PERSONAL INFORMATION PROTECTION ACT

Act No. 10465, Mar. 29, 2011

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose)

The purpose of this Act is to prescribe matters concerning the management of personal information in order to protect the rights and interests of all citizens and further realize the dignity and value of each individual by protecting personal privacy, etc. from collection, leakage, misuse and abuse of individual information.

Article 2 (Definitions)

The terms used in this Act shall be defined as follows:

1. The term "private information" means information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified, (including information by which the individual in question cannot be identified but can be identified through simple combination with other information);

2. The term "management" means to collect, create, record, save, hold, process, edit, search, output, correct, recover, use, provide, disclose, destroy personal information, and other acts similar thereto;

3. The term "subject of information" means a person who can be identified by the managed information and therefore is the subject of the given piece of information;

4. The term "personal information file" means an aggregate of personal information systematically arranged or organized according to a specific rule in order for the personal information to be readily retrievable;

5. The term "personal information manager" means a public institution, corporate body, organization, individual, etc. who manages personal information directly or via another person to administer personal information files as part of his/her duties;

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

(a) The National Assembly, courts, institutions that deal with administrative affairs of the National Election Commission, central administrative agencies (including agencies respectively under the direct jurisdiction of the President and the Prime Minister) and its affiliated agencies, and local governments;

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

7. The term "image data processing equipment" means equipment prescribed by Presidential Decree that is permanently installed in a certain space to photograph the images, etc. of a person or object, or to transmit such images via a wired or wireless network.

Article 3 (Principles for Protecting Personal Information)

1. A personal information manager shall make clear the purpose of managing personal information, collect personal information lawfully and legitimately, and limit the collection to the minimum extent necessary to achieve such purpose.

2. A personal information manager shall manage personal information within the appropriate extent necessary for achieving the purpose of managing the personal information, and not use it for the purposes other than intended ones.

3. A personal information manager shall guarantee that personal information is kept accurate, complete and up-to-date to the extent necessary for the purpose of managing the personal information.

4. A personal information manager shall manage personal information safely, in consideration of the risk that the rights of a subject of information may be infringed on and the level of accompanying risks depending on the management methods, kinds, etc. of personal information.

5. A personal information manager shall disclose to the general public matters concerning the management of personal information, including, but not limited to, personal information management policies, and guarantee the rights of a subject of information such as the right, etc. to request an inspection.

6. A personal information manager shall manage personal information in such a manner that the privacy infringement of a subject of information is minimized.

7. A personal information manager shall ensure that personal information is managed anonymously whenever such management is possible.

8. A personal information manager shall endeavor to gain the trust of a subject of information by fulfilling his/her responsibilities and obligations conferred or imposed by or under this Act, relevant Acts and subordinate statutes.

Article 4 (Rights of Subject of Information)

A subject of information has the following rights in connection with the management of his/her personal information:

1. A right to receive information concerning the management of personal information;

2. A right to choose and decide whether he/she consents to the management of his/her personal information, the scope of consent, and related matters;

3. A right to verify whether personal information is managed and to request an inspection of personal information (including issuance of a certified copy; hereinafter the same shall apply);

4. A right to request the suspension, correction, deletion and destruction of personal information;

5. A right to receive relief from damage caused by the management of personal information according to prompt and fair procedures.

Article 5 (Responsibilities of State, etc.)

1. The State and a local government shall devise policy measures to prevent any harmful effect from collecting personal information for any purpose other than the intended purpose, misusing, abusing, or excessively monitoring and tracking, etc. personal information, thereby protecting human dignity and personal privacy.

2. The State and a local government shall establish necessary policy measures, including but not limited to the improvement of Acts and subordinate statutes, in order to protect the rights of a subject of information under Article 4.

3. The State and a local government shall respect, facilitate and support personal information protection activities that are voluntarily performed by personal information managers in order to improve irrational social practices in the management of personal information.

4. Where the State and a local government enacts or amends Acts, subordinate statutes or municipal ordinances, it shall do so in compliance with the purpose of this Act.

Article 6 (Relationship with other Acts)

Unless otherwise provided for in other Acts including the Act on Promotion of information and Communications Network Utilization and Information Protection, etc.

Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., and the Use and Protection of Credit Information Act

Use and Protection of Credit Information Act, the protection of personal information shall be governed by this Act.

CHAPTER II ESTABLISHMENT, ETC. OF PERSONAL INFORMATION PROTECTION POLICIES

Article 7 (Personal Information Protection Committee)

1. A Personal Information Protection Committee (hereinafter referred to as "Protection Committee") shall be established under the direct jurisdiction of the President to deliberate and resolve on matters concerning the protection of personal information. The Protection Committee shall independently perform affairs under its authority.

2. The Protection Committee shall be comprised of not more than 15 members including one Chairperson and one standing member, and a public official in political service shall be appointed as the standing member.

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

4. Members shall be either appointed or commissioned by the President from among the following persons. In such cases, five members elected at the National Assembly and five members designated by the Chief Justice of the Supreme Court shall be respectively appointed or commissioned:

(a) A person who is recommended by a civil society organization or consumer organization related to the protection of personal information;

(b) A person who is recommended by an enterprisers' organization comprised of personal information managers;

(c) Other persons who have knowledge and experience in personal information.

(d) The term of office of the Chairperson and the members shall be three years, and the consecutive appointment may be permitted only once.

