The purpose of use of personal information (in case of provision of personal information, it means the purpose of use of the recipient);
3. Particulars of personal information to be used or provided;
4. The period when personal information is retained and used (in case of provision of personal information, it means the period for retention and use by the recipient); and
5. The fact which data subjects are entitled to deny consent, and disadvantage affected resultantly from the denial of consent.

(4) When the public institution uses personal information for other purpose than the intended one, or provides it to a third party under subparagraphs 2 through 6, 8 and 9, the public institution shall post the legal grounds for such use or provision, purpose and scope, and other necessary matters on the Official Gazette or its Website as prescribed by the Ordinance of the Ministry of Interior.

(5) When the personal information controller provides personal information to a third party for other purpose than the intended one in the case applicable to any of subparagraphs of paragraph (2), the personal information controller shall request the recipient of personal information to restrict the purpose and method of use and other necessary matters, or to prepare for necessary safeguards to ensure the safety of personal information. In this case, the person who is requested shall take necessary measures to ensure the safety of personal information.

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

The person who receives personal information from the personal information controller shall not use personal information for other purpose than the intended one, or shall not provide it to a third party except the case applicable to any of the following subparagraphs:

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

Article 20 (Notification of Other Sources, etc. of Personal Information Than Data Subject)

(1) When the personal information controller processes personal information collected from other sources than data subject, the personal information controller shall notify such data subject of everything stated in the following subparagraphs immediately on demand from such data subject:

1. The source of collected personal information;
2. The purpose of processing of personal information; and
3. The fact that a data subject is entitled to demand suspension of the processing of personal information.

(2) paragraph (1) shall not apply to the case where any of the following subparagraphs is applicable; *provided, however*, that it is explicitly superior to the rights of data subjects under this Act.

1. Where personal information, which is the object to demand notification, is included in the personal information files applicable to any of the subparagraphs of Article 32(2); or
2. Where such notification likely causes harm to the life or body of other person, or unfairly damages the properties and other profits of other person.

Article 21 (Destruction of Personal Information)

(1) When the personal information controller shall destroy the personal information without delay when such personal information becomes unnecessary owing to the expiry of retention period, attainment of purpose of personal information processing, etc.; *provided, however*, that the same shall not apply where preservation of it is mandatory by other laws and regulations.

(2) When the personal information controller destroys the personal information under paragraph (1), necessary measures to block recovery or revival shall be taken.

(3) When the personal information controller is obliged to preserve, rather than destroy, the personal information under the proviso of paragraph (1), the relevant personal information or personal information files shall be stored and managed apart from other personal information.

(4) Other necessary matters such as the method to destroy the personal information, its destruction process, etc. shall be stated by the Presidential Decree.

Article 22 (Method to Obtain Consent)

(1) When the personal information controller obtains the consent from the data subjects (including their legal representatives as stated in paragraph (5). Hereinafter the same applies to this Article) with respect to personal information processing under this Act, the personal information controller shall notify the data subjects of the fact by separating the

matters requiring consent and helping the data subjects to recognize it explicitly, and obtain their consent thereof, respectively.

(2) When the personal information controller obtains the consent from the data subjects with respect to personal information processing in accordance with Articles 15(1) i, 17(1) i and 24(1) i, the personal information controller shall segregate the personal information which needs the data subjects' consent to processing, from the personal information which needs no consent in executing a contract with data subjects. In this case, the burden of proof that no consent is required in processing the personal information shall be borne by the personal information controller.

(3) The personal information controller shall, when it intends to obtain the data subjects' consent to personal information processing so as to promote goods and services or solicit purchase hereof, notify the data subjects of the fact by helping the data subjects to recognize it explicitly, and obtain their consent thereof.

(4) The personal information controller shall not deny the provision of goods or services to the data subjects on ground that the data subjects would not consent to the matter eligible for selective consent pursuant to paragraph (2), or would not consent pursuant to paragraph (3) and Article 18(2) i.

(5) The personal information controller shall, when it is required to obtain the consent in accordance with this Act so as to process the personal information of minors of age below 14, obtain the consent from their legal representatives. In this case, the minimum personal information necessary to obtain the consent from legal representatives may be collected directly from such minors without the consent of their legal representatives.

(6) Other matters than those provided from paragraphs (1) through (5), necessary to secure a detailed method to obtain the consent from data subjects and the minimum information pursuant to paragraph (5), shall be stated by the Presidential Decree in consideration of collection media of personal information.

Section 2 Limitation to Processing Personal Information

Article 23 (Limitation to Processing Sensitive Data)

The personal information controller shall not process the personal information (hereinafter referred to as the "sensitive data") including ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life, and other personal information which is likely doing harm to privacy of data subjects, as prescribed by the Presidential Decree; *provided, however*, that the same shall not apply where any of the following subparagraph is applicable:

1. Where the personal information controller informs data subjects of each subparagraph of Articles 15(2) or 17(2), and obtains the consent from data subjects apart from the consent to other personal information processing; or

2. Where laws and regulations require, or permit, the processing of sensitive data.

Article 24 (Limitation to Processing Unique Identifier)

(1) The personal information controller shall not, except the cases stated in the following subparagraphs, process the identifier assigned so as to identify an individual in accordance with laws and regulations, as prescribed by the Presidential Decree (hereinafter referred to as the "Unique Identifier"):

1. Where the personal information controller informs data subjects of each subparagraph of Articles 15(2) or 17(2), and obtains the consent from data subjects apart from the consent to other personal information processing; or
2. Where laws and regulations require, or permit, the processing of the Unique Identifier in a concrete manner.

(2) *Deleted*

(3) In case the personal information controller processes the Unique Identifiers pursuant to each subparagraph of paragraph (1), the personal information controller shall take necessary measures to ensure the safety including encryption, as prescribed by the Presidential Decree, so that such Unique Identifiers may not be lost, stolen, leaked, forged, altered or damaged. *<Amended Jul. 24, 2015>*

(4) *Deleted*

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

(1) Notwithstanding Article 24(1), the personal information controller shall not, except the cases stated in the following subparagraphs, process the resident registration number:

1. Where laws and regulations require or allow processing of the resident registration number in a concrete manner;
2. Where it is deemed explicitly necessary for the impending protection of life, body and interest on property of the data subject or a third person; or
3. Where it is unavoidable to process the resident registration number in line with subparagraphs 1 and 2 subject to the Order of the Ministry of Interior.

(2) Notwithstanding Article 24(3), the personal information controller shall preserve the resident registration numbers in safety by means of encryption so that they may not be lost, stolen, leaked, forged, altered or damaged. In this case, any necessary matters regarding the scope of encryption objects and encryption timing by object, etc. shall be provided by the Presidential Decree in consideration of the volume of data processing and data breach impact, etc. *<Newly Inserted Mar. 24, 2014; Jul. 24, 2015; Effective Jan. 1, 2016>*

(3) The personal information controller shall provide the data subject with effective methods to sign up without using the resident registration number in the stage of being admitted to

membership via the Internet homepage while processing the resident registration number pursuant to each subparagraph of paragraph 1.

(4) The Minister of Interior may prepare and support such measures as legislative arrangements, policy making, necessary facilities and systems build-up in order to support the provision of methods pursuant to paragraph (2).

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

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

(1) No one shall install and operate visual data processing devices at open places except in the cases as stated in the following subparagraphs:

1. Where laws and regulations allow it in a concrete manner;
2. Where it is necessary for the prevention and investigation of crimes;
3. Where it is necessary for the safety of facilities and prevention of fire;
4. Where it is necessary for regulatory control of traffic; or
5. Where it is necessary for the collection, analysis and provision of traffic information.

(2) No one shall install and operate visual data processing devices so as to look into the places which likely threat individual privacy noticeably, such as a bathroom open to the public, toilet, sweating room and dressing room; *provided, however*, that the same shall not apply to the facilities, which detain or protect persons pursuant to laws and regulations, such as a penitentiary, mental health center stated by the Presidential Decree.

(3) The head of public institutions who intends to install and operate visual data processing devices pursuant to each subparagraph of paragraph (1) and the person who intends to install and operate visual data processing devices pursuant to the proviso of paragraph (2) shall gather opinions of relevant specialists and interested persons through such formalities as public hearings, information sessions, etc. stated by the Presidential Decree.

