

# **Enforcement Decree of the Personal Information Protection Act**

Established September 29, 2011

## **Chapter 1. General Provisions**

### **Article 1 (Purpose)**

The purpose of this Decree is to provide for matters delegated by the Personal Information Protection Act and other things necessary for the enforcement thereof.

### **Article 2 (Scope of Public Institution)**

“Other national institutions and public entities which are designated by the Presidential Decree” in Item b. Subparagraph 6 of Article 2 of the Personal Information Protection Act (hereinafter referred to as the “Act”) shall refer to any of the following institutions:

1. The National Human Rights Commission of Korea pursuant to Article 3 of the National Human Rights Commission Act;
2. The public institution pursuant to Act 4 of the Act for the Management of Public Institutions;
3. A regional corporation and a regional industrial complex under the Regional Public Enterprise Act;
4. A special legal entity established by the special act; or
5. Each level of school established by the Elementary and Secondary Education Act, the Higher Education Act and other relevant acts.

### **Article 3 (Scope of Visual Data Processing Devices)**

The “devices designated by the Presidential Decree” in Subparagraph 7 of Article 2 of the Act shall refer to any of the following devices:

1. Closed circuit television (CCTV) shall mean any of the following Items:
  - a. A device which shoots videos, etc. through a continuously installed camera at a certain place, or transmits such videos, etc. to the specified place via transmission channel of wired/wireless closed circuits, etc.
  - b. A device which may videotape or record such visual information filmed or transmitted pursuant to Item a.
2. Network (Internet protocol) camera shall mean a device with which its installer or operator may collect, store or process such visual information, filmed through a

continuously installed device at a certain place, via the wired/wireless Internet at any place.

## **Chapter 2. Personal Information Protection Commission**

### **Article 4 (Exclusion, Challenge and Refrainment of Commissioner)**

- (1) Any member of the Personal Information Protection Commission (hereinafter referred to as the “Commission”, or abbreviated as PIPC) subject to Article 7(2) of the Act shall be excluded from participating in the deliberation and resolution of the matters, if applicable to any of the following Subparagraphs:
1. Any matter in which a PIPC member, his/her spouse, relatives within 4<sup>th</sup> degree, spouse’s relatives within 2<sup>nd</sup> degree, or an organization or institution to which the said persons belong, has or have some interests;
  2. Any matter to which a PIPC member has given any testimony or expert opinion, or was involved as an agent or representative; or
  3. Any matter in which a person has some interests, to whom a PIPC member or the public institution, juristic person or other organization to which the PIPC member belongs has provided advice or assistance.
- (2) Any person who has direct interests in the matter for deliberation and resolution of the PIPC may, when he/she finds a PIPC member has a reason to be excluded pursuant to Paragraph (1) or deems it difficult to expect a fair deliberation and resolution from the PIPC member, file a challenge application with the PIPC citing such reasons. In this case, the Chairperson shall determine the challenge.
- (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 matter.

### **Article 5 (Expert Committee)**

- (1) In order to review in advance the matters for deliberation and resolution subject to Article 8(1) of the Act in a professional manner, the PIPC may establish expert committee by sector (hereinafter referred to as the “Expert Committee”).
- (2) The Expert Committee subject to Paragraph (1) shall be comprised of five (5) or less members including one chairperson, who is designated or commissioned by the Chairperson of the Commission subject to the consent of the Commission among the persons in the following Subparagraphs, while the chairperson of the Expert Committee is designated by the Chairperson of the Commission among the Expert Committee members.
1. The PIPC member;

2. Public officials engaged in the data protection-related job of the central administrative department or agency;
  3. Persons with sufficient expertise and experience in data protection; or
  4. Persons belonging to, or recommended by, data protection-related organizations or business associations.
- (3) The Expert Committee meeting shall start with the majority of its members present, and its resolution shall be made with the majority approval of the members present.

**Article 6 (Disclosure of Proceedings)**

The meetings of the Commission shall be open to the public; *provided, however*, that they may be closed when the PIPC Chairperson deems it necessary.

**Article 7 (Dispatch of Public Official, etc.)**

The Commission may request the public institution to dispatch public officials, or officers and employees where the Commission deems it necessary to conduct its functions.

**Article 8 (Organization and Number of Staff)**

Necessary matters regarding the organization and number of staff of the Commission other than the provisions of this Decree shall be otherwise stipulated by the Presidential Decree.

**Article 9 (Attendance Fee, etc.)**

The Commissioner who attended the meetings of the Commission or the Expert Committee, the person who attended the meetings of the Commission or the Expert Committee pursuant to Article 8(2) of the Act may be paid allowances, travel expenses and other necessary costs within the scope of the budget; *provided, however*, that the same shall not apply when the public official attended the meeting directly related with his/her own work.

**Article 10 (Operational Rule of the Commission, etc.)**

Necessary matters regarding the organization and operation of the Commission or the Expert Committee other than the provisions of the Act and this Decree shall be stipulated by the PIPC Rule subject to the resolution of the Commission.

**Chapter 3. Process to Establish Basic Plan and Implementation Plan**

**Article 11 (Basic Plan Set-up Process, etc.)**

- (1) The Minister of Public Administration and Security (MOPAS) shall establish the Personal Information Protection Basic Plan subject to Article 9 of the Act (hereinafter referred to as the “Basic Plan”) every three years, and submit it to the PIPC making it subject to the deliberation and resolution of the PIPC until December 31 of the year two years before the start of the three-year plan.
- (2) When the MOPAS establishes the Basic Plan pursuant to Paragraph (1), it may reflect the sub-plan by sector submitted by the head of central administrative department or agency concerned on the Basic Plan. In this case, the MOPAS may notify the head of such central administrative department or agency of guidelines on how to set up sub-plans by sector.
- (3) The MOPAS shall, without delay upon fixing the Basic Plan, notify the head of central administrative department or agency concerned of the Basic Plan.

**Article 12 (Implementation Plan Set-up Process, etc.)**

- (1) The MOPAS shall establish guidelines on how to set up the Implementation Plan of the next-to-next year by December 31 of each year, and notify the head of central administrative department or agency concerned of the Implementation Plan.
- (2) The head of central administrative department or agency concerned shall, of the Basic Plan subject to the guidelines of Paragraph (1), establish the Implementation Plan under its jurisdiction to be implemented during the next year, and submit it to PIPC until the end of February each year.
- (3) The PIPC shall deliberate and resolve the Implementation Plan submitted pursuant to Paragraph (2) until April 30 that year.