(e) The Chairperson shall convene a meeting of the Protection Committee if he/she deems such meeting necessary or at least one quarter of all incumbent members request it.

(f) The resolution of a meeting of the Protection Committee shall require the attendance of a majority of all incumbent members and the consent of a majority of those present.

(g) A secretariat shall be established under the Protection Committee to support the business affairs of the Protection Committee.

(h) In addition to the matters provided for in paragraphs (a) through (h), necessary matters concerning the organization and operation of the Protection Committee shall be prescribed by

Presidential Decree.

Article 8 (Functions, etc. of Protection Committee)

1. The Protection Committee shall deliberate and resolve on the following matters:

(a) Basic plans under Article 9 and implementation plans under Article 10;

(b) Matters concerning the improvement of policies, systems, Acts and subordinate statutes concerning the protection of private information;

(c) Matters concerning the coordination of opinions among public institutions in regards to the management of personal information;

(d) Matters concerning the interpretation and application of Acts and subordinate statutes concerning the protection of personal information;

(e) Matters concerning the use and provision of personal information under Article 18.2.(e);

(f) Matters concerning the findings of impact assessment under Article 33.3;

(g) Matters concerning the presentation of opinions under Article 61.1;

(h) Matters concerning the recommendation of measures under Article 64.4;

(i) Matters concerning the publication of handling results under Article 66;

(j) Matters concerning the preparation and submission of annual reports under Article 67.1;

(k) Matters referred to a meeting by the President, the Chairperson or at least two members of the Protection Committee with regard to the protection of personal information;

(l) Other matters to be deliberated and resolved on by the Protection Committee pursuant to this Act, other Acts and subordinate statutes.

2. If necessary to deliberate and resolve on the matters referred to in each subparagraph of paragraph 1, the Protection Committee may hear the opinion of a relevant public official, a person, civil society organization, or relevant business person that has professional knowledge about the protection of personal information and request a relevant agency, etc. to submit data, etc.

Article 9 (Basic Plans)

1. In order to protect personal information and guarantee the rights and interests of a subject of information, the Minister of Public Administration and Security shall prepare a basic plan for protection of personal information every three years through consultation with the heads of relevant central administrative agencies, submit it to the Protection Committee, and implement it upon deliberation and resolution thereon by the Protection Committee.

2. The basic plan shall contain the following matters:

(a) Basic objective and implementation direction-setting in the protection of personal information;

(b) Improving systems, Acts and subordinate statutes related to the protection of personal information;

(c) Measures for preventing the infringement of personal information;

(d) Vitalizing autonomous regulation over the protection of personal information;

(e) Vitalizing education and public relations concerning the protection of personal information;

(f) Fostering experts in the protection of personal information;

(g) Other necessary matters for the protection of personal information.

3. The National Assembly, the court, the Constitutional Court and the National Election Commission (including its affiliated agencies) may establish and implement a basic plan for protection of its personal information.

Article 10 (Implementation Plans)

1. The head of a central administrative agency shall annually prepare an implementation plan for protection of personal information pursuant to the basic plan, submit it to the Protection Committee, and implement it following deliberation and resolution thereon by the Protection Committee.

2. Necessary matters for establishment and implementation of implementation plans shall be prescribed by Presidential Decree.

Article 11 (Requests for Submission of Data, etc.)

1. In order to efficiently establish and promote the basic plans, the Minister of Public Administration and Security may request a personal information manager, the head of a central administrative agency concerned, the head of a local government, related organization, etc. to submit data or state his/her opinion about the current status of compliance with the law by the personal information managers and management status of personal information.

2. The head of a central administrative agency may request personal information managers under his/her jurisdiction to submit data, etc. pursuant to paragraph 1 in order to efficiently establish and promote the implementation plans.

3. A person requested to submit data, etc. under paragraphs 1 and 2 shall comply therewith unless extenuating circumstances exist.

4. Necessary matters, including, but not limited to, the scope and method of submitting data, etc. under paragraphs 1 and 2 shall be prescribed by Presidential Decree.

Article 12 (Personal Information Protection Guidelines)

1. The Minister of Public Administration and Security may establish standard personal information protection guidelines (hereinafter referred to as "standard guidelines") concerning standards for managing personal information, types and preventive measures of infringements on personal information, and other matters, and encourage the personal information managers to comply therewith.

2. The head of a central administrative agency may establish personal information protection guidelines concerning the management of personal information under his/her jurisdiction pursuant to the standard guidelines, and encourage the personal information managers to comply therewith.

3. The National Assembly, the court, the Constitutional Court and the National Election Commission may establish and implement the personal information protection guidelines of relevant agencies (including its affiliated agencies).

Article 13 (Facilitation and Support of Autonomous Regulation)

The Minister of Public Administration and Security shall establish the following necessary policy measures in order to facilitate and support the personal information managers in performing autonomous activities for protection of personal information:

1. Education and public relations concerning the protection of personal information;

2. Fostering and support of agencies and organizations related to the protection of personal

information;

3. Supporting the introduction and implementation of a certification mark regarding the protection of personal information;

4. Supporting the personal information managers in establishing and implementing autonomous rules;

5. Other necessary matters for supporting the personal information managers in their autonomous protection activities of personal information.