(4) The person who intends to install and operate visual data processing devices pursuant to each subparagraph of paragraph (1) (hereinafter referred to as the “V/D Operator”) shall take necessary measures including posting on a signboard so that data subjects may recognize it with ease as prescribed by the Presidential Decree; *provided, however*, that the same shall not apply to such facilities as prescribed by the Presidential Decree.

(5) The V/D Operator shall not handle arbitrarily visual data processing devices for other purposes than the initial one, nor direct the said devices toward different spots, nor use sound recording functions.

(6) The V/D Operator shall take necessary measures to ensure the safety pursuant to Article 29, so that personal information may not be lost, stolen, leaked, forged, altered or damaged. *<Amended Jul. 24, 2015>*

(7) The V/D Operator shall work out the appropriate policy to operate and manage visual data processing devices as prescribed by the Presidential Decree. In this case, it may be

discharged to make the privacy policy pursuant to Article 30.

(8) The V/D Operator may outsource the installation and operation of visual data processing devices; *provided, however*, that the public institutions considering outsourcing shall comply with the procedure and requirements stated by the Presidential Decree.

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

(1) The personal information controller shall, when it consigns processing of personal information to a third party, go through such paper-based formalities as stated in the following subparagraphs:

1. Prevention of processing personal information for other purposes than the consigned purpose;
2. Technical and managerial safeguards of personal information; and
3. Other things for the safe management of personal information as prescribed by the Presidential Decree.

(2) The personal information controller, that consigns processing of personal information to a third party pursuant to paragraph (1) (hereinafter referred to as the "consignor") shall disclose what has been consigned and who carries out the consigned processing of personal information (hereinafter referred to as the "consignee") so that data subjects may recognize it at any time with ease in such a way as prescribed by the Presidential Decree.

(3) The consignor shall, in case of consigning public relations of goods or services, or soliciting of sales, notify data subjects of the work consigned and the consignee in such a way as prescribed by the Presidential Decree. The same shall apply to cases where the work consigned or the consignee has been changed.

(4) The consignor shall educate the consignee so that personal information of data subjects may not be lost, stolen, leaked, forged, altered or damaged owing to the consignment of work, and supervise how the consignee processes such personal information in a safe manner by inspecting the consigned work of processing and so on as prescribed by the Presidential Decree. *<Amended Jul. 24, 2015>*

(5) The consignee shall not use personal information beyond the scope of work consigned by the personal information controller, nor provide personal information to a third party.

(6) With respect to the compensation of damages arising out of processing personal information consigned to the consignee in violation of this Act, the consignee shall be deemed as an employee of the personal information controller.

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

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

(1) The personal information controller shall, in case of transfer of personal information to others owing to the transfer of business in whole or in part, or merger, etc., notify in advance the relevant data subjects of the particulars in the following subparagraphs in such a way as stated in the Presidential Decree:

1. The fact that the personal information will be transferred;
2. The name (referring to the company name in case of a juridical person), address, telephone number and other contact points of the recipient of the personal information (hereinafter referred to as the "business transferee"); andnotify the data subjects of the fact in such a way as stated in the Presidential Decree; *provided, however*, that the same shall not apply where the personal
3. The method and procedure to withdraw the consent in case the data subject would not want the transfer of his/her personal information.

(2) Upon receiving the personal information, the business transferee shall without delay information processor has already notified data subjects of the fact of such transfer pursuant to paragraph (1).

(3) The business transferee may, in case of receiving personal information owing to business transfer, merger, etc., use, or provide to a third party, the personal information only for the initial purpose prior to transfer. In this case, the business transferee shall be deemed as the personal information controller.

Article 28 (Supervision of Handler of Personal Information)

(1) While processing the personal information, the personal information controller shall conduct appropriate control and supervision against the person who processes the personal information under the command and supervision of the personal information controller, such as an officer or employee, dispatched worker, part-timer, etc. (hereinafter referred to as the "personal information handler") so that the personal information may be managed.

(2) The personal information controller shall provide necessary educational program to the personal information handler on a regular basis so as to ensure appropriate handling of the personal information.

CHAPTER IV. SAFEGUARDS OF PERSONAL INFORMATION

Article 29 (Duty of Safeguards)

The personal information controller shall take such technical, managerial and physical measures as internal management plan and preservation of log-on records, etc. necessary to ensure the safety as specified by the Presidential Decree so that personal information may not be lost, stolen, leaked, forged, altered or damaged. *<Amended Jul. 24, 2015>*

Article 30 (Establishment and Disclosure of Privacy Policy)

(1) The personal information controller shall establish the personal information processing policy including the particulars in the following subparagraphs (hereinafter referred to as the "Privacy Policy"). In this case, the public institutions shall set up the Privacy Policy toward the personal information files to be registered pursuant to Article 32:

1. The purpose of personal information procession;
2. The period for processing and retention of the personal information;
3. Provision of the personal information to a third party (if applicable);
4. Consignment of personal information processing (if applicable);
5. The rights and obligations of data subjects and how to exercise the rights; and
6. Other matters in relation to personal information processing as stated in the Presidential Decree.

(2) The personal information controller shall, when it establishes or modifies the Privacy Policy, disclose the content so that data subjects may recognize it with ease in such a way as prescribed by the Presidential Decree.

(3) If there are discrepancies between the Privacy Policy and the agreement executed by and between the personal information controller and data subjects, what is beneficial to data subjects prevails.

(4) The Minister of Interior may prepare the Privacy Policy Guidelines and encourage the personal information controller to comply with such guidelines.

Article 31 (Designation of Privacy Officer)

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

(2) The privacy officer shall carry out the job in the following subparagraphs:

1. To establish and implement the data protection plan;
2. To make regular survey of the actual state and practices of personal information processing, and to improve shortcomings;
3. To treat grievances and remedial compensation in relation to personal information processing;
4. To set up the internal control system to prevent the leak, or abuse and misuse, of personal information;
5. To prepare and implement the data protection education program;
6. To protect, and control and manage the personal information files; and
7. Other functions for the appropriate processing of personal information as prescribed by the Presidential Decree.

(3) In carrying out the job as stated in each subparagraph of paragraph (2), the Privacy Officer may inspect the personal information status and systems more often than not, if

necessary, and request the report thereon from the relevant parties.

(4) The Privacy Officer shall, when he/she gets to know any violation of this Act and other relevant laws and regulations in relation to data protection, take immediately corrective measures, and shall, if necessary, report such corrective measures to the head of institution itself or relevant organizations.

(5) The personal information controller shall not have the Privacy Officer give or take disadvantage without any justifiable ground while conducting the job as stated in the subparagraphs of paragraph (2).

(6) The requirements to be designated as the Privacy Officer, data protection job, qualifications and other necessary matters shall be provided by the Presidential Decree.

Article 32 (Registration and Disclosure of Personal Information Files)

(1) The head of public institutions operating the personal information files shall register the matters stated in the following subparagraphs with the Minister of Interior. The same shall apply where the registered matters are modified:

1. The title of the personal information files;
2. The grounds and purposes for the operation of the personal information files;
3. Particulars of personal information which are recorded in the personal information files;
4. The method of processing personal information;
5. The period of retaining personal information;
6. The recipient of personal information in case it is provided routinely or repetitively; and
7. Other matters as prescribed by the Presidential Decree.

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

1. The personal information files which record the national security, diplomatic secrets and other matters relating to grave national interests;
2. The personal information files which record the investigation of crimes, indictment and prosecution, punishment, and enforcement of care and custody, corrective order, protective order, security observation order and immigration;
3. The personal information files which record the examination of law violating activities pursuant to the Law of Punishment on Tax Criminals and the Customs Act;
4. The personal information files which are used exclusively for internal job performance of the public institution; or
5. The personal information files which are classified as secret pursuant to other laws and regulations.

(3) The Minister of Interior may, if necessary, review the registration and its content of the personal information files stated in paragraph (1), and advise the relevant head of the public institutions to improve such files.

(4) The Minister of Interior shall make public the current status of the registered personal information files stated in paragraph (1) so that any one may access to them with ease.

(5) Necessary matters in relation to the registration stated in paragraph (1), the method, scope and procedure of public disclosure stated in paragraph (4) shall be provided by the 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 provided by the respective rules of the National Assembly, the Court, the Constitutional Court and the National Election Commission.

Article 32-2 (Certification of Personal Information Protection)

(1) The Minister of Interior may certify whether the data processing and other data protection related action of the personal information controller abide by this Act, etc.

(2) The certification pursuant to paragraph (1) shall be effective for three years.