**Article 13 (Scope and Method of Materials requested by MOPAS)**

- (1) The MOPAS may request materials or opinion, etc. regarding any of the following Subparagraphs from the personal information processor pursuant to Article 11(1) of the Act.
  1. Matters regarding the management of personal information files and the installation and operation of visual data processing devices dealt by the relevant personal information processor;
  2. Matters regarding the designation of the privacy officer subject to Article 31 of the Act;
  3. Matters regarding the technical, managerial and physical measures to ensure the safety of personal information;
  4. Matters regarding the demand of access, modification, deletion or suspension of processing from the data subject, and the measures taken to meet such demand; or

5. Other matters necessary to establish and implement the Basic Plan including the compliance of this Act and the Enforcement Decree.
- (2) When the MOPAS requests materials or opinion, etc. pursuant to Paragraph (1), it shall request them to the minimum extent necessary to establish and implement efficiently the Basic Plan.
- (3) Where the head of central administrative department or agency requests the materials from the personal information processor under its jurisdiction pursuant to Article 11(2) of the Act, the provisions of Paragraphs (1) and (2) shall apply *mutantis mutandis*. In this case, the MOPAS shall be deemed the head of central administrative department or agency, and Article 11(1) of the Act shall be deemed Article 11(2) of the Act.

**Article 14 (Promotion and Support of Self-Regulation)**

The MOPAS may provide data protection-related institutions or organizations with necessary assistance within the scope of budget to promote the self-regulatory data protection activities of personal information processors pursuant to Article 13(2) of the Act.

**Chapter 4. Processing of Personal Information**

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

Where the public institution uses personal information for other purpose than the intended one, or provides it to a third party pursuant to each Subparagraph of Article 18(2) of the Act, it shall record the matters in the following Subparagraphs in the Book for Out-of Purpose Use or Control of Provision of Personal Information, and manage such book.

1. The name of the personal information or its file used or provided as such;
2. The name of the institution which uses or is provided with personal information;
3. The purpose of use or being provided;
4. The statutory ground for such use or being provided;
5. The items of personal information to be used or provided;
6. The date, frequency or period to use or provide personal information;
7. The manner of use or being provided; or
8. Any restriction or necessary measure which the personal information processor requested from the recipient pursuant to Article 18(5) of the Act.

**Article 16 (How to Destroy Personal Information)**

When the personal information processor destroy the personal information pursuant to Article 21 of the Act, it shall take one of the methods categorized in following Subparagraphs:

1. In case of electronic files, permanent erasure not to restore data; or
2. In case of other records, prints, documents, etc. except Subparagraph 1, destruction or incineration.

#### **Article 17 (Method of Obtaining Consent)**

(1) The personal information processor shall obtain the consent pursuant to Article 22 of the Act from the data subjects in a way of the following Subparagraphs:

1. To issue a document containing consent directly to the data subject, deliver via mail or facsimile, or obtain the document on which the data subject fixed signature or seal;
2. To inform the data subject of the consent via telephone, and confirm his/her intent of consent;
3. To inform the data subject of the consent via telephone, and let him/her confirm consent via the Internet, and reconfirm his/her intent of consent via telephone;
4. To post the content to be consented by the data subject on the website, and let him/her express his/her consent to it;
5. To send e-mail with the content to be consented by the data subject, and receive the return e-mail with his/her consent to it; or
6. Other method to inform the data subject of the content to be consented in a way similar to Subparagraphs 1 through 5, and confirm his/her intent of consent.

(2) The personal information processor may, in order to obtain the consent from the legal representatives of minors of age below 14 pursuant to Article 22(5) of the Act, collect the information on the name and address of their legal representatives directly from such minors.

(3) The head of central administrative department or agency may, of various methods of consent stated in Paragraph (1), advise the personal information processor to selectively obtain the appropriate consent based on the standard of the Personal Information Protection Guidelines (hereinafter referred to as the “Guidelines”) established pursuant to Article 12(2) of the Act in consideration of the characteristics of business and the number of data subjects, etc. of the personal information processor under its jurisdiction.

#### **Article 18 (Scope of Sensitive Information)**

The “information as stated by the Presidential Decree” in the main sentence other than

each Subparagraph in Article 23 of the Act shall mean any of the following Subparagraphs; *provided, however*, that, where the public institution processes any of the following Subparagraphs pursuant to Subparagraphs 5 through 9 of Article 18(2) of the Act, the said information shall be excluded therefrom:

1. DNA information acquired from genetic examination, etc.; or
2. Criminal history data pursuant to Article 2v of the Act Regarding the Extinction of Punishment.

#### **Article 19 (Scope of Unique Identifiers)**

The “information as stated by the Presidential Decree” in the provision other than each Subparagraph in Article 24(1) of the Act shall mean any of the following Subparagraphs (hereinafter referred to as the “Unique Identifier”); *provided, however*, that, where the public institution processes any of the following Subparagraphs pursuant to Subparagraphs 5 through 9 of Article 18(2) of the Act, the said information shall be excluded therefrom:

1. The resident registration number pursuant to Article 7(3) of the Resident Registration Act;
2. The passport number pursuant to Article 7(1) i of the Passport Act;
3. The driver’s license number pursuant to Article 80 of the Road Transportation Act;
4. The alien registration number pursuant to Article 31(4) of the Immigration Control Act;

#### **Article 20 (Provider of Obligatory Sign-up Process Other than Resident Registration Number)**

(1) The personal information processor who is required to provide sign-up process without the resident registration number (hereinafter referred to as the “Alternative Sign-up Tool”) pursuant to Article 24(2) of the Act shall mean any of the following Subparagraphs:

1. The public institution; or
2. The personal information processor, other than the public institution, who is operating the webpage whose visitors exceed 10 thousand on average a day during the preceding three months as of the of the previous year.

(2) The MOPAS shall, with regard to the provision of the Alternative Sign-up Tool subject to Paragraph (1), post the matters in the following Subparagraphs on its webpage:

1. The name and URL address of the website of the personal information processor who is required to provide the Alternative Sign-up Tool subject to Paragraph (1);
2. The type and substance of the Alternative Sign-up Tool to be provided; and

3. The period for which the Alternative Sign-up Tool is provided.

**Article 21 (Safety Measures of Unique Identifiers)**

Article 30 shall apply *mutantis mutandis* to the safety measures subject to Article 24(3) of the Act. In this case, Article 29 of the Act shall read Article 24(3) of the Act, and the personal information shall read the Unique Identifier,

**Article 22 (Exception to the Limitation to Installation and Operation of Visual Data Processing Devices)**

- (1) The “facilities as stated by the Presidential Decree” in the proviso of Article 25(2) of the Act shall mean any of the following Subparagraphs:
  1. The penitentiary facilities subject to Article 2 iv of the Act Concerning the Enforcement of Punishment and Treatment of Inmates;
  2. The mental health care institution (with accommodation facilities), mental patient rehabilitation facilities and mental treatment facilities subject to Article 3 iii, iv and v of the Mental Health Act;
- (2) The head of central administrative department or agency may establish detailed matters necessary to ensure the privacy of data subjects to be infringed upon to the minimum extent into the Personal Information Protection Guidelines, and encourage the Guidelines to be complied with where the personal information processor under its jurisdiction installs and operates the visual data processing devices at the facilities specified in Paragraph (1) pursuant to the proviso of Article 25(2) of the Act.