Article 14 (International Cooperation)

1. The Government shall establish necessary policy measures for improving the protection level of personal information in an international environment.

2. The Government shall establish relevant policy measures to ensure that the trans-border transfer of personal information does not infringe on the rights of a subject of information.

CHAPTER III MANAGEMENT OF PERSONAL INFORMATION

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

Article 15 (Collection and Use of Personal Information)

1. A personal information manager may collect personal information and use it for the intended purpose of collection in any of the following cases:

(a) Where he/she has obtained the consent of a subject of information;

(b) Where there exist special provisions in any Act or it is inevitable to fulfill an obligation imposed by or under any Act and subordinate statute;

(c) Where it is inevitable for a public institution to perform its affairs provided for in any Act and subordinate statute, etc.;

(d) Where it is inevitably necessary for entering into and performing a contract with a subject of information;

(e) Where it is deemed obviously necessary for physical safety and property interests of a subject of information or a third person when the subject of information or his/her legal

representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.;

(f) Where it is necessary for a personal information manager to realize his/her legitimate interests and this obviously takes precedence over the rights of a subject of information. In such cases, this shall be limited to cases where such information is substantially relevant to a personal information manager's legitimate interests and reasonable scope is not exceeded.

2. When a personal information manager obtains consent referred to in paragraph 1 (a), he/she shall notify a subject of information of the following matters. When the personal information manager changes any of the following matters, he/she shall inform the same and obtain consent thereto:

(a) Purposes for which personal information is collected and used;

(b) Items of personal information to be collected;

(c) Period for which personal information is held and used;

(d) Fact that a subject of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent.

Article 16 (Restrictions on Collection of Personal Information)

1.Where a personal information manager collects personal information in any case referred to in any subparagraph of Article 15.1, he/she shall collect the minimum information necessary for achieving the purpose thereof. In such cases, the personal information manager is responsible for proving that he/she collects the minimum personal information.

2. A personal information manager shall not reject providing a subject of information with goods or services on the ground that the subject of information does not give consent to collect his/her personal information other than the minimum necessary information.

Article 17 (Provision of Personal Information)

1. A personal information manager may provide (including sharing; hereinafter the same shall apply) a third person with the personal information of a subject of information in any of the following cases:

(a) Where he/she has obtained the consent of a subject of information;

(b) Where he/she provides personal information under a purpose for which the personal

information was collected pursuant to Article 15.1 (b), (c) and (e).

2. When a personal information manager obtains consent referred to in paragraph 1 (a), he/she shall notify a subject of information of the following matters. When the personal information manager changes any of the following matters, he/she shall inform the same and obtain consent thereto:

(a) A recipient of personal information;

(b) Purposes for which a recipient of personal information uses such information;

(c) Items of personal information to provide;

(d) Period for which a recipient of personal information holds and uses such information;

(e) The fact that a subject of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent.

3. When a personal information manager provides a third person at any overseas location with personal information, he/she shall notify a subject of information of the matters referred to in each subparagraph of paragraph 2 and obtain the consent thereto, and shall not enter into a contract concerning the trans-border transfer of personal information stipulating any details contravening this Act.

Article 18 (Restrictions on Use and Provision of Personal Information)

1. No personal information manager shall use personal information beyond the scope provided for in Article 15.1, or provide a third person with personal information beyond the scope provided for in Article 17.1 and 3.

2. Notwithstanding paragraph 1, a personal information manager may use personal information for any purpose other than the intended ones or provide a third person with such information in any of the following cases unless the interests of a subject of information or a third person are likely to be unduly infringed on: Provided, That this shall be limited to a public institution in cases under subparagraphs (e) through (i):

(a) Where he/she has obtained the consent of a subject of information;

(b) Where special provisions exist in any other Act;

(c) Where it is deemed obviously necessary for physical safety and property interests of a subject of information or a third person when the subject of information or his/her legal

representative cannot give prior consent as he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.;

(d) Where personal information is necessary for compiling statistics, or scientific research purposes, etc., and the personal information is provided in a form by which a specific individual cannot be identified;

(e) Where using personal information for any purpose other than the intended purpose or a failure to provide a third person with such information makes it impossible to perform affairs provided for in any other Act, and this has undergone deliberation and resolution by the Protection Committee;

(f) Where it is necessary for providing a foreign government or international organization with personal information in order to implement a treaty or any other international agreement;

(g) Where it is necessary for investigating a crime, and instituting and sustaining a public prosecution;

(h) Where it is necessary for a court to perform its judicial affairs;

(i) Where it is necessary for executing a punishment, care and custody or protective disposition.

3. When a personal information manager obtains consent referred to in paragraph 2 (a), he/she shall notify a subject of information of the following matters. When the personal information manager changes any of the following matters, he/she shall inform the same and obtain consent thereto:

(a) A recipient of personal information;

(b) Purposes for which personal information is used (referring to the purposes for which a recipient of personal information uses such information in cases of provision);

(c) Items of personal information to use or provide;

(d) Period for which personal information is held and used (referring to the period for which a recipient of personal information holds and uses it in cases of provision);

(e) The fact that a subject of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent

4. Where a public institution uses personal information for any purpose other than the intended purpose or provides a third person with such information pursuant to paragraph 2 (b) through (f), (h) and (i), it shall publish necessary matters concerning the legal basis, purpose, scope, etc. of such use or provision in its official gazette, Internet website, etc., as prescribed by Ordinance of the Ministry of Public Administration and Security.