(3) The Minister of Interior may withdraw the certification pursuant to paragraph (1) as prescribed by the Presidential Decree if any of the following subparagraphs falls on the case; *provided, however,* that it shall be cancelled in case of subparagraph 1.

1. Personal information protection has been certified by fraud or other unjust means;
2. *Ex post facto* management under paragraph (4) has been denied or obstructed;
3. The certification criteria under paragraph (8) have not been satisfied; or
4. Personal information protection related statutes are breached in a serious manner.

(4) The Minister of Interior shall conduct *ex post facto* management more than once a year to maintain the effectiveness of the certification of personal information protection.

(5) The Minister of Interior may authorize a specialized institution stated by the Presidential Decree to conduct certification subject to paragraph (1), withdrawal of such certification subject to paragraph (3), *ex post facto* management subject to paragraph (4), management of the certification examiners subject to paragraph (7).

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

(7) The qualification, criteria of disqualification, etc. of the certification examiners who conduct the certification examination subject to paragraph (1) shall be stated by the Presidential Decree taking account of specialty, career and other necessary things.

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

[*This Article Newly Inserted Jul. 24, 2015; Effective Jul. 25, 2016*]

Article 33 (Privacy Impact Assessment)

(1) The head of the public institution shall, in case of probable violation of personal information of data subjects owing to the operation of personal information files applicable to the criteria as specified by the Presidential Decree, conduct the assessment for the analysis and improvement of such risk factors (hereinafter referred to as the "Privacy Impact Assessment"), and submit its result to the Minister of Interior. In this case, the head of the public institution shall request the Privacy Impact Assessment to among the institutions (hereinafter referred to as the "PIA institution") designated by the Minister of Interior.

(2) The Privacy Impact Assessment shall cover the matters of the following subparagraphs:

1. The number of personal information being processed;
2. Whether the personal information is provided to a third party or not;
3. The probability to violate the rights of data subjects and the degree of such risk; and
4. The other matters as prescribed by the Presidential Decree.

(3) The Minister of Interior may provide its opinion subject to the deliberation and resolution of the Commission upon receiving the PIA result as stated in paragraph (1).

(4) The head of the 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 PIA result attached thereto.

(5) The Minister of Interior shall work out necessary measures, such as fostering relevant specialists, and developing and disseminating PIA criteria, so as to activate the Privacy Impact Assessment.

(6) Necessary matters in relation to the Privacy Impact Assessment, such as the designation criteria and designation revocation of the PIA institution, assessment criteria, method and procedure, etc. pursuant to paragraph (1) shall be provided by the Presidential Decree.

(7) 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 provided by the respective rules of the National Assembly, the Court, the Constitutional Court and the National Election Commission.

(8) The personal information controller other than the public institution shall make efforts in a positive way to conduct the Privacy Impact Assessment if the violation of personal information of data subjects is highly probable in operating the personal information files.

Article 34 (Data Breach Notification, etc.)

(1) The personal information controller shall notify the aggrieved data subjects without delay of the fact in the following subparagraphs when it becomes to know that personal information is leaked:

1. What kind of personal information was leaked;

2. When and how personal information was leaked;
3. Any information how data subject can do to minimize probable damage suffered from personal information leakage;
4. Countermeasures of the personal information controller and remedial procedure; and
5. Help desk of the personal information controller and contact points for data subjects to report sufferings.

(2) The personal information controller shall prepare countermeasures to minimize the damage in case of personal information leakage, and take necessary measures.

(3) In case where a large scale of data breach above the level specified by the Presidential Decree takes place, the personal information controller shall, without delay, report the notification stated in paragraph (1) and the result of measures stated in paragraph (2) to the Minister of Interior and such specific institution as stated in the Presidential Decree. In this case, the Minister of Interior and such specific institution as stated in the Presidential Decree may provide technical assistance for the prevention and recovery of further damage, etc.

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

Article 34-2 (Imposition, etc. of Surcharge)

(1) The Minister of Interior may impose and collect surcharges not exceeding 500 million won in case where a personal information controller caused the loss, theft, leak, forgery, alteration or damage of resident registration numbers; *provided, however*, that this shall not apply if and when the personal information controller has fully taken measures necessary to ensure the safety subject to Article 24(3) to prevent any loss, theft, leak, forgery, alteration or damage of resident registration numbers. *<Amended Nov. 19, 2014; Jul. 24, 2015>*

(2) When imposing the surcharges pursuant to paragraph (1), the Minister of Interior shall take into consideration the following subparagraphs: *<Amended Nov. 19, 2014; Jul. 24, 2015>*

1. Efforts being taken to perform the safety measures subject to Article 24(3);
2. Status of resident registration numbers which suffered loss, theft, leak, forgery, alteration or damage;
3. Fulfillment of subsequent measures to prevent the spread of damage.

(3) The Minister of Interior shall collect an additional surcharge within the scope of 6/100 per annum of the unpaid surcharge that is determined by the Presidential Decree for the period from the next day of the expiration of the period of the surcharge payment to the previous day of surcharge payment, in case the person subject to surcharge payment pursuant to paragraph (1) fails to pay the surcharge within the period of payment. In this case, the additional surcharge may be collected for not exceeding 60 months. *<Amended*

Nov. 19, 2014>

(4) The Minister of Interior shall, in case a person subject to the surcharge payment pursuant to paragraph (1) fails to pay the sum of surcharge within the period of payment, give a notice with the period of payment specified in it and, in case original and additional surcharges pursuant to paragraph (2) are not paid within the period of payment, collect surcharges in similar to national taxes in arrears. *<Amended Nov. 19, 2014>*

(5) Other matters necessary for the imposition and collection of surcharges shall be determined by the Presidential Decree.

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

CHAPTER V. GUARANTEE OF THE RIGHTS OF DATA SUBJECT

Article 35 (Access to Personal Information)

(1) The data subject may demand access to his/her own personal information, which is processed by the personal information controller, to the relevant personal information controller.

(2) Notwithstanding paragraph (1), when the data subject intends to request access to his/her own personal information to the public institution, the data subject may request directly to the said institution, or indirectly through the Minister of Interior as prescribed by the Presidential Decree.

(3) The personal information controller shall, when it is requested access pursuant to paragraphs (1) and (2), let the data subjects have access to the relevant personal information for the period as prescribed by the Presidential Decree. In this case, if there is any justifiable ground not to permit access for such period, the personal information controller may postpone access after notifying the relevant data subjects of the said ground. If the said ground expires, the postponement shall, without delay, be lifted.

(4) In case where any of the following subparagraphs is applicable, the personal information controller may restrict or deny access after it notifies data subjects of the reason:

1. Where access is prohibited or restricted by law;
2. Where access may probably cause damage to the life or body of others, or improper violation of properties and other benefits of others; or
3. Where the public institutions have grave difficulties in carrying out any of the following Items:
   a. Imposition, collection or repayment of taxes;
   b. Evaluation of academic achievements or admission affairs at the schools established by the Elementary and Middle Education Act and the Higher Education Act, at lifelong educational facilities established by the Lifelong Education Act, and other higher educational institutions established by other laws;

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; or
e. Ongoing audit and examination under other laws.

(5) Necessary matters in relation to the method and procedure of request of access, access restriction, notification, etc. pursuant to paragraphs (1) through (4) shall be provided by the Presidential Decree.

Article 36 (Correction or Deletion of Personal Information)

(1) The data subjects, who have access to his/her own personal information Article 35, may demand the correction or deletion of such personal information to the personal information controller; *provided, however*, that the deletion is not allowed where the said personal information shall be collected by other laws and regulations.

(2) Upon receiving the demand from the data subject pursuant to paragraph (1), the personal information controller shall, without delay, investigate the personal information in question, and take necessary measures to correct or delete as demanded by the said data subject unless otherwise specifically in relation to correction or deletion provided by other laws and regulations. Then the personal information controller shall notify the relevant data subject of the result.

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

(4) When the demand of data subjects is applicable to the proviso of paragraph (1), the personal information controller shall, without delay, notify the relevant data subjects of its content.

(5) While investigating the personal information in question pursuant to paragraph (2), the personal information controller may, if necessary, demand to the relevant data subjects the evidence necessary to confirm the correction and deletion of the personal information.

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

Article 37 (Suspension of Processing of Personal Information)

(1) The data subject may demand the personal information controller to suspend the processing of his/her own personal information. In this case, if the personal information controller is the public institution, only the personal information contained in the personal information files to be registered pursuant to Article 32 may be demanded to suspend to process.