**Article 23 (Gathering Opinion on Visual Data Processing Devices)**

- (1) The head of public institution who intends to install and operate visual data processing devices pursuant to each Subparagraph of Article 25(1) of the Act shall gather opinions from relevant specialists and interested parties subject to any procedure of the following Subparagraphs:
  1. The administrative notification in advance or gathering opinions under the Administrative Procedure Act; or
  2. An explanatory meeting, survey or polling for the neighborhood residents, etc. directly affected by the installation of the very visual data processing devices.
- (2) Any person who intends to install and operate the visual data processing devices at the facilities subject to the proviso of Article 25(2) of the Act shall gather opinions from the persons specified in each of the following Subparagraphs.
  1. The related specialists; or
  2. Anyone engaged in the pertinent facilities, any person confined or accommodated in

the pertinent facilities, or interested parties including the guardian of the said person.

**Article 24 (Positing of Notice)**

(1) Any person who intends to install and operate visual data processing devices pursuant to each Subparagraph of Article 25(1) of the Act (hereinafter referred to as the “V/D Operator”) shall post the matters as mentioned in the following Subparagraphs on a signboard pursuant to the main sentence of Article 25(4) of the Act so that data subjects may recognize it with ease; *provided, however*, that a signboard, indicating the operation of visual data processing devices in the pertinent facilities and whole area, may be posted at the entry and other easily noticeable place in case a multitude of visual data processing devices are installed in a building.

1. The purpose and place of installation;
2. The scope and time of filming; and
3. The name of operator in charge and telephone number.

(2) Notwithstanding Paragraph (1), where the visual data processing device installed and operated by the V/D Operator falls on any of the following Subparagraphs, the V/D Operator may post the matters as specified in each Subparagraph of Paragraph (1) on its website instead of posting of the said signboard:

1. Where the visual data processing device installed by the public institution for the purpose of long distance filming, over-speed and traffic signal violation enforcement service or traffic flow survey, etc. and the possibility of data breach is significantly low; or
2. Where a signboard is hardly to be posted because of terrain characteristics or is not easily noticeable to data subjects, i.e., a visual data processing device installed for surveillance of mountain fire.

(3) Unless the matters as specified in each Subparagraph of Paragraph (1) can be posted on its website, the V/D Operator shall make public the said matters in each Subparagraph of Paragraph (1) in a way of more than one of the following Subparagraphs:

1. Posting at easily noticeable places at the V/D Operator’s workplace, business premise, office, stores, etc. (hereinafter referred to as the “workplace”); and/or
2. Publishing at the Official Gazette (only in case the V/D Operator is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the Special City, Metropolitan City, Province or Special Self-governing Province (hereinafter referred to as the “City and Province”) where the V/D Operator’s workplace is located.

(4) The head of public institution may not install the signboard pursuant to the proviso of Article 25(4) with regard to the visual data processing device installed at the facilities as specified at any of the following Subparagraphs:

1. Military facilities subject to Article 2 ii of the Military Base and Military Facilities Protection Act;
2. National key facilities subject to Article 2 xiii of the Integrated Defence Act; or
3. Security target facilities subject to Article 36 of the Security Work Regulation.

**Article 25 (Policy on the Operation and Maintenance of Visual Data Processing Devices)**

(1) The V/D Operator shall establish the policy to operate and maintain visual data processing devices including the following Subparagraphs pursuant to Article 25(7) of the Act:

1. The statutory ground and purpose to install visual data processing devices;
2. The number of visual data processing devices installed, the location of installation and the scope of filming;
3. The manager and department in charge, and the person who is entitled to access the visual information;
4. The duration time of filming, retention period, retention place and processing method of the visual information;
5. The method how, and the place where, the V/D Operator checks the visual information;
6. The measures taken to meet the data subject's request to access the visual information;
7. The technical, managerial and physical safeguards to protect the visual information; and
8. Other things necessary to install, operate and maintain the visual data processing devices.

(2) Article 31(2) and (3) shall apply *mutantis mutandis* to the disclosure of the policy to operate and maintain visual data processing devices established pursuant to Paragraph (1). In this case, the personal information processor shall read the V/D Operator, and for Article 30(2) of the Act, read Article 25(7) of the Act, and for the privacy policy, read the policy on the operation and maintenance of visual data processing devices, respectively.

**Article 26 (Entrusting the Installation and Operation of Visual Data Processing Devices of Public Institutions)**

(1) Where the public institution outsources or entrusts the installation and operation of

visual data processing devices to others pursuant to the proviso of Article 25(8) of the Act, it shall do so by means of the document containing the following Subparagraphs:

1. The purpose and scope of entrusted work;
2. Matters regarding restriction of re-entrusting;
3. Matters regarding the safety measures including restriction of access to visual data;
4. Matters regarding inspection of the status quo of visual data retained; and
5. Matters regarding damage liability in case of breach of contractual obligations on the part of the trustee.

(2) Where the outsourcing takes place pursuant to Paragraph (1), the signboard etc. subject to Article 24(1) through (3) shall include the name and telephone number of the trustee.

#### **Article 27 (Guidelines for the Installation and Operation of Visual Data Processing Devices)**

The MOPAS may establish the Standard Personal Information Protection Guidelines subject to Article 12(1) of the Act regarding the installation and operation standards of visual data processing devices, outsourcing of their installation and operation, etc. as well as other matters provided for in the Act and this Decree, and encourage the V/D Operator to comply with the Standard Guidelines.

#### **Article 28 (Measures taken when Outsourcing Personal Information Processing)**

(1) “Other things as stated by the Presidential Decree” in Article 26(1) iii shall mean any of the following Subparagraphs:

1. The purpose and scope of entrusted work;
2. Matters regarding restriction of re-entrusting;
3. Matters regarding the safety measures including restriction of access to personal information;
4. Matters regarding supervision and inspection of the status quo of personal information retained in relation to outsourcing; and
5. Matters regarding damage liability in case of breach of contractual obligations on the part of the consignee subject to Article 26(2) of the Act (hereinafter referred to as the “consignee”).

(2) “Such a way as stated by the Presidential Decree” in Article 26(2) of the Act shall mean the manner in which the personal information processor entrusting the processing of personal information (hereinafter referred to as the “consignor”) posts continuously the entrusted works and the consignee on its website.