5. Where a personal information manager provides a third person with personal information for any purpose other than the intended purpose in any case referred to in each subparagraph of paragraph 2, he/she shall place restrictions on a recipient of the personal information in connection with the purpose and method of use and other necessary measures, or request the person to prepare necessary measures for securing the safety of personal information. In such cases, a person in receipt of such request shall take necessary measures for securing the safety of personal information.

Article 19 (Restrictions on Use and Provision of Personal Information by Recipients of Such Information)

No person who receives personal information from a personal information manager shall use such personal information for any purpose other than the intended purpose of provision or provide a third person with such information, except for any of the following cases:

1. Where he/she has obtained separate consent from a subject of information;

2. Where special provisions exist in any other Act.

Article 20 (Notification on Sources, etc. of Personal Information Collected from Those other than Subject of Information)

1. When a personal information manager manages personal information collected from a person other than a subject of information, he/she shall immediately notify the subject of information of the following matters, if so requested by the subject of information:

(a) Collection source of personal information;

(b) Purpose for which personal information is managed;

(c) the fact that the subject of information has the right to request the suspension of managing the information

2. Paragraph 1 shall not apply to any of the following cases: Provided, That this shall be limited to cases having obvious priority over the rights of a subject of information by or under this Act:

(a) Where the personal information which is a subject matter of notification is included in a personal information file applicable under any subparagraph of Article 32.2;

(b) Where providing notification could harm any third person's life or physical safety, or unreasonably infringe on any third person's property and other interests.

Article 21 (Destruction of Personal Information)

1. When personal information becomes unnecessary as its holding period expires, its management purpose is achieved and by any other ground, a personal information manager shall destroy the personal information without delay: Provided, That this shall not apply where the personal information must be preserved pursuant to any other Act or subordinate statute.

2. When a personal information manager destroys personal information pursuant to paragraph 1, he/she shall take a measure to prevent the personal information from being recovered and recycled.

3. Where a personal information manager does not destroy personal information, pursuant to the proviso to paragraph, and is required to preserve personal information, he/she shall save and administer the personal information or personal information file in question separately from any other personal information.

4. Necessary matters concerning the methods and procedures of destroying personal information and other related matters shall be prescribed by Presidential Decree.

Article 22 (Methods of Obtaining Consent)

1. When a personal information manager obtains the consent of a subject of information (including his/her legal representative under paragraph 5: hereinafter the same shall apply in this Article) about the management of personal information, he/she shall classify respective matters requiring consent and notify the subject of information of such matters to clearly understand them, and obtain consent respectively to such matters.

2. When a personal information manager obtains the consent of a subject of information about the management of personal information pursuant to Articles 15.1 (a), Article 17.1 (a), subparagraph 1 of Article 23 and Article 24.1 (a) he/she shall classify the personal information that can be managed without obtaining the consent of the subject of information and the personal information requiring the consent of the subject of information for the purpose of entering into a contract with the subject of information. In such cases, a personal information manager is responsible for proving that the subject personal information is the one that can be managed without obtaining consent.

3. When a personal information manager intends to obtain the consent of a subject of information on the management of his/her personal information in order to publicize or solicit the sale of goods or services to him/her, the personal information manager shall notify the subject of information thereof to clearly understand this and obtain his/her consent thereto.

4. No personal information manager shall refuse to provide a subject of information with goods or services on the ground that the subject of information fails to give his/her consent to matters he/she is entitled to give selective consent pursuant to paragraph 2 or fails to give his/her consent required under paragraph 3 and Article 18.2 (a).

5. When a personal information manager needs to obtain consent required under this Act in order to manage personal information of a child under the age of 14 years, he/she shall obtain the consent of his/her legal guardian. In such cases, minimum information necessary for obtaining the consent of the legal guardian may be directly collected from the relevant child without consent of the legal guardian.

6. In addition to the matters provided for in paragraphs 1 through 5, detailed methods of obtaining the consent of a subject of information and necessary matters concerning the details of minimum information under paragraph 5 shall be prescribed by Presidential Decree, considering media, etc. of collecting personal information.

SECTION 2 Restrictions on Management of Personal Information

Article 23 (Restrictions on Management of Sensitive Information)

A personal information manager shall not manage any information on thought, beliefs, joining or withdrawal from a labor union or political party, a political opinion, health, sexual life, etc., and other personal information prescribed by Presidential Decree which could substantially infringe on the privacy of a subject of information (hereinafter referred to as "sensitive information"): Provided, That this shall not apply in any of the following cases:

1. Where a subject of information is notified of the matters referred to in each subparagraph of Article 15.2 or 17.2 and his/her separate consent is obtained in addition to his/her consent to the management of general personal information;

2. Where any Act or subordinate statute requires or permits the management of sensitive information.

Article 24 (Restrictions on Management of Unique Identifying Information)

1. A personal information manager shall not manage information prescribed by Presidential

Decree which is identifying information uniquely assigned to each individual to tell him/her from others pursuant to Acts and subordinate statutes (hereinafter referred to as "unique identifying information") except in the following cases:

(a) Where a subject of information is notified of the matters referred to in each subparagraph of Article 15.2 or 17.2 and his/her separate consent is obtained, in addition to his/her consent to the management of other personal information;

(b) Where any Act or subordinate statute clearly requires or permits the management of unique identifying information.