(2) Upon receiving the demand pursuant to paragraph (1), the personal information controller

shall, without delay, suspend to process the said personal information in whole or in part as demanded by the data subject; *provided, however*, that, where any of the following subparagraphs is applicable, the personal information controller may reject the demand of the said data subject:

1. Where it is specifically provided by law or it is inevitable to observe the obligations under the laws and regulations;
2. Where it may probably cause damage to the life or body of others, or improper violation of properties and other benefits of others;
3. Where the public institution cannot carry out its work as prescribed by other laws without processing the personal information in question; or
4. Where the data subject fails to express explicitly termination of the contract even though it is difficult to perform the contract such as provision of service as agreed upon with the said data subject without processing the personal information in question.

(3) When rejecting the demand pursuant to the proviso of paragraph (2), the personal information controller shall, without delay, notify the data subjects of the reason.

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

(5) Necessary matters in relation to the method and procedure of the demand or rejection of suspension of processing, notification, etc. pursuant to paragraphs (1) through (3) shall be provided by the Presidential Decree.

Article 38 (Method and Procedure for Excercise of Rights)

(1) The data subject may delegate to his/her attorney the access pursuant to Article 35, correction or deletion pursuant to Article 36, demand to suspend the processing pursuant to Article 37 (hereinafter referred to as collectively the "access demand") in writing or in the way and procedure as prescribed by the Presidential Decree.

(2) The legal representative for the minor of age below 14 may request the access demand for the minor to the personal information controller.

(3) The personal information controller may demand from the person who requests the access demand the fee and postage (only in case of request mailing of the photocopy) as prescribed by the Presidential Decree.

(4) The personal information controller shall prepare the detailed method and procedure to enable the data subjects to do the access demand, and make it public to the said data subjects.

(5) The personal information controller shall prepare, and guide towards, necessary procedure for data subjects to raise objections against its rejection to the access demand from the said data subjects.

Article 39 (Responsibility for Damages)

(1) Any data subject who suffers damage caused by the personal information controller in violation of this Act may claim the damages against the personal information controller. In this case, the said personal information controller may not be released from the responsibility for damages if it fails to prove non-existence of its wrongful intent or negligence.

(2) *Deleted <Jul. 24, 2015>*

(3) When a data subject suffers damage out of loss, theft, leak, forgery, alteration or damage of personal information, caused by wrongful intent or gross negligence of the personal information controller, the court may fix the damages within the scope not exceeding three times of such damage; *provided, however*, that it shall not apply to the said personal information controller who has proved non-existence of its wrongful intent or gross negligence. *<Newly Inserted Jul. 24, 2015; Effective Jul. 25, 2016>*

(4) The court shall, in fixing the damages pursuant to paragraph (3) take into account of the matters stated by the following subparagraphs: *<Newly Inserted Jul. 24, 2015; Effective Jul. 25, 2016>*

1. The degree of wrongful intent or expectation of likelihood of losses;
2. The amount of loss caused by violations;
3. Economic benefit caused by violations and gained by the personal information controller;
4. The fine and surcharge to be levied subject to violations;
5. The duration, velocity, etc. of violations;
6. The wealth of the personal information controller;
7. The efforts to retrieve the affected personal information exerted by the personal information controller after the loss, theft and leak of personal information; and
8. The efforts to remedy the damage suffered by a data subject exerted by he personal information controller.

Article 39-2 (Claim for Statutory Damages)

(1) Notwithstanding Article 39(1), the data subject, who suffers damage out of loss, theft, leak, forgery, alteration or damage of personal information, caused by wrongful intent or negligence of the personal information controller, may claim a considerable amount of damages to the extent not exceeding three million won. In this case, the said personal information controller may not be released from the responsibility for damages if it fails to prove non-existence of its wrongful intent or negligence.

(2) In case of the claims subject to paragraph (1), the court may fix the reasonable amount of damages to the extent stated by paragraph (1) taking account of whole arguments in the proceedings and the examination of evidence.

(3) The data subject who has claimed damages pursuant to Article 39 may change such claim to the claim subject to paragraph (1) until the closing of fact-finding proceedings.
[*This Article Newly Inserted Jul. 24, 2015; Effective Jul. 25, 2016*]

CHAPTER VI. PERSONAL INFORMATION DISPUTE MEDIATION COMMITTEE

Article 40 (Establishment and Composition of Committee)

(1) The Personal Information Dispute Mediation Committee (hereinafter referred to as the "Dispute Mediation Committee") shall be established to mediate any dispute over personal information.

(2) The Dispute Mediation Committee shall consist of not more than 20 members including one Chairman, and the members shall be *ex officio* and commissioned members. <*Amended Jul. 24, 2015*>

(3) The commissioned members shall be commissioned by the Chairman from among the persons stated in any of the following subparagraphs, and the public official who works for the State organ as prescribed by the Presidential Decree shall be an *ex officio* member: <*Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015*>

1. Persons who once served as public officials who belong to the College of High-ranking Government Officials of the central administrative departments or agencies in charge of data protection, or persons who presently work or have worked at equivalent positions in the public sector and related organizations, and have job experiences in data 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; or
5. Persons who presently work or have worked as senior officers for the trade associations composed of personal information controllers.

(4) The Chairman shall be commissioned by the Chairperson of the Commission from among the Committee members except public officials. <*Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015*>

(5) The term of office for the Chairman and commissioned Committee members shall be two years, and their term of office may be only once extended. <*Amended Jul. 24, 2015*>

(6) In order to conduct efficiently the dispute settlement, the Dispute Mediation Committee may, if necessary, establish a petit panel which is composed of five or less Committee

members in each sector of mediation cases as prescribed by the Presidential Decree. In this case, the resolution of the petit panel delegated by the Dispute Mediation Committee shall be construed as that of the Dispute Mediation Committee.

(7) The Dispute Mediation Committee or a petit panel shall be open with more than half of its members present, and its resolution shall be made by the affirmative votes of the majority of present members.

(8) The Commission may deal with the affairs necessary for dispute mediation including filing of dispute mediation cases and fact finding, etc. *<Amended Jul. 24, 2015>*

(9) The matters necessary to operate the Dispute Mediation Committee except those stated by this Act shall be provided by the Presidential Decree.

[*Effective Jul. 25, 2016*]

Article 41 (Guarantee of Members' Status)

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

Article 42 (Exclusion, Challenge and Refrainment of Member)

(1) Any Committee member, if applicable to any of the following subparagraphs, shall be excluded from participating in the deliberation and resolution of a case requested for dispute mediation (hereafter in this Article referred to as the "case"):

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

(2) Any party may, when he/she finds it difficult to expect a fair deliberation and resolution from the Committee members, file a challenge application with the Chairman. In this case, the Chairman shall determine the challenge application without any resolution of the Dispute Mediation Committee.

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

Article 43 (Application for Mediation of Dispute, etc.)

(1) Any person, who wants any dispute over the personal information mediated, may apply for mediation of such dispute to the Dispute Mediation Committee.

(2) The Dispute Mediation Committee shall, upon receiving an application for dispute mediation from a party of the case, inform the counterparty of the application for mediation.

(3) When the public institution is informed of the notice of dispute mediation pursuant to paragraph (2), the public institution shall respond to it except otherwise exempted by specific circumstances.

Article 44 (Time Limitation of Mediation Procedure)

(1) The Dispute Mediation Committee shall examine the case and prepare draft mediation within 60 days from the date of receiving such application pursuant to Article 43(1); *provided, however*, that, in case of unavoidable circumstances, the Dispute Mediation Committee may resolve to extend such period.

(2) When 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 (Request for Materials, etc.)

(1) Upon receiving the application for dispute mediation pursuant to Article 43(1), the Dispute Mediation Committee may request parties involved in a dispute to provide materials necessary to mediate the dispute. In this case, the relevant parties shall comply with the request unless any justifiable ground exists.

(2) The Dispute Mediation Committee may, when deemed necessary, let parties involved in a dispute or relevant witnesses appear before the Committee to hear their opinions.

Article 46 (Settlement Advice before Mediation)

After receiving the application for dispute mediation pursuant to Article 43(1), the Dispute Mediation Committee may present a draft settlement and recommend a settlement before mediation.