(3) If it is not possible to post on the website pursuant to Paragraph (2), the consignor shall make public the entrusted works and the consignee in a way of more than one of

the following Subparagraphs:

1. Posting at easily noticeable places of the consignor's workplace, etc.;
  2. Publishing at the Official Gazette (only in case the consignor is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the City and Province where the consignor's workplace is located.
  3. Publishing at a periodical, newsletter, PR magazine or invoice to be published under the same title more than twice a year and distributed to data subjects on a continual basis; and/or
  4. Delivering to the data subject the paper-based agreement entered into between the consignor and the data subject so as to supply goods and/or services.
- (4) "Such a way as stated by the Presidential Decree" in the first sentence of Article 26(3) of the Act shall mean in writing, e-mail, facsimile, telephone, short message service (SMS) or other way equivalent hereto (hereinafter referred to as the "in writing, etc.")
- (5) Where the consignor fails to inform the data subject of the entrusted work and the consignee in such a way as stated in Paragraph (4) without fault, it shall post the relevant matters on its website for more than 30 days; *provided, however*, that the consignor, if not operating the website, shall post them at easily noticeable places like workplace, etc. for more than 30 days.
- (6) Where the consignee carries out the processing of personal information, the consignor shall supervise what the personal information processor is required to comply with pursuant to the Act and this Decree and has complied with each Subparagraph of Article 26(1) of the Act, pursuant to Article 26(4) of the Act.

**Article 29 (Notification of Transfer of Personal Information following Business Transfer, etc.)**

- (1) "Such a way as stated by the Presidential Decree" in the main sentence other than each Subparagraph of Article 27(1) and in the main sentence of Article 27(2) of the Act shall mean in writing, etc.
- (2) Where a person intends to transfer the personal information pursuant to Article 27(1) of the Act (hereinafter referred to as the "transferor" in this Paragraph) fails to inform the data subject of the matters as stated in each Subparagraph of Article 27(1) of the Act in such a way as stated in Paragraph (1) without fault, it shall post the relevant matters on the website for more than 30 days; *provided, however*, that the transferor, if not operating the website, shall post them at easily noticeable places like workplace,

etc. for more than 30 days.

## **Chapter 5. Safe Maintenance of Personal Information**

### **Article 30 (Safety Measures of Personal Information)**

- (1) The personal information processor shall take measures to ensure the safety of each of the following Subparagraphs pursuant to Article 29 of the Act:
1. To set up and implement the internal management plan for the safe processing of personal information;
  2. To control access to the personal information and restrict the authority to access hereto;
  3. To adopt such encryption technology as to store and transmit the personal information in safety and other measures equivalent hereto;
  4. To retain log-in records in order to respond data breach incidents and to take measures to prevent the forgery and falsification hereof;
  5. To install and upgrade security programs to protect personal information;
  6. To take such physical measures as storage to keep personal information in safety or locking system; or
- (2) The MOPAS may provide such necessary assistance as building up the system with which the personal information processor may secure the safety measures subject to Paragraph (1).
- (3) The MOPAS shall make and notify the detailed standards regarding safety measures subject to Paragraph (1).

### **Article 31 (Establishment and Disclosure of Privacy Policy)**

- (1) “Other matters as stated in the Presidential Decree” in Article 20(1) vi shall mean the matters of following Subparagraphs:
1. Items of personal information to be processed;
  2. Matters in relation to destruction of personal information; and
  3. Matters in relation to safety measures of personal information subject to Article 30.
- (2) The personal information processor shall post continuously the Privacy Policy established or modified pursuant to Article 30(2) of the Act on its website.
- (3) If it is not possible to post on the website pursuant to Paragraph (2), the personal information processor shall make public the Privacy Policy established or modified in a way of more than one of the following Subparagraphs:
1. Posting at easily noticeable places of the personal information processor’s workplace, etc.;

2. Publishing at the Official Gazette (only in case the personal information processor is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the City and Province where the personal information processor's workplace is located.
3. Publishing at a periodical, newsletter, PR magazine or invoice to be published under the same title more than twice a year and distributed to data subjects on a continual basis; and/or
4. Delivering to the data subject the paper-based agreement entered into between the personal information processor and the data subject so as to supply goods and/or services.

**Article 32 (Duty of Privacy Officer and Qualification, etc.)**

- (1) "Other functions as stated by the Presidential Decree" in Article 31(2) vii shall mean any of the following Subparagraphs:
  1. The Privacy Policy established, modified and implemented pursuant to Article 30 of the Act;
  2. Maintenance of materials related with personal information protection; and
  3. Destruction of personal information whose purpose of processing is attained or retention period expires.
- (2) The personal information processor shall, in case of designating the privacy officer pursuant to Article 31(1) of the Act, designate him/her by category of the following Subparagraphs:
  1. The public institution: Public officials, etc. who satisfy the standards by category of the following Items:
    - a. The administrative bodies of the National Assembly, the Court, the Constitutional Court and the National Election Commission, the central administrative departments or agencies: public official who belongs to the College of High-ranking Government Officials (hereinafter referred to as the "high-ranking public official") or the public official equivalent hereto;
    - b. Other national institution than Item a, headed by a public official in political service: 3<sup>rd</sup> grade or higher public official (including the high-ranking public official) or the public officials equivalent hereto;
    - c. Other national institution than Items a and b, headed by a high-ranking public official, 3<sup>rd</sup> grade public official or the public officials equivalent hereto or higher: 4<sup>th</sup> grade or higher official or the public officials equivalent hereto;
    - d. Other national institution than Items a. through c. (including their affiliated bodies):

- head of the department in charge of data protection of the relevant institution;
- e. City and Province and the Office of Education hereof: 3<sup>rd</sup> grade or higher public official or the public officials equivalent hereto;
  - f. City, County and Self-governing Gu: 4<sup>th</sup> grade public official or the public official equivalent hereto;
  - g. Each level of school subject to Article 2 v: a person in charge of whole administrative affairs of the relevant school;
  - h. Other public institution than the institution subject to Items a. through g.: head of the department engaged in personal information processing-related works; *provided, however,* that, in case there are two or more heads of the department engaged in personal information processing-related works, the head of the pertinent institution shall designate the privacy officer among them.
2. The personal information processor other than the public institution: a person who satisfies any of the following Items:
- a. Business proprietor or representative; or
  - b. Head of the department engaged in personal information processing-related works or a person who has good knowledge in data protection.
- (3) The MOPAS may provide such necessary assistance as establishing and running the education programs for the privacy officers so that they may efficiently carry out the job stated in Article 31(2) of the Act.