2. A personal information manager meeting the standards prescribed by Presidential Decree shall provide a subject of information with a way to register as a member through an Internet webpage without providing his/her resident registration number.

3. Where a personal information manager manages unique identifying information pursuant to any subparagraph of paragraph 1, he/she shall take measures, such as encryption, etc. which are necessary for securing safety, as prescribed by Presidential Decree, in order to prevent the unique identifying information from loss, theft, leakage, alteration, or corruption.

4. The Minister of Public Administration and Security may prepare various measures, including but not limited to amendments of relevant Acts and subordinate statutes, establishment of plans, and building necessary facilities and systems in order to assist in making the methods referred to in paragraph 2 available.

Article 25 (Restrictions on Installation and Operation of Image Data Processing Equipment)

1. No one shall install and operate image data processing equipment in a public space except in the following cases:

(a) Where the installation and operation of image data processing equipment is concretely permitted by Acts and subordinate statutes;

(b) Where the installation and operation of image data processing equipment is necessary for preventing and investigating a crime;

(c) Where the installation and operation of image data processing equipment is necessary for facility safety and fire prevention;

(d) Where the installation and operation of image data processing equipment is necessary for traffic control

(e) Where the installation and operation of image data processing equipment is necessary for collecting, analyzing and providing traffic information.

2. No one shall install and operate image data processing equipment with which people can see the inside of a space where the privacy of an individual could be substantially infringed on, such as a public bath, restroom, sauna, fitting room, etc. used by many and unspecified persons: Provided, That this shall not apply to facilities prescribed by Presidential Decree, such as a prison, mental health facility, etc. used to detain or protect persons pursuant to applicable Acts and subordinate statutes.

3. The head of a public institution who intends to install and operate the image data processing equipment pursuant to each subparagraph of paragraph 1 and a person who intends to install and operate the image data processing equipment pursuant to the proviso to paragraph 2 shall collect opinions from relevant experts and interested persons by taking procedures prescribed by Presidential Decree, such as holding a hearing or consultation.

4. A person who intends to install and operate image data processing equipment pursuant to each subparagraph of paragraph 1 (hereinafter referred to as "operator of image data processing equipment") shall take necessary measures, including the installation, etc. of a signboard, as prescribed by Presidential Decree, so that a subject of information can readily recognize such equipment: Provided, That this shall not apply to facilities prescribed by Presidential Decree.

5. An operator of image data processing equipment shall not arbitrarily handle the image data processing equipment for purposes other than the intended purpose of installation, shoot other locations, and use a recording function.

6. An operator of image data processing equipment shall take necessary measures for securing safety pursuant to Article 29 in order to prevent personal information from loss, theft, leakage, alteration or corruption.

7. An operator of image data processing equipment shall formulate the operation and management policies of image data processing equipment, as prescribed by Presidential Decree. In such cases, he/she may choose not to formulate personal information management policies under Article 30.

8. An operator of image data processing equipment may entrust business affairs concerning the installation and operation of image data processing equipment: Provided, That where a public institution entrusts business affairs concerning the installation and operation of image data processing equipment, it shall comply with the procedures and requirements prescribed by Presidential Decree.

Article 26 (Restrictions on Management of Personal Information Following Entrustment of Affairs)

1. When a personal information manager entrusts a third person with the management affairs of personal information, he/she shall do so in writing stating the following matters:

(a) Matters concerning prohibiting a third person from managing personal information for any purpose other than for performance of entrusted affairs;

(b) Matters concerning technical and administrative protection measures for personal information;

(c) Other matters prescribed by Presidential Decree for the safe administration of personal information.

2. A personal information manager who entrusts the management affairs of personal information pursuant to paragraph 1 (hereinafter referred to as "truster") shall disclose the details of entrusted affairs and the identity of a person who performs the management affairs of personal information upon entrustment (hereinafter referred to as "trustee"), as prescribed by Presidential Decree, so that a subject of information can readily use them at any time.

3. Where a truster entrusts the affairs of publicizing or soliciting the sale of goods or services, he/she shall inform a subject of information of the details of entrusted affairs and a trustee, as prescribed by Presidential Decree. The same shall also apply when the details of entrusted affairs or a trustee is changed.

4. A truster shall educate a trustee to prevent the personal information of a subject of information from loss, theft, leakage, alteration or corruption, due to the entrustment of affairs, and supervise whether the trustee safely manages the personal information, by inspecting management status, etc., as prescribed by Presidential Decree.

5. No trustee shall use personal information or provide a third person with such information beyond the scope of relevant affairs entrusted by a personal information manager.

6. When liability to pay compensation arises as a trustee violates this Act in the course of managing personal information in connection with the entrusted affairs, the trustee shall be deemed an employee of a personal information manager.

7. Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to a trustee.

Article 27 (Restrictions on Transfer of Personal Information Following Business Transfer, etc.)

1. Where a personal information manager transfers personal information to a third person following the transfer, merger, etc. of all or part of his/her business, he/she shall, in advance, notify the subject of information in question, of the following matters, as prescribed by Presidential Decree:

(a) The fact that personal information is to be transferred;

(b) Name (referring to the name of a corporation, if the third person is a corporation), address, telephone number and other contacts of a recipient of personal information (hereinafter referred to as "business transferee, etc.");

(c) Methods and procedures available when a subject of information does not want his/her personal information to be transferred.