Article 47 (Dispute Mediation)

(1) The Dispute Mediation Committee may include any of the following subparagraphs and prepare a draft mediation:

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

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

(3) Each party presented with the draft mediation pursuant to paragraph (1) shall notify the

Dispute Mediation Committee of his/her acceptance or denial of the draft mediation within 15 days from the day of receipt of such draft mediation, without which such mediation shall be deemed to be denied.

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

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

Article 48 (Rejection and Suspension of Mediation)

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

(2) In case where one of the parties files a lawsuit during the course of examining a medication case, the Dispute Mediation Committee shall suspend the dispute mediation and notify the parties thereof.

Article 49 (Collective Dispute Mediation)

(1) The state and local governments, data protection organizations and institutions, data subjects and personal information controllers may request or apply for a comprehensive dispute mediation (hereinafter referred to as the "Collective Dispute Mediation") to the Dispute Mediation Committee in case where data subject sufferings or violations of rights take place to a multitude of data subjects or in a similar manner, and such incidents are stated by the Presidential Decree.

(2) Upon receiving the request or application for the Collective Dispute Mediation pursuant to paragraph (1), the Dispute Mediation Committee may commence by its resolution the proceedings for the Collective Dispute Mediation pursuant to paragraphs (3) through (7). In this case, the Dispute Mediation Committee shall give a notice of commencing the proceedings for a period as specified by the Presidential Decree.

(3) The Dispute Mediation Committee may accept an application for dispute mediation that he/she shall be added to the party of such dispute mediation, from other data subject or personal information controller than the party of the Collective Dispute Mediation.

(4) The Dispute Mediation Committee may, by its resolution, select a person or more persons as a representative party, who most appropriately represents the common interest among the party of the Collective Dispute Mediation pursuant to paragraphs (1) and (3)

(5) When the personal information controller accepts the Collective Dispute Mediation award presented by the Dispute Mediation Committee, the Dispute Mediation Committee may

advise the personal information controller to prepare and submit the compensation plan for the benefit 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 party 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 the Collective Dispute Mediation shall be less than 60 days from the next day when the notice pursuant to paragraph (2) expires; *provided, however*, that, in case of unavoidable circumstances, the Dispute Mediation Committee may resolve to extend such period.

(8) Other necessary matters such as the Collective Dispute Mediation proceedings, etc. shall be stated by the Presidential Decree.

Article 50 (Mediation Proceedings, etc.)

(1) Except the provisions of Articles 43 through 49, necessary matters concerning the method of, and procedures for, mediating any dispute, and dealing with such dispute mediation, etc. shall be provided by the Presidential Decree.

(2) The Civil Mediation Act shall apply *mutatis mutandis* to the matters which is not provided by this Act in relation to the operation of the Dispute Mediation Committee and dispute mediation procedures.

CHAPTER VII. DATA PROTECTION COLLECTIVE SUIT

Article 51 (Subject of Collective Suit, etc.)

Any organization applicable to any of the following subparagraphs may, if the personal information controller rejects or would not accept the Collective Dispute Mediation pursuant to Article (49), file a lawsuit with the court to prevent or suspend the violations (hereinafter referred to as the "Collective Suit"):

1. An organization, registered with the Korea Fair Trade Commission pursuant to Article 29 of the Consumer Framework Act, which is fully qualified by the following Items:
   a. An organization whose by-laws states the purpose to constantly augment the rights and interests of data subjects exists;
   b. The number of full members shall be more than one thousand; and
   c. Three years have elapsed since the registration pursuant to Article 29 of the Consumer Framework Act.
2. A non-profit organization pursuant to Article 2 of the Non-Profit Private Organization Support Act, which is fully qualified by the following Items:
   a. More than a hundred data subjects, who experienced the same sufferings as a matter

of law or fact, have requested to file the Collective Suit;

b. An organization, whose by-laws states the purpose of data protection, has conducted such activities for the last three years;

c. The number of regular members shall be more than five thousand; and

d. An organization has been registered with the central administrative department or agency.

Article 52 (Exclusive Jurisdictions)

(1) The Collective Suit 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 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, main office or the address of the business manager located in the Republic of Korea.

Article 53 (Retention of Attorney)

The plaintiff of the Collective Suit shall retain an attorney-at-law as a litigation attorney.

Article 54 (Application for Approval of Lawsuit)

(1) An organization which intends to file the Collective Suit shall submit the application for approval of lawsuit describing the followings as well as the petition:

1. Plaintiff and its litigation attorney;
2. Defendant; and
3. Detailed infringements upon the rights of data subjects

(2) The following materials shall be attached to the application for approval of lawsuit as stated in paragraph (1):

1. Evidential materials which prove that the lawsuit filing organization be qualified with any of each subparagraph of Article 51; and
2. Evidential documents which prove that the personal information controller rejected the dispute mediation or would not accept the mediation award.

Article 55 (Requirement for Approval of Suit, etc.)

(1) The court shall approve in a decision the Collective Suit only when all requirements of the following subparagraph are satisfied:

1. That the personal information controller rejected the dispute mediation by the Dispute Mediation Committee or would not accept its mediation award; and
2. That no defect was found in the descriptions in the application for approval of lawsuit as stated in Article 54.

(2) The court decision which approves or disapproves the Collective Suit may be objected by an immediate appeal.

Article 56 (Effect of Conclusive Judgment)

When the decision dismissing plaintiff's complaint became conclusive, such other organizations as stated in Article 51 cannot file a Collective Suit regarding the identical case; *provided, however*, that the same shall not apply where any of the following subparagraphs is applicable:

1. After the decision became conclusive, a new evidence has been found by the state, local government or the state or local government-invested institutions regarding the said case; or
2. Where the decision dismissing the lawsuit proves to be caused intentionally by plaintiff.

Article 57 (Application of Civil Procedure Act, etc.)

(1) Where this Act does not have specific provisions regarding the Collective Suit, the Civil Procedure Act shall apply.

(2) When the decision which approves the Collective Suit as stated in Article 55 was made, a preservation order pursuant to Part IV of the Civil Enforcement Act may be made.

(3) The matters necessary for the procedure shall be provided by the Supreme Court Rule.

CHAPTER VIII. SUPPLEMENTARY PROVISIONS

Article 58 (Partial Exclusion of Application)

(1) Chapters 3 through 7 shall not apply to the personal information stated in any of the following subparagraphs:

1. Personal information collected by the Statistics Act among personal information processed by the public institutions;
2. Personal information collected or requested to provide so as to analyze the information related to national security;
3. Personal information processed temporarily in case it is urgently necessary for the public safety and welfare, public health, etc.; or
4. Personal information collected and used for its own purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties, respectively.

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

(3) Articles 15, 30 and 31 shall not apply to the personal information which is processed by

a personal information controller so as to operate groups or associations for friendship such as alumni associations and hobby clubs.

(4) In case of processing personal information pursuant to each subparagraph of paragraph (1), the personal information controller is required to process such personal information as little as possible to the extent necessary to attain the intended purpose for a minimum period. Also the personal information controller shall make necessary arrangements such as technical, managerial and physical safeguards, individual grievance treatment and other necessary measures for the safe maintenance and appropriate processing of personal information.

Article 59 (Prohibited Activities)

No one who processes or processed personal information shall do any of the following subparagraphs:

1. To get personal information or obtain the consent to personal information processing in a fraudulent, improper or unfair manner;
2. To leak personal information obtained in the course of business, or provide it without authority to other's use; or
3. To damage, destroy, alter, forge or leak other's personal information without legal authority or beyond proper authority.

Article 60 (Confidentiality, etc.)

Any person who is or was engaged in the business stated in the following subparagraphs shall not leak secrets acquired while performing his/her duties to any other person, nor use such secrets for other purpose than the initial one; *provided, however*, that the same shall not apply where specific provisions are provided in other acts:

1. The work of the Personal Information Protection Commission under Article 8;
2. The privacy impact assessment work under Article 33; and
3. The dispute mediation work by the Dispute Mediation Committee under Article 40.

Article 61 (Suggestions and Advice for Improvement)

(1) The Minister of Interior may provide its opinion to the authority concerned subject to the deliberation and resolution of the Commission when it is deemed necessary with respect to the laws and regulations which contain provisions likely affecting data protection.

(2) The Minister of Interior may advise the personal information controller to improve the actual state of personal information processing when it is deemed necessary for data protection. In this case, upon receiving the advice, the personal information controller shall make sincere efforts to perform the advice, and inform the Minister of Interior of its result.