### **Article 33 (Registered Items of Personal Information Files)**

“Other matters as stated by the Presidential Decree” in Article 32(1) vii shall mean any of the following Subparagraphs:

1. The name of public institution operating personal information files;
2. The number of data subjects whose data are retained in personal information files;
3. The department of the public institution, engaged in personal information processing-related works
4. The department receiving and processing the request to access personal information subject to Article 41; and
5. The scope of personal information to which access is restricted or denied of personal information in the relevant files pursuant to Article 35(4) of the Act, and the ground for such restriction or denial.

### **Article 34 (Registration and Disclosure of Personal Information Files)**

- (1) The head of public institution operating personal information files shall apply for registration of such items subject to Article 32(1) of the Act and Article 33 of this

Decree (hereinafter referred to as the “registered items”) to the MOPAS within 60 days from the day starting its operation in accordance with the MOPAS Ordinance. The same shall apply to the modifications of registered items after registration.

- (2) The MOPAS shall post the status quo of registered personal information files pursuant to Article 32(4) of the Act on its website.
- (3) The MOPAS may build up and operate the systems so that the registration or modification of the registered items may be electronically processed.

#### **Article 35 (Object of Privacy Impact Assessment)**

The “personal information files applicable to the criteria as specified by the Presidential Decree” in Article 33(1) shall mean the personal information files which can be processed electronically and conform to any of the following Subparagraphs:

1. The personal information files which will be established, operated or modified, and contain the sensitive data subject to Article 23 of the Act (hereinafter referred to as the “sensitive data”) or Unique Identifiers of more than 50 thousand data subjects for processing;
2. The personal information files which is established and operated, and will be matched with other personal information files being established and operated inside or out of the relevant public institution, and, as a result of matching, will contain the personal information of more than 50 thousand data subjects;
3. The personal information files which will be established, operated or modified, and contain the personal information of more than one million data subjects; or
4. The personal information files of which operating system, including the data retrieval system, will be changed after the privacy impact assessment subject to Article 33(1) of the Act (hereinafter referred to as the "PIA"). In this case, the PIA shall be limited to the changed system.

#### **Article 36 (Consideration at the time of PIA)**

The “other matters as stated by the Presidential Decree” in Article 33(2) iv shall mean any of the following Subparagraphs:

1. Whether sensitive data or Unique Identifiers will be processed; or
2. The retention period of personal information.

#### **Article 37 (Designation of PIA institution and Cancellation hereof)**

- (1) The MOPAS may designate the legal entity, which satisfies all the requirements of the following Subparagraphs pursuant to the second sentence of Article 33(1) of the Act, as the PIA institution:

1. The juristic person whose total revenue paid for the works which fall under any of the following Items is more than 200 million won for the preceding five years:
    - a. PIA works or equivalent hereto;
    - b. Data protection consulting (meaning the analysis and assessment of information systems and the provision of corresponding countermeasures against electronic incidents. The same applies hereafter) of the works building up the information systems (including data protection system) subject to Article 2 xiii of the Electronic Government Act;
    - c. Data protection consulting of the works monitoring the information systems subject to Article 2 xiv of the Electronic Government Act;
    - d. The works conducted pursuant to Article 33(1) i and ii of the Information and Communications Industry Promotion Act; and
    - e. Data protection consulting of the works to be included in the data protection industry subject to Article 2 viii of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.
  2. The juristic person who employs regularly more than 10 professionals subject to Schedule 1;
  3. The juristic person who is equipped with the office and facilities in the following Items:
    - a. The office with facilities for identification and entry control; and
    - b. Facilities for the safe maintenance of data and materials.
- (2) Anyone who intends to be designated as a PIA institution shall submit to the MOPAS the Application for PIA Institution with attachments (including electronic message. The same applies hereto.) as specified in the following Subparagraphs subject to the MOPAS Ordinance:
1. The articles of incorporation;
  2. The name of representative and officers;
  3. The documents verifying the professional qualifications subject to Paragraph (1) ii; and
  4. Other documents as specified by the MOPAS Ordinance.
- (3) Upon receipt of the Application for PIA Institution pursuant to Paragraph (2), the MOPAS shall, through the sharing of administrative information subject to Article 36(1) of the Electronic Government Act, check each document specified in the following Subparagraphs; *provided, however*, that, in case the applicant would not consent to the confirmation of Subparagraph 2, the pertinent document shall be attached thereto:
1. The certificate of registry of the juristic person; and
  2. The certificate of alien registration subject to Article 88(2) of the Immigration

Control Act (applicable to only aliens).

- (4) Upon designation of the PIA institution subject to Paragraph (1), the MOPAS shall, without delay, issue a letter to designate the PIA Institution, and notify the specifications of the following Subparagraphs via the Official Gazette. The same applies to the modification of such notified specifications:
1. The name, address and telephone number of the PIA institution, and the name of its representative; and
  2. The conditions attached to the designation, if any.
- (5) The MOPAS may cancel the designation of the PIA institution subject to Paragraph (1) if such designated PIA institution falls under any of the following Subparagraphs; *provided, however*, that the MOPAS shall cancel the designation in case of Subparagraphs 1 and 2.
1. Where the PIA institution has been designated by fraudulent or unfair means;
  2. Where the PIA institution wants the cancellation of such designation or has wound up its business;
  3. Where the PIA institution cannot satisfy any more the qualifications subject to Paragraph (1);
  4. Where the PIA institution fails to perform the duty of report subject to Paragraph (6);
  5. Where the PIA institution has conducted the PIA work with wrongful intent or grave negligence, and is deemed incapable of duly conducting PIA works; or
  6. Other breaches of duty subject to this Act or this Decree.
- (6) The PIA institution designated subject to Paragraph (1) shall, upon occurrence of any of the following Subparagraphs after designation hereof, report to the MOPAS within seven (7) days from the day of such occurrence in accordance with the MOPAS Ordinance; *provided, however*, that it shall report within 30 days from the day of such occurrence in case of Subparagraphs 3:
1. Where any of the Subparagraphs of Paragraph (1) has been changed;
  2. Where the matter stated in Paragraph (4) i has been changed; or
  3. Where the transfer or merger of the PIA institution has occurred;
- (7) Where the MOPAS intends to cancel the designation of the PIA institution pursuant to Paragraph (5), the MOPAS shall hold hearings thereon.