2. When a transferee, etc. has received personal information, he/she shall immediately notify a subject of information of the fact, in accordance with methods prescribed by Presidential Decree: Provided, That this shall not apply where the fact of transfer has been already notified pursuant to paragraph 1.

3. When a transferee, etc. has received personal information following the transfer, merger, etc. of business, he/she may use the personal information or provide a third person with such information for the original purpose as at the transfer. In such cases, the transferee, etc. shall be deemed a personal information manager.

Article 28 (Supervision over Personal Information Handlers)

1. A personal information manager shall appropriately control and supervise persons, such as executives, employees, dispatcher workers, part-time workers, etc. who manage personal information under his/her instructions and supervision (hereinafter referred to as "personal information handler") to ensure the safe administration of personal information in managing such information.

2. A personal information manager shall provide personal information handlers with necessary education on a regular basis to ensure the appropriate handling of personal information.

CHAPTER IV SAFE ADMINISTRATION OF PERSONAL INFORMATION

Article 29 (Duty to Take Safety Measures)

A personal information manager shall establish an internal administration plan, keep access records, and

take technical, administrative and physical measures necessary for securing safety, as prescribed by Presidential Decree, in order to prevent personal information from loss, theft, leakage, alteration or damage.

Article 30 (Establishment and Disclosure of Personal Information Management Policies)

1. A personal information manager shall establish personal information management policies containing the following matters (hereinafter referred to as "personal information management policies"). In such cases, a public institution shall establish such personal information management policies for personal information files to be registered pursuant to Article 32:

(a) Purpose for which personal information is managed;

(b) Period for which personal information is held and used;

(c) Matters concerning providing a third person with personal information (where applicable);

(d) Matters concerning entrusting the management of personal information (where applicable);

(e) Matters concerning the rights and duties of a subject of information, and how to exercise them;

(f) Other matters prescribed by Presidential Decree concerning the management of personal information.

2. Where a personal information manager establishes or amends the personal information management policies, he/she shall disclose them in accordance with methods prescribed by Presidential Decree so that a subject of information can readily use them.

3. Where the details of the personal information management policies are inconsistent with those of a contract entered into between a personal information manager and a subject of information, whichever is more advantageous to the subject of information shall govern.

4. The Minister of Public Administration and Security may draw up a guideline for preparing the personal information management policies and recommend a personal information manager to comply therewith.

Article 31 (Designation of Personal Information Protection Managers)

1. A personal information manager shall designate a personal information protection manager to take overall responsibility for the management of personal information.

2. A personal information protection manager shall carry out the following duties:

(a) Establishing and implement a personal information protection plan;

(b) Periodically investigating and improving personal information management status and practices;

(c) Handling complaints concerning the management of personal information and remedying damage therefrom;

(d) Establishing an internal control system to prevent the leakage and misuse of personal information;

(e) Establishing and implementing an education plan for the protection of personal information;

(f) Protecting, administering and supervising personal information files;

(g) Other duties prescribed by Presidential Decree for the appropriate management of personal information.

3. A personal information protection manager may frequently investigate the management status, system, etc. of personal information or require a related party to report thereon if necessary while performing the duties referred to in each subparagraph of paragraph 2.

4. Where a personal information protection manager becomes aware of a violation of this Act, other relevant Acts and subordinate statutes in connection with the protection of personal information, he/she shall take a corrective measure immediately, and report the corrective measure to the agency or organization to which he/she belongs, where necessary.

5. A personal information manager shall ensure that a personal information protection manager does not cause, or suffer from, any disadvantage without reasonable grounds in performing the duties referred to in each subparagraph of paragraph 2.

6. Designation requirements, duties and qualifications of personal information protection managers, and other necessary matters shall be prescribed by Presidential Decree.

Article 32 (Registration and Disclosure of Personal Information Files)

1. Where the head of a public institution administers personal information files, he/she shall register the following matters with the Minister of Public Administration and Security. The same

shall also apply to any changes to the registered matters:

(a) Name of personal information file;

(b) Basis and purpose of administering a personal information file;

(c) Items of personal information to be recorded in a personal information file;

(d) Method of managing personal information;

(e) Period for which personal information is held;

(f) Recipients if personal information is provided on a regular basis or repeatedly;

(g) Other matters prescribed by Presidential Decree.

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

(a) Personal information files recording national safety, diplomatic confidential information, and other matters concerning the State's critical interests;

(b) Personal information files recording matters concerning criminal investigations, instituting and sustaining a public prosecution, execution of a punishment and protective custody, reformation disposition, protective disposition, security and observation disposition and immigration control;

(c) Personal information files recording matters concerning investigations into offences provided for in the Punishment of Tax Evaders Act, Punishment of Tax Evaders Act and the Customs Act, Customs Act;

(d) Personal information files used by public institutions for dealing with their internal affairs only;

(e) Classified personal information files pursuant to other Acts and subordinate statutes.

3. The Minister of Public Administration and Security may review the registered matters and details of personal information files referred to in paragraph 1, if necessary, and recommend the head of a relevant public institution to make the improvement thereof.

4. The Minister of Public Administration and Security shall disclose the registration status of personal information files under paragraph 1 in order for anyone to readily inspect them.