(3) The head of the central administrative department or agency concerned may advise the personal information controller, in accordance with the laws under its jurisdiction, to improve the actual state of personal information processing when it is deemed necessary for data protection. In this case, upon receiving the advice, the personal information controller shall make sincere efforts to perform the advice, and inform the head of the central administrative department or agency concerned of its result.

(4) The central administrative departments and agencies, local governments, the National Assembly, the Court, the Constitutional Court and the National Election Commission may suggest their opinion, or provide guidance or inspection with respect to data protection to their affiliated entities and public authorities under their jurisdiction.

Article 62 (Report of Violations, etc.)

(1) Anybody who suffers infringement on the rights or interests relating to his/her personal information in the course of personal information processing conducted by personal information controllers may report such sufferings to the Minister of Interior.

(2) The Minister of Interior may designate a specialized institution so as to efficiently perform the work to receive and handle the claim report pursuant to paragraph (1), as provided by the Presidential Decree. In this case, such specialized institution shall establish and operate and a personal information infringement call center (hereinafter referred to as the "DP Call Center").

(3) The DP Call Center shall perform the duties stated in the following subparagraphs:

1. To receive the claim report and counsel in relation to personal information processing;
2. To investigate and confirm the incident and hear opinions of interested party; and
3. To do works incidental to subparagraphs 1 and 2.

(4) The Minister of Interior may, if necessary, dispatch its public officials in accordance with Article 32-4 of the National Officials Act to such specialized institution as stated in paragraph (2) so as to efficiently perform the duty to investigate and confirm the incident pursuant to subparagraph 2 of paragraph (3).

Article 63 (Request for Materials and Inspection)

(1) The Minister of Interior may, if any of the following subparagraphs is applicable, have the personal information controller furnish the relevant materials such as goods, documents, etc.:

1. Where any breach of this Act has been found or suspected;
2. Where the breach of this Act has been reported or civil complaint thereon has been received; or
3. Where it is necessary for data protection of the data subjects as stated in the Presidential Decree.

(2) When the personal information controller fails to furnish the materials pursuant to paragraph (1), or are deemed to have violated this Act, the Minister of Interior may have its officials enter the office or business place of the said personal information controller and others related with such violations to inspect current business operations and examine ledger and books, or other documents, etc. In this case, the officials, who conduct the inspection or examination, shall carry certificates showing their authority, produce them to persons concerned. *<Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015>*

(3) The head of central administrative department or agency concerned may request the personal information controller to furnish the materials pursuant to paragraph (1), or conduct inspection or examination of the personal information controller and others related with the violations in question pursuant to paragraph (2) in accordance with laws under its jurisdiction. *<Amended Jul. 24, 2015>*

(4) When finding or suspecting any breach of this Act, the Commission may demand the Minister of Interior or the head of central administrative department or agency concerned to take measures pursuant to the part other than each subparagraph of paragraph (1), or paragraph (3). In this case, the Minister of Interior or the head of central administrative department or agency concerned, who was demanded as such, shall respond to it except otherwise exempted by specific circumstances. *<Amended Jul. 24, 2015>*

(5) The Minister of Interior and the head of central administrative department or agency concerned shall not provide to a third party the documents, materials, etc. furnished or collected pursuant paragraphs (1) and (2), nor make them public, except otherwise required by this Act. *<Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015>*

(6) In case the Minister of Interior and the head of central administrative department or agency concerned received the materials submitted via the information and communications networks, or made them digitalized, they shall take systemic and technological security measures lest the personal information, trade secrets, etc. should be leaked out. *<Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015>*

(7) The Minister of Interior may inspect the current status of personal information protection jointly with the head of central administrative department or agency concerned for the prevention of personal information breach incident and efficient response. *<Newly Inserted Jul. 24, 2015>*

Article 64 (Corrective Measures, etc.)

(1) The Minister of Interior may, when it deems that any infringement upon personal information is substantially grounded and to leave it unattended likely causes irreparable injury, order the violator of this Act (excluding the central administrative departments and agencies, local governments, the National Assembly, the Court, the Constitutional Court and the National Election Commission) to take the relevant measures applicable to any of the

following subparagraphs:

1. To suspend any violation of personal information;
2. To temporarily suspend processing of personal information; or
3. Other necessary measures for the protection of, or prevention of infringement upon, personal information.

(2) The head of central administrative department or agency concerned may, when it deems that any infringement upon personal information is substantially grounded and to leave it unattended likely causes irreparable injury, order the personal information controller to take the relevant measures applicable to any of the subparagraphs of paragraph (1) in accordance with laws under its jurisdiction.

(3) Local governments, the National Assembly, the Court, the Constitutional Court and the National Election Commission may order their affiliated entities and public authorities under their jurisdiction, which are found to violate this Act, to take the relevant measures applicable to any of the subparagraphs of paragraph (1).

(4) The Commission may, when the central administrative department and agency, local government, the National Assembly, the Court, the Constitutional Court or the National Election Commission violates this Act, advise the head of the authority concerned to take the relevant measures applicable to any of the subparagraphs of paragraph (1). In this case, upon receiving the advice, the authority concerned shall respect it.

Article 65 (Accusation and Recommendation of Disciplinary Action)

(1) The Minister of Interior may, when the suspicion of crime that the personal information controller has violated this Act or other data protection-related laws and regulations is deemed substantially grounded, accuse the fact to the competent investigative agency. *<Amended Mar. 23, 2013>*

(2) The Minister of Interior may, when any violation of this Act or other data protection-related laws and regulations is substantially grounded, advise the head of authority or organization concerned to take disciplinary action against the person responsible for it (including a representative officer and the executive officer in charge). In this case, upon receiving the advice, the relevant personal information controller shall respect it, and notify the Minister of Interior of the result. *<Amended Mar. 23, 2013; Aug 6, 2013>*

(3) The head of central administrative department or agency concerned may, in accordance with laws under its jurisdiction, accuse the personal information controller pursuant to paragraph (1), or the head of authority or organization concerned to take disciplinary advice pursuant to paragraph (2). In this case, upon receiving the advice pursuant to paragraph (2), the head of authority or organization concerned shall respect it, and notify the head of central administrative department or agency concerned of the result.

Article 66 (Disclosure of Results)

(1) The Minister of Interior may, subject to the deliberation and resolution of the Commission, disclose the advice for improvement pursuant to Article 61, the corrective order pursuant to Article 64, the accusation or disciplinary advice pursuant to Article 65 and the imposition of fine for negligence pursuant to Article 75 and its result, respectively.

(2) The head of central administrative department or agency concerned may, in accordance with laws under its jurisdiction, disclose the matter pursuant to paragraph (1).

(3) The method, criteria and procedure of disclosure pursuant to paragraphs (1) and (2) provided by the Presidential Decree.

Article 67 (Annual Report)

(1) The Commission shall prepare for the report each year, based upon necessary materials furnished by the authorities concerned, in relation to the data protection policy measures and implementation thereof, and submit (including transmission via the information and communications networks) it to the National Assembly before the opening of the plenary session.

(2) The annual report pursuant to paragraph (1) shall include any of the following subparagraphs:

1. Infringement upon the rights of data subjects and the current status of remedies thereof;
2. The result of survey in relation to actual state of personal information processing;
3. The current status of implementation of data protection policy measures and achievements thereof;
4. Overseas legislation and policy developments related with personal information; and
5. Other matters to be disclosed or reported with respect to data protection policy measures.

Article 68 (Delegation and Entrustment of Authority)

(1) A part of the authority of the Minister of Interior or the head of central administrative department or agency concerned under this Act may be delegated or entrusted as provided by the Presidential Decree to the mayor of the Special City or Metropolitan City, the governor of provinces or the Special Autonomous Province, or such specialized institution as prescribed by the Presidential Decree.

(2) The institution to which a part of the authority of the Minister of Interior or the head of central administrative department or agency concerned has been delegated or entrusted pursuant to paragraph (1) shall notify the Minister of Interior or the head of central administrative department or agency concerned of the result of such work delegated or entrusted.

(3) The Minister of Interior may, in case of delegating or entrusting a part of its authority to such specialized institution as stated in paragraph (1), contribute the expenses necessary

to perform the duties of the relevant specialized institution.

Article 69 (Legal Fiction of Officials in Applying Penal Provisions)

The officers and employees of the authorities concerned, who are conducting the job entrusted by the Minister of Interior or the head of central administrative department or agency concerned, shall be deemed officials in applying Articles 129 through 132 of the Criminal Act.