#### **Article 38 (Criteria of Privacy Impact Assessment)**

- (1) The criteria of PIA subject to Article 33(6) of the Act are any of the following Subparagraphs:
1. The type and characteristics of personal information processed by the relevant public

- institution, the number of data subjects, and the possibility of subsequent data breach;
2. The standard of the safety measures subject to Articles 24(3), 25(6) and 29 of the Act, and the possibility of subsequent data breach;
  3. The countermeasure against data breach risk factors, if any; and
  4. Other necessary measures subject to the Act or this Decree, or any factor affecting breach of duties.
- (2) The PIA institution which is requested to do PIA pursuant to Article 33(1) of the Act shall prepare the PIA report containing the assessment stated in the following Subparagraphs, and send the report to the head of the pertinent public institution, after it has analysed and assessed the data breach risk factors arising out of the operation of personal information files according to the PIA criteria specified in Paragraph (1). The head of the pertinent public institution shall submit the PIA report to the MOPAS (including improving measures subject to Subparagraph 3, if any problem in the PIA report) prior to the build-up and operation of the personal information files in conformity with each Subparagraph of Article 35 of the public institution:
1. The summary of works related with, and the purpose of, the operation of personal information files;
  2. Outline of personal information files, object of PIA;
  3. The analysis and assessment of the data breach risk factors according to the PIA criteria and the measures in need of improvement; and
  4. Manpower conducting PIA, and cost and expenses.
- (3) The MOPAS may establish detailed standards regarding the designation of the PIA institution and the PIA process in addition to the provisions of the Act and this Decree, and notify it.

#### **Article 39 (Scope of Data Breach Notification and Where to Report)**

- (1) The “data breach above the level specified by the Presidential Decree” shall mean the personal information of over 10 thousand data subjects.
- (2) The “specific institution stated in the Presidential Decree” in the first and second sentence of Article 34(3) of the Act shall mean any of the following Subparagraphs:
  1. The National Information Agency (NIA) subject to Article 14 of the Framework Act on National Information; or
  2. The Korea Internet and Security Agency (KISA) subject to Article 52 of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.

#### **Article 40 (Method and Procedure of Data Breach Notification)**

- (1) When the personal information processor becomes to know that personal information is leaked, it shall, without delay, notify in writing, etc. the aggrieved data subjects of the fact in the Subparagraphs of Article 34(1) of the Act; *provided, however*, that the personal information processor may give notice to the data subjects without delay right after it has taken contingent measures, including shut-down of access route, check-up of weak point and deletion of leaked personal data, necessary to prevent the dissemination of leaked data and additional leakage.
- (2) Notwithstanding Paragraph (1), where the personal information processor became to know the data leakage pursuant to the main sentence of Paragraph (1), took contingent measures after awareness of the data breach pursuant to the proviso of Paragraph (1), but could not confirm the detailed data breach specified by Article 34(1) i and ii of the Article, the personal information processor is allowed to notify the data subjects at first of the fact of data breach and confirmed leakage of data in writing, etc. and later confirmed facts additionally.
- (3) Notwithstanding Paragraphs (1) and (2), where the personal information of over 10 thousand data subjects has been leaked pursuant to Article 34(3) of the Act and Article 39(1) of this Decree, in addition to notification in writing, etc. the personal information processor shall post the relevant matters stated in Subparagraphs of Article 34(1) of the Act on its website for more than seven (7) days; *provided, however*, that the personal information processor, if not operating the website, shall post the relevant matters stated in Subparagraphs of Article 34(1) of the Act at easily noticeable places like workplace, etc. for more than seven (7) days.

## **Chapter 6. Ensuring the Rights of Data Subjects**

### **Article 41 (Access to Data Procedure, etc.)**

- (1) Where the data subject requests the access to his/her own personal information pursuant to Article 35(1) and (2) of the Act, he/she shall submit to the personal information processor the Personal Information Access Request specifying the matter to access among the following Subparagraphs in accordance with the MOPAS Ordinance:
  1. The item and substance of personal information;
  2. The purpose of collection and use of personal information;
  3. The period when personal information is retained and used;
  4. The status quo of personal information provided to a third party; and
  5. The fact that the data subject has given consent to data processing, and the content hereof.
- (2) Where the data subject intends to demand the access to his/her own personal

information via the MOPAS pursuant to Article 35(2) of the Act, he/she shall submit to the MOPAS the Personal Information Access Request subject to Paragraph (1). In this case, the MOPAS shall, without delay, forward the Personal Information Access Request to the pertinent public institution.

- (3) The “period as stated by the Presidential Decree” in the first sentence of Article 35(3) of the Act shall mean ten (10) days.
- (4) Where the personal information processor allows the data subject to access the relevant data within ten (10) days from the day of receipt of the Personal Information Access Request subject to Paragraph (1), and allows the data subject to access only a part of the requests subject to Article 42(1), the personal information processor shall inform the relevant data subject, by means of the Access Notification determined by the MOPAS Ordinance, of the personal information to access and the date, time, venue, etc. (In case of partial access of the Access Request subject to Article 42(1), the ground hereof and how to appeal shall be included herein.)

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

- (1) Where a part of the access request subject to Article 41(1) falls under any of Subparagraphs of Article 35(4) of the Act, the personal information processor may restrict the access to such part, but shall ensure the data subject to access other personal information than the restricted part.
- (2) Where the personal information processor intends to postpone access of the data subject pursuant to the second sentence of Article 35(3) of the Act, or deny access of the data subject pursuant to Article 35(4) of the Act, the personal information processor shall inform the relevant data subject of the grounds for the access postponement and denial and the method how to appeal by means of the Access Postponement and Denial Notice determined by the MOPAS Ordinance within ten (10) days from the day of receipt of the access request.

**Article 43 (Correction, Deletion, etc. of Personal Information)**

- (1) Where the data subject intends to demand the personal information processor to correct or delete the personal information pursuant to Article 36(1) of the Act, he/she shall submit to the pertinent personal information processor the Personal Information Correction or Deletion Request determined by the MOPAS Ordinance.
- (2) The personal information processor processing personal information provided by other personal information processor shall, upon receipt of the correction or deletion request of personal information pursuant to Article 36(1) of the Act, correct or delete the relevant personal information as requested, or shall, without delay, forward such request

to the head of pertinent institution which has provided the relevant personal information, and take necessary measures in view of the outcome hereof.

- (3) The personal information processor shall inform the pertinent data subject of the fact that it has duly corrected or deleted the relevant personal information pursuant to Article 36(2) of the Act within ten (10) days from the day of receipt of the correction or deletion request subject to Paragraphs (1) and (2); otherwise, if the personal information processor did not follow the deletion request because it falls under the proviso of Article 36(1) of the Act, it shall inform the relevant data subject of the fact and grounds for the denial, and the method how to appeal by means of the Personal Information Correction or Deletion Outcome Notice determined by the MOPAS Ordinance.