5. Necessary matters concerning registration under paragraph 1 and the method, scope and procedure for disclosure under paragraph 4 shall be prescribed by Presidential Decree.

6. The registration and disclosure of personal information files by the National Assembly, the courts, the Constitutional Court and the National Election Commission (including its affiliated agencies) shall be stipulated by the National Assembly Regulations, the Supreme Court Regulations, the Constitutional Court Regulations, and the National Election Commission Regulations.

Article 33 (Personal Information Impact Assessment)

1. Where the administration of personal information files meeting the standards prescribed by Presidential Decree is likely to infringe on the personal information of a subject of information, the head of a public institution shall conduct an assessment (hereinafter referred to as "impact assessment") to analyze risk factors and discover improvements, and submit the results thereof to the Minister of Public Administration and Security. In such cases, the head of a public institution shall request any agency designated by the Minister of Public Administration and Security (hereinafter referred to as "assessment agency") to conduct an impact assessment.

2. The following matters shall be considered in conducting impact assessment:

(a) Number of personal information to be managed;

(b) Whether personal information is provided to a third person;

(c) Risk of infringing on the rights of a subject of information and the degree of risk;

(d) Other matters prescribed by Presidential Decree.

3. The Minister of Public Administration and Security may present his/her opinion on the results of impact assessment submitted under paragraph 1, following deliberation and resolution thereon by the Protection Committee.

4. When the head of a public institution registers personal information files which underwent the impact assessment under paragraph 1, pursuant to Article 32.1, he/she shall attach the results of impact assessment thereto.

5. To invigorate an impact assessment, the Minister of Public Administration and Security shall train relevant experts, develop and disseminate impact assessment standards, and take necessary measures.

6. Necessary matters concerning the designation standards of assessment agencies under

paragraph 1, the revocation of designation, criteria for assessment, the method, procedure, etc. of impact assessment shall be prescribed by Presidential Decree.

7. The impact assessment of the National Assembly, the courts, the Constitutional Court and the National Election Commission (including its affiliated agencies) shall be conducted as stipulated by the National Assembly Regulations, the Supreme Court Regulations, the Constitutional Court Regulations, the National Election Commission Regulations.

8. A personal information manager, other than a public institution shall actively endeavor to conduct an impact assessment if he/she has concern over the infringement of the personal information of a subject of information due to the administration of personal information.

Article 34 (Notification, etc. on Leakage of Personal Information)

1. When a personal information manager becomes aware that personal information has leaked out, he/she shall notify the relevant subject of information of the following matters without delay:

(a) Items of leaked personal information;

(b) When and how personal information has leaked;

(c) Information on means, etc. available to a subject of information to minimize damage that could inflicted on by leakage;

(d) A person information manager's actions and damage remedy procedures;

(e) A department in charge of receiving reporting, etc. and contact if damage is inflicted on a subject of information.

2. Where personal information has leaked, a personal information manager shall prepare measures to minimize the damage therefrom, and take necessary measures.

3. Where personal information has leaked in excess of the scale prescribed by Presidential Decree, a personal information manager shall immediately report the notification under paragraph 1 and the result of measures taken under paragraph 2 to the Minister of Public Administration and Security or specialized institutions prescribed by Presidential Decree. In such cases, the Minister of Public Administration and Security or the specialized institution prescribed by Presidential Decree may provide technical support for preventing the spread of damage and recovering from damage.

4. Necessary matters concerning the timing, method, procedure, etc. of notification under

paragraph 1 shall be prescribed by Presidential Decree.

CHAPTER V GUARANTEEING RIGHTS OF SUBJECTS OF INFORMATION

Article 35 (Inspection of Personal Information)

1. A subject of information may request a personal information manager to allow him/her to inspect his/her personal information managed by such a personal information manager.

2. Notwithstanding paragraph 1, when a subject of information intends to request a public institution to allow the inspection, he/she may directly request such a public institution or via the Minister of Public Administration and Security, as prescribed by Presidential Decree.

3. When a personal information manager has received an inspection request pursuant to paragraphs 1 and 2, he/she shall ensure that a subject of information can inspect the relevant personal information within a period prescribed by Presidential Decree. In such cases, if there exist justifiable grounds making it impractical to inspect such information within the specified period, the personal information manager may notify the subject of information of the grounds therefor and postpone an inspection, and permit the inspection without delay once the grounds cease to exist.

4. In any of the following cases, a personal information manager may notify a subject of information of the grounds therefor and restrict or reject an inspection:

(a) Where an inspection is prohibited or restricted by Acts;

(b) Where it is apprehended that any third person's life and body may be harmed, or any third person's property and other interests may be unduly infringed on;

(c) Where a public institution causes any inconvenience while carrying out any of the following affairs:

(i) Affairs concerning the imposition, collection or refund of taxes;

(ii) Affairs concerning grade evaluation or the selection of newly enrolled students at schools of each level under the Elementary and Secondary Education Act, Elementary and Secondary Education Act and the Higher Education Act, Higher Education Act, lifelong education centers under the Lifelong Education Act, Lifelong Education Act, and other higher education institutions established under other Acts;

(iii) Affairs concerning tests of academic ability, functions and employment, and

qualification evaluation;

(iv) Affairs concerning an assessment or decision in progress in connection with the calculation, etc. of compensation or benefits;

(v) Affairs concerning an audit and an investigation in progress under other Acts.