CHAPTER IX. PENAL PROVISIONS

Article 70 (Penal Provision)

Any person referred to in any of the following subparagraphs shall be subject to imprisonment with prison labor for not more than 10 years or by a fine not exceeding 100 million won. *<Amended Jul. 24, 2015>*

1. A person who has caused the suspension, paralysis or other severe hardship of work of public institutions by altering or deleting the personal information processed by the said institutions for the purpose to disturb the personal information processing of the said institutions
2. A person who has obtained the personal information processed by others by fraud or other unjust means or method and provided it to a third party for profit or unjust purpose, and who has abetted and arranged such thing.

Article 71 (Penal Provision)

Any person referred to in any of the following subparagraphs shall be subject to imprisonment with prison labor for not more than 5 years or by a fine not exceeding 50 million won:

1. A person who has provided personal information to a third party without consent of data subjects in violation of Article 17(1) i even though Article 17(1) ii is not applicable, and knowingly received the said personal information;
2. A person who has used, or provided a third party with, personal information in violation of Articles 18(1) and (2), 19, 26(5) or 27(3), and knowingly received the said personal information for the profit-making or unfair purposes;
3. A person who has processed sensitive data in violation of Article 23;
4. A person who has processed the Unique Identifier in violation of Article 24(1);
5. A person who has leaked, or provided to other persons without authority, the personal information acquired on business in violation of Article 59 ii, and knowingly received the said personal information for the profit-making or unfair purposes; or
6. A person who has damaged, destroyed, altered, forged or leaked the personal

information of others in violation of Article 59 iii.

Article 72 (Penal Provision)

Any person referred to in any of the following subparagraphs shall be subject to imprisonment with prison labor for not more than 3 years or by a fine not exceeding 30 million won:

1. A person who has handled arbitrarily visual data processing devices for other purposes than the initial one, or directed the said devices toward different spots, or used sound recording functions in violation of Article 25(5)
2. A person who has got personal information or obtained the consent to personal information processing in a fraudulent, improper or unfair manner, and a person who has knowingly received such personal information for the profit-making or unfair purposes in violation of Article 59 i; or
3. A person who has leaked secrets acquired while performing his/her duties to other person, or used such secrets for other purpose than the initial one in violation of Article 60.

Article 73 (Penal Provision)

Any person referred to in any of the following subparagraphs shall be subject to imprisonment with prison labor for not more than 2 years or by a fine not exceeding 10 million won: *<Amended Jul. 24, 2015>*

1. A person who has failed to take necessary measures to ensure the safety in violation of Articles 24(3), 25(6) or 29, and caused the personal information to be lost, stolen, leaked, forged, altered or damaged;
2. A person who has failed to take necessary measures to correct or delete in violation of Article 36(2), and continuously use, or provide to a third party, the personal information; or
3. A person who has failed to suspend to process personal information in violation of Article 37(2), and continuously use, or provide to a third party, the personal information.

Article 74 (Joint Penal Provision)

(1) If the representative of a corporation, or the agent, manager or other employee of a corporation or an individual violated the provision of Article 70 with respect to the business of such corporation or individual, not only the actor but also the corporation or individual shall be subject to a fine not exceeding 70 million won; *provided, however*, that the same shall not apply where such corporation or individual was not negligent in taking due care and supervisory duty to prevent the actor from the said violation.

(2) If the representative of a corporation, or the agent, manager or other employee of a corporation or an individual violated any of the provisions from Articles 71 through 73 with respect to the business of such corporation or individual, not only the actor but also the corporation or individual shall be subject to a fine prescribed in the relevant Article; *provided, however*, that the same shall not apply where such corporation or individual was not negligent in taking due care and supervisory duty to prevent the actor from the said violation.

Article 74-2 (Confiscation, Additional Collection, etc.)

Any money, goods or other benefits received by an offender in violation of Articles 70 through 73 in relation to such violations shall be confiscated, or, if confiscation is impossible, the value thereof may be collected. In this case, such confiscation or additional collection may be levied in addition to other penal provision.

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

Article 75 (Fine for Negligence)

(1) A person referred to in any of the following subparagraphs shall be subject to a fine for negligence not exceeding 50 million won:

1. A person who has collected personal information in violation of Article 15(1);
2. A person who has failed to obtain the consent from the legal representative in violation of Article 22(5); or
3. A person who has installed and operated visual data processing devices in violation of Article 25(2).

(2) A person referred to in any of the following subparagraphs shall be subject to a fine for negligence not exceeding 30 million won: *<Amended Mar. 23, 2013; Nov. 19, 2014; Jul. 24, 2015>*

1. A person who has failed to notify data subjects of necessary information in violation of Articles 15(2), 17(2), 18(3) or 26(3);
2. A person who has denied the provision of goods or services to data subjects in violation of Articles 16(3) or 22(4);
3. A person who has failed to notify data subjects of the fact stated in the subparagraphs of Article 20(1) in violation of the same paragraph;
4. A person who has failed to destroy the personal information in violation of Article 21(1);

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

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

5. A person who has failed to provide data subjects with an alternative method without using

their resident registration numbers in violation of Article 24-2(3);

6. A person who has failed to take necessary measures to ensure the safety in violation of Articles 24(3), 25(6) or 29;
7. A person who has installed and operated visual data processing devices in violation of Article 25(1);
7-2. A person who has marked and promoted the certification by fraud despite failure of such certification in violation of Article 32-2(6);
8. A person who has failed to notify data subjects of the fact in the subparagraphs of Article 34(1) in violation of the same paragraph;
9. A person who has failed to report the result of notification in violation of Article 34(3);
10. A person who has restricted or denied the access to the personal information in violation of Article 35(3);
11. A person who has failed to take necessary measures to correct or delete in violation of Article 36(2);
12. A person who has failed to take necessary measures including destruction of the personal information whose processing was suspended in violation of Article 37(4); or
13. A person who has failed to observe the corrective measures pursuant to Article 64(1).

(3) A person referred to in any of the following subparagraphs shall be subject to a fine for negligence not exceeding 10 million won:

1. A person who has failed to store and manage personal information separately in violation of Article 21(3);
2. A person who has obtained the consent in violation of Article 22(1) through (3);
3. A person who has failed to take necessary measures including posting on a signboard in violation of Article 25(4);
4. A person who has failed to go through such paper-based formalities during the consignment of works as stated in the subparagraphs of Article 26(1) in violation of the same paragraph;
5. A person who has failed to disclose the consigned works and the consignee in violation of Article 26(2);
6. A person who has failed to notify data subjects of the transfer of personal information in violation of Article 27(1) and (2);
7. A person who has failed to establish, or disclose, the personal information processing policy in violation of Article 30(1) or (2);
8. A person who has failed to designate the privacy officer in violation of Article 31(1);
9. A person who has failed to provide data subjects with necessary information in violation of Articles 35(3) and (4), 36(2) and (4) or 37(3);
10. A person who has failed to furnish the materials such as goods, documents, etc.

pursuant to Article 63(1), or who submitted them in a fraudulent way; or

11. A person who has rejected, obstructed or avoided the entry, inspection and examination pursuant to Article 63(2).

(4) The fine for negligence pursuant to paragraphs (1) through (3) shall be imposed and collected by the Minister of Interior and the head of central administrative department or agency concerned as provided by the Presidential Decree. In this case, the head of central administrative department or agency concerned shall impose and collect the fine for negligence from the personal information controller in the field under its jurisdiction.

Article 76 (Special Exemption to the Application of Fine for Negligence)

While applying the provisions on the fine for negligence subject to Article 75, additional fine for negligence shall not be imposed on the act subject to surcharge payment pursuant to Article 34-2.

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

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on the day when 6 months elapse after its promulgation; *provided, however*, that Article 24(2) and Article 75(2) v shall enter into force on the day when one year elapses after its promulgation.

Article 2 (Repeal of Other Act)

The Act on the Protection of Personal Information Maintained by Public Agencies shall be repealed.

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

As at the Enforcement Date, the activities of, or activities against, the Personal Information Dispute Mediation Committee under the existing Act on the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. shall be deemed as such activities under this Act applicable thereto.

Article 4 (Transitional Measures Regarding Personal Information under Processing)

The personal information processed legally under other laws and regulations prior to the enforcement of this Act shall be deemed to be processed under this Act.