#### **Article 44 (Suspension of Processing of Personal Information)**

- (1) The data subject, who intends to demand the personal information processor to suspend the processing of his/her own personal information pursuant to Article 37(1) of the Act, shall submit to the personal information processor the Personal Information Processing Suspension Request determined by the MOPAS Ordinance.
- (2) The personal information processor shall inform the pertinent data subject of the fact that it has duly suspended the processing of personal information pursuant to the main sentence of Article 37(2) of the Act within ten (10) days from the day of receipt of the processing suspension request subject to Paragraph (1); otherwise, if the personal information processor did not follow the processing suspension request because it falls under the proviso of Article 37(2) of the Act, it shall inform the relevant data subject of the fact and grounds for the denial, and the method how to appeal by means of the Personal Information Processing Suspension Outcome Notice determined by the MOPAS Ordinance.

#### **Article 45 (Scope of Attorneys)**

- (1) The person who may represent the data subject pursuant to Article 38 of the Act is any of the following Subparagraphs:
1. A legal representative of the data subject; or
  2. A person who is delegated by the data subject.
- (2) The attorney subject to Paragraph (1), representing the data subject pursuant to Article 38 of the Act, shall submit to the personal information processor the power of attorney of the data subject determined by the MOPAS Ordinance.

#### **Article 46 (Confirmation of Data Subject or Attorney)**

- (1) Where the personal information processor has received the access request subject to

Article 41(1), the correction or deletion request subject to Article 43(1), the processing suspension request subject to Article 44(1) (hereinafter in Articles 46 through 48 referred to collectively as the “request of access, etc.”), it shall confirm if the person doing the request of access, etc. is the principal or duly authorized attorney.

- (2) Where the personal information processor, which is the public institution eligible for sharing of administrative information subject to Article 36(1) of the Electronic Government Act, shall, through the sharing of administrative information, confirm as provided in Paragraph (1); *provided, however*, that the same shall not apply in case the pertinent public institution is not able to share administrative information or the data subject would not consent to such confirmation.

#### **Article 47 (Amount of Fees, etc.)**

- (1) The amount of the fee and postage as stipulated in Article 38(3) of the Act shall be determined by the pertinent personal information processor within the scope of actual cost necessary for the request of access, etc.; *provided, however*, that, it is subject to the ordinance of the relevant local government if the personal information processor is the local government.
- (2) The personal information processor shall not claim the fee and postage if the cause of the request of access, etc. is on the part of personal information processor.
- (3) The payment of the fee or postage as stipulated in Article 38(3) of the Act shall be made by the category in the following Subparagraphs; *provided, however*, that the personal information processor, which is the National Assembly, the Court, the Constitutional Court and the National Election Commission, the central administrative department or its affiliated agency (hereinafter in this Article referred as the “State institution”) or local government, may claim the fee or postage by the electronic payment means subject to Article 2 xi of the Electronic Financial Transactions Act, or via the communications billing services subject to Article 2 x of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.:
1. In case of the personal information processor which is the State institution: revenue stamp;
  2. In case of the personal information processor which is the local government: revenue certificate;
  3. In case of other personal information processor than the State institution and local government: such payment method as determined by the relevant personal information processor.

#### **Article 48 (Build-up of Access Request Supporting System, etc.)**

- (1) The personal information processor may build up and operate the supporting system which processes electronically the access request, etc. and notifications hereto, and establish other work procedures.
- (2) The MOPAS may build up and operate the system so that the MOPAS may support efficiently the public institution to process the access request, etc. and notifications hereto in relation to the personal information maintained by the public institution.

## **Chapter 7. Personal Information Dispute Mediation**

### **Article 49 (Composition of Mediation Panels and Operation)**

- (1) The mediation panel subject to Article 40(6) of the Act (hereinafter referred as the “mediation panel”) shall be composed of five or less Committee members, designated by the Chairperson of the Personal Information Dispute Mediation Committee subject to Article 40(1) of the Act (hereinafter referred to as the "Dispute Mediation Committee" or abbreviated as DMC), but one of whom shall be a Commissioner with an attorney-in-law license.
- (2) The DMC Chairperson shall call the meeting the mediation panel.
- (3) The DMC Chairperson shall notify each member of the mediation panel of the date, time, venue and agenda no later than seven (7) days prior to the meeting; *provided, however,* that the same shall not apply in case of emergency.
- (4) The presider of the mediation panel shall be elected by the mediation panel among its members.
- (5) Other necessary matters regarding the composition and operation of the mediation panel than the provisions in Paragraphs (1) through (4) shall be determined by the DMC Chairperson subject to the deliberations of the Dispute Mediation Committee.

### **Article 50 (Secretariat, etc.)**

- (1) The secretariat of the Dispute Mediation Committee subject to Article 40(8) of the Act shall conduct its functions including investigation of dispute mediation cases by the order of the DMC Chairperson.
- (2) The MOPAS shall designate the Korean Internet and Security Agency as a specialized institution supporting the Dispute Mediation Committee with the operation of its secretariat pursuant to Article 40(8) of the Act.

### **Article 51 (Operation of Dispute Mediation Committee, etc.)**

- (1) The DMC Chairperson shall convene the meeting of the Dispute Mediation Committee, and become its chairman.

- (2) The DMC Chairperson shall notify each member of the Dispute Mediation Committee of the date, time, venue and agenda no later than seven (7) days prior to the meeting; *provided, however,* that the same shall not apply in case of emergency.
- (3) The meetings of the Dispute Mediation Committee and the mediation panel shall not be open to the public; *provided, however,* that attendance of the parties or interested parties is allowed by the deliberation of the Dispute Mediation Committee if it is deemed necessary.

**Article 52 (Application for Collective Dispute Mediation)**

“Incidents stated by the Presidential Decree” in Article 49(1) of the Act shall mean the incidents which satisfy all requirements of the following Subparagraphs:

1. The number of the data subjects suffering from loss or infringement upon rights is more than 50 people except the data subjects in the following Items:
  - a. The data subjects who have agreement with the personal information processor on the dispute settlement or compensation of damages;
  - b. The data subjects whose dispute based on the same cause is dealt with by a dispute mediation body established by other statutes; or
  - c. The data subjects who has filed a lawsuit with a court against the relevant data breach incidents.
2. Major issues are common as a matter of fact or law.

**Article 53 (Initiation of Collective Dispute Mediation Procedure)**

- (1) The “period as specified by the Presidential Decree” in the second sentence of Article 49(1) of the Act shall mean the period of more than 14 days.
- (2) The notice of commencing the proceedings of the Collective Dispute Mediation subject to the second sentence of Article 49(2) of the Act shall be made on the website of the Dispute Mediation Committee as well as a general daily newspaper subject to the Act for the Promotion of Newspapers, etc. circulating all across the nation.