Article 5 (Transitional Measures Regarding Application of Penal Provisions)

(1) The application of the penal provisions to the acts committed in violation of the previous Act on the Protection of Personal Information Maintained by Public Agencies prior to the enforcement of this Act shall be governed by the previous Act on the Protection of Personal Information Maintained by Public Agencies.

(2) The application of the penal provisions to the acts committed in violation of the existing Act on the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. prior to the enforcement of this Act shall be governed by the existing Act on the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.

Article 6 (Amendment to Other Acts)

(1) A part of the Act on the Excavation of Corpse of the Soldiers Killed in the Battle during the Korean War shall be amended as follows:

In Article 14(1) ii, Article 2 ii of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 2 i of the Personal Information Protection Act.

(2) A part of the Public Official Ethics Act shall be amended as follows:

In Article 6(6) and (9), Article 10 of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 18 of the Personal Information Protection Act, respectively.

(3) A part of the National Officials Act shall be amended as follows:

In Article 19-3(3), Article 2 i of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 2 vi of the Personal Information Protection Act, and the Act on the Protection of Personal Information Maintained by Public Agencies in paragraph (4) of the same Article shall be the Personal Information Protection Act.

(4) A part of the Invention Promotion Act shall be amended as follows:

In Article 10-2(1) of the Act on the Protection of Personal Information Maintained by Public Agencies shall be the Personal Information Protection Act.

(5) A part of the Act on the Use and Protection of Credit Information shall be amended as follows:

Article 23(2) ii shall be the Personal Information Protection Act.

(6) A part of the Children Welfare Act shall be amended as follows:

In Article 9-2(3) of the Act on the Protection of Personal Information Maintained by Public Agencies shall be the Personal Information Protection Act

(7) A part of the Cancer Management Act, wholly amended by Law No. 10333, shall be amended as follows:

In the second part of Article 14(1), Article 3(2) of the Act on the Protection of

Personal Information Maintained by Public Agencies shall be Article 58(1) of the Personal Information Protection Act; and

In the second part of Article 49, Article 10(3) of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 18(2) of the Personal Information Protection Act.

(8) A part of the Act on the Prevention of Discrimination of the Disabled and Redress, etc. shall be amended as follows:

In the second part of Article 3 viii c, Article 2 ii of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 2 i of the Personal Information Protection Act; and

In Article 22(2), the Act on the Protection of Personal Information Maintained by Public Agencies shall be the Personal Information Protection Act

(9) A part of the e-Signature Act shall be amended as follows:

Article 24(2) shall be deleted.

(10) A part of the e-Government Act shall be amended as follows:

In the Article 21(2), Article 2 ii of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 2 i of the Personal Information Protection Act;

In the Article 39(4), Article 5 of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 32 of the Personal Information Protection Act, and subject to the deliberation of the Public Agency Data Protection Deliberation Committee under Article 20(1) of the same Act shall be subject to the deliberation and resolution of the Personal Information Protection Commission under Article 7 of the Personal Information Protection Act; and

In the Article 42(1), Article 2 viii of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 2 iii of the Personal Information Protection Act, and Article 10(3) i and Article 10(5) of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 18(2) i and Article 19 i of the Personal Information Protection Act.

(11) A part of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. shall be amended as follows:

Section 4 of Chapter 4 (Articles 33, 33-2, 34 through 40), subparagraph 1 of Article 66, and Article 67 shall be repealed, respectively;

In Articles 4(1) and (3), Article 64-2(3) second part, Articles 65(1) and 69, the Minister of Interior, the Minister of Knowledge and Economy, and the Broadcasting and Communications Commission shall be the Minister of Knowledge and Economy and the Broadcasting and Communications Commission, respectively; and

In the provision except each subparagraph of Article 64(1), Articles 64(3), 64(4) first

part, 64(5) first part, 64(6), 64(9), 64(10), 64-2(1), 64-2(2), the first part of the provision except each subparagraph of Article 64-2(3), Articles 65(3), 76(1) xii and 76(4) through (6), the Minister of Public Administration or the Broadcasting and Communications Commission shall be the Broadcasting and Communications Commission, respectively.

(12) A part of the Act for the Fair Collection of Claims shall be amended as follows:
In the Article 2 v, Article 2 ii of the Act on the Protection of Personal Information Maintained by Public Agencies shall be Article 2 i of the Personal Information Protection Act.

(13) A part of the Immigration Control Act shall be amended as follows:
In the Articles 12-2(6) and 38(3), the Act on the Protection of Personal Information Maintained by Public Agencies shall be the Personal Information Protection Act, respectively.

(14) A part of the Act on the Establishment of the Korea Scholarship Foundation, etc. shall be amended as follows:
In the Article 50(3), the Act on the Protection of Personal Information Maintained by Public Agencies shall be the Personal Information Protection Act.

Article 7 (Relations to Other Acts and Regulations)

In case where other acts and regulations cite the previous Act on the Protection of Personal Information Maintained by Public Agencies or its provisions as at the Enforcement Date of this Act, if any provision of this Act can apply to such circumstances, this Act or the corresponding provision of this Act shall apply thereto instead of the previous provision.

ADDENDA

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

Article 1 (Enforcement Date)

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

(2) *Omitted*

Articles 2 – 5. *Omitted*

Article 6 (Amendment to Other Acts)

(1) - (149) *Omitted*

(150) A part of the Personal Information Protection Act shall be amended as follows:
The Minister of Public Administration and Security shall read the Minister of Interior.

(151) - (710) *Omitted*

Article 7. *Omitted*

ADDENDA

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

Article 1 (Enforcement Date)

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

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

(1) The personal information controller who is processing resident registration numbers as of the entry into force of this Act shall destroy the resident registration numbers possessed by it within two years from the enforcement date of this Act; *provided, however*, that this shall not apply when any subparagraph of Article 24-2(1) amended hereby is applicable.

(2) The personal information controller who fails to destroy the resident registration numbers possessed by it within the period pursuant to paragraph (1) is deemed to be in violation of the amended Article 24-2(1).

ADDENDUM

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

This Act shall enter into force on the day of promulgation; *provided, however*, that Articles 24-2 and 75(2) v. amended by Act 11990 shall enter into force on January 1, 2016.

ADDENDA

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

Article 1 (Enforcement Date)

This Act shall enter into force on the day of its promulgation; *provided, however*, that the Act amended pursuant to Addenda Article 6, which was promulgated prior to the enforcement of this Act with such amendments not yet enforced, shall enter into force on the day of enforcement of the relevant Act.

Articles 2 – 5. *Omitted*

Article 6 (Amendment to Other Acts)

(1) - (55) *Omitted*

(56) A part of the Personal Information Protection Act shall be amended as follows:

The Minister of Safety and Public Administration shall read the Minister of Interior.

(57) - (258) *Omitted*

Article 7. *Omitted*

ADDENDA

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

Article 1 (Enforcement Date)

This Act shall enter into force on the day of its promulgation; *provided, however*, that Articles 8(1), 8-2, 9, 11(1), 32-2, 39(3) and (4), 39(2), 40, 75(2)7-2 shall enter into force on the elapse of one year after its promulgation; Articles 24-2(2) first sentence and 75(2)4-3 on January 1, 2016, respectively.

Article 2 (Exemplary Application of Damages)

The amendments of Article 39(3) and (4) and 39-2 shall apply to the claim of damages for personal information suffering loss, theft, leak, forgery, alteration or damage after the enforcement of this Act.

Article 3 (Transitional Measures Regarding Personal Information Protection Certification)

Any person who has obtained the personal information protection certification from the Minister of Interior shall be deemed to have obtained such certification under the amended provision of Article 32-2.

Article 4 (Transitional Measures Regarding the Qualification of Personal Information Protection Certification Examiner)

Any person who has obtained the qualification of the personal information protection certification examiner shall be deemed to have obtained such qualification under this Act.

Article 5 (Transitional Measures Regarding the Term of Personal Information Dispute Mediation Committee Members)

Any member of the Personal Information Dispute Mediation Committee, who has been appointed or commissioned by the Minister of Interior prior to the enforcement of this Act, shall be deemed to have been commissioned by the Personal Information Protection Commission under the amended provision of Article 40.

Article 6 (Transitional Measures Regarding Penal Provisions, etc.)

The application of the penal provisions or the fine for negligence to the violations prior to the enforcement of this Act shall be governed by the previous provisions.