**Article 54 (Application for Participation in Collective Dispute Mediation Proceedings)**

- (1) The data subject or personal information processor other than the parties of the Collective Dispute Mediation subject to Article 49 of the Act (hereinafter referred to as the "Collective Dispute Mediation"), who intends to participate in the said Collective Dispute Mediation in addition as a party, shall apply for it in writing during the notice period subject to the second sentence of Article 49(2) of the Act.
- (2) The Dispute Mediation Committee shall, upon receipt of the application for the

Collective Dispute Mediation as a party pursuant to Paragraph (1), inform the applicant of whether it has accepted or not in writing within 10 days from the expiry of the notice period in Paragraph (1).

**Article 55 (Collective Dispute Mediation Proceedings)**

- (1) After the Collective Dispute Mediation proceedings start, the data subject who falls under any of the Items a. through c. of Article 52 i shall be excluded from the party.
- (2) Once the Collective Dispute Mediation proceedings of the case which satisfies each requirement of the Subparagraphs of Article 52 start, the failure to meet the requirement of Subparagraph 1 of Article 52, if any of Items a. through c. of Subparagraph 1 of the same Article is applicable, do not suspend the Collective Dispute Mediation proceedings.

**Article 56 (Attendance Fee and Transportation Expenses)**

The Commissioner who attended the meetings of the Dispute Mediation Committee or the mediation panel may be paid allowances and travel expenses within the scope of the budget; *provided, however*, that the same shall not apply when the public official attended the meeting directly related with his/her own work.

**Article 57 (Dispute Mediation Rule)**

Necessary matters regarding the operation of the Dispute Mediation Committee and the Collective Dispute Mediation other than the provisions of the Act and this Decree shall be determined by the DMC chairperson subject to the resolution of the Dispute Mediation Committee.

**Chapter 8. Miscellaneous and Penal Provisions**

**Article 58 (Advice for Improvement and Disciplinary Action)**

- (1) The advice for improvement subject to Article 61(2) and (3) of the Act and the disciplinary action subject to Article 65(2) and (3) of the Act shall be made in writing which clarifies explicitly the matters to be advised, grounds hereof and outcome of the action, period for return mail, etc.
- (2) The person who has received the advice pursuant to Paragraph (1) shall take necessary measures in line with the advice, and notify the MOPAS or the head of relevant central administrative department or agency of the outcome in writing; *provided, however*, that in case of special circumstances, in which it is deemed difficult to take measures as advised, such circumstances shall be explained to the addressee.

**Article 59 (Report of Violations, etc.)**

The MOPAS shall designate the Korea Internet and Security Agency as a specialized institution performing efficiently the work to receive and handle the claim report on data protection-related right or interests pursuant to Article 62(2) of the Act.

**Article 60 (Demand of Submission of Materials and Inspection)**

- (1) The “case as stated in the Presidential Decree” in Article 63(1) iii of the Act shall mean the case where data subject’s right or interest has been breached like personal information leakage, etc. or data breach probability is significantly high.
- (2) The MOPAS may request the head of the Korea National Information Agency or the Korea Internet and Security Agency to provide necessary assistance including technic advice to handle submission of materials and inspection hereof.

**Article 61 (Disclosure of Investigation Results)**

- (1) The MOPAS and the head of relevant central administrative department or agency shall make the matters in the following Subparagraphs on the website as well as a general daily newspaper subject to the Act for the Promotion of Newspapers, etc. circulating all across the nation:
  1. The substance of violations;
  2. The violators; and
  3. The advice for improvement, corrective order, accusation, disciplinary advice and imposition of fine for negligence and the outcome hereof.
- (2) In case of disclosure of the matters in the following Subparagraphs of Paragraph (1) pursuant to Article 66(1) and (2) of the Act, the MOPAS and the head of relevant central administrative department or agency shall take into consideration the substance and degree of violations, violation period and frequency, the scope of damage caused by violations and the outcome hereof.
- (3) Prior to request for PIPC’s deliberation and resolution subject to Article 66(1) of the Act, the MOPAS and the head of relevant central administrative department or agency shall inform the person to be disclosed of such fact and give him/her an opportunity to submit evidentiary materials or defensive opinion.

**Article 62 (Delegation of Authority)**

- (1) The MOPAS shall entrust the authority in the following Subparagraphs to the Korea National Information Agency:
  1. Education and public relations for data protection subject to Article 13(1) of the Act;

2. Fostering relevant specialists and developing PIA criteria subject to Article 33(5) of the Act;
  3. Receiving and processing access request subject to Article 35(2) of the Act; and
  4. Receiving the PIA Institution Application subject to Article 37(2) and receiving the report subject to Article 37(6).
- (2) The MOPAS shall entrust the authority to support the provision of the Alternative Sign-up Tool to the Korea Local Information Research & Development Institute subject to Article 72(1) of the Electronic Government Act.
- (3) The MOPAS shall entrust the authority to request materials and inspection subject to Article 63 of the Act (applicable only to receiving and processing of reports addressed to the DP Call Center subject to Article 62 of the Act) to the Korean Internet and Security Agency.

**Article 63 (Imposition of Fine for Negligence)**

The criteria for the imposition of the fine for negligence subject to Paragraphs (1) through (3) of Article 75 of the Act shall be as stated in Schedule 2.

**ADDENDA**

**Article 1 (Enforcement Date)**

This Decree shall enter into force on September 30, 2011; *provided, however*, that Article 20 and Item i of Paragraph 2 shall enter into force on March 30, 2012.

**Article 2 (Repeal of Other Statute)**

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

**Article 3 (Transitional Measures Regarding the Basic Plan and the Implementation Plan)**

*omitted*

**Article 4 (Transitional Measures Regarding the Encryption of Personal Information collected and retained by Personal Information Processor)**

The personal information processor who has collected and retained personal information as at the Enforcement Date shall complete the encryption of the personal information stored in electronic media (including the Unique Identifier to which Article 21 shall apply) subject to Article 30(1) iii by December 31, 2012.

**Article 5 (Transitional Measures Regarding the Registration of Personal Information Files)**

The head of public institution, which operates personal information files as at the Enforcement Date (excluding the public institution which has already registered personal information files prior to the Enforcement Date), shall apply for the registration thereof to the MOPAS pursuant to Article 34 within 60 days from the Enforcement Date.

**Article 6 (Transitional Measures Regarding PIA)**

The head of public institution operating, or building up to operate, personal information files subject to the Subparagraphs of Article 35 as at the Enforcement Date shall conduct the PIA of the relevant personal information files within five (5) years from the Enforcement Date, and submit the result hereof to the MOPAS.

**Article 7 (Amendment to Other Statutes)**

(1) A part of the Enforcement Decree of the Act on the Fair Franchise Business shall be amended as follows:

In Article 5-4(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) through (6) *omitted*

**Article 8 (Relations to Other Acts and Regulations)**

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 Decree, if any provision of this Decree can apply to such circumstances, this Act or the corresponding provision of this Decree shall apply thereto instead of the previous provision.