5. Necessary matters concerning the method of and procedure for requesting and restricting inspections or providing notices, etc. pursuant to paragraphs 1 through 4 shall be prescribed by Presidential Decree.

Article 36 (Correction or Deletion of Personal Information)

1. A subject of information who has inspected his/her personal information pursuant to Article 35 may request a personal information manager to correct or delete his/her personal information: Provided, That if other Acts and subordinate statutes stipulates the particular personal information be collected, the subject of information shall not request the deletion thereof.

2. Upon receiving a request from a subject of information pursuant to paragraph 1, a personal information manager shall investigate the personal information in question without delay, take necessary measures, such as correction, deletion, etc. based on a request from the subject of information, and notify the subject of information of the result unless other Acts and subordinate statutes stipulate special procedures for the correction or deletion of the personal information.

3. When a personal information manager deletes personal information pursuant to paragraph 2, he/she shall take measures to prevent the personal information from being recovered or recycled.

4. Where a request from a subject of information falls under the proviso to paragraph 1, a personal information manager shall notify a subject of information of the details thereof without delay.

5. If it is necessary for conducting an investigation under paragraph 2, a personal information manager may require a subject of information in question to submit evidence necessary for verifying a request for correction or deletion.

6. Necessary matters concerning the method, procedure, etc. of requesting correction or deletion, and providing notification shall be prescribed by Presidential Decree.

Article 37 (Suspension, etc. from Managing Personal Information)

1. A subject of information may request a personal information manager to suspend managing his/her personal information. When the manager is a public institution, the subject of

information may request the suspension on his/her personal information among the personal information files to be registered pursuant to Article 32.

2. A personal information manager in receipt of a request under paragraph 1 shall immediately suspend the management of the personal information completely or partially at the request of a subject of information: Provided, That the personal information manager may reject a request from a subject of information to suspend management in any of the following cases:

(a) Where there exists special provisions in any Act or it is inevitable to comply with statutory obligations;

(b) Where it is apprehended that any third person's life and body may be harmed, or any third person's property and other interests may be unduly infringed on;

(c) Where a public institution is unable to carry out its affairs stipulated by or under other Acts unless it manages personal information;

(d) Where it is impractical to perform a contract, such as a failure to provide a subject of information with stipulated services unless the personal information manager manages personal information, and the subject of information fails to clearly express his/her intention to terminate the contract.

3. When a personal information manager has refused a request to suspend management pursuant to the proviso to paragraph 2, he/she shall immediately notify a subject of information of the reason therefor.

4. A personal information manager shall immediately take necessary measures, such as the destruction, etc. of the relevant personal information, the management of which is suspended at the request of a subject of information.

5. Necessary measures concerning the method and procedure of requesting or refusing the suspension of management, and providing notification pursuant to paragraphs 1 through 3 shall be prescribed by Presidential Decree.

Article 38 (Methods and Procedures of Exercising Rights)

1. A subject of information may have his/her representative to make a request for inspection under Article 35, correction or deletion under Article 36, and the suspension, etc. of management under Article 37 (hereinafter referred to as "request for inspection, etc.") according to the method and procedure prescribed by Presidential Decree, such as in writing.

2. A legal guardian of a child under the age of 14 years may make a request to a personal

information manager for inspection, etc. of the child's personal information.

3. A personal information manager may charge fees and postage (limited to cases where a request is made to send a certified copy by mail) to a person who makes a request for inspection, etc., as prescribed by Presidential Decree.

4. A personal information manager shall prepare detailed methods and procedures available for the subjects of information to make a request for inspection, etc., and disclose them to the subjects of information.

5. A personal information manager shall prepare necessary procedures and provide a notice thereon to the subjects of information so that they can raise an objection if dissatisfied with measures, such as refusal, etc. of a request for inspection, etc.

Article 39 (Liability to Compensate for Damage)

1. If a subject of information suffers loss as a personal information manager has performed any act violating this Act, he/she may claim for loss to the personal information manager. In such cases, the personal information manager cannot be exempted from responsibility unless he/she proves that he/she has performed such act neither intentionally nor by negligence.

2. Where a personal information manager has fulfilled his/her obligations by or under this Act and has not been negligent in giving due attention and supervision, his/her responsibility to compensate for damage due to the loss, theft, leakage, alteration or corruption of the personal information can be mitigated.

CHAPTER VI PERSONAL INFORMATION DISPUTE MEDIATION COMMITTEE

Article 40 (Establishment and Composition)

1. A committee for mediation of disputes on personal information (hereinafter referred to as the "Dispute Mediation Committee") shall be established to mediate disputes over personal information.

2. The Dispute Mediation Committee shall be comprised of not more than 20 members, including one chairperson, and one of its members shall be a standing member.

3. Members shall be appointed or commissioned by the Minister of Public Administration and Security among the following persons:

(a) A public official belonging to the Senior Civil Service of a central administrative agency

taking charge of the protection affairs of personal information, or a person who has ever served or currently serves with any equivalent position in any public sector or related organization and who has experience in protection affairs of personal information;

(b) A person who has ever served or currently serves as an associate professor or with a higher or equivalent position in a university or an officially recognized research institute;

(c) A person who has served or currently serves as a judge, public prosecutor, or attorney-at-law;

(d) A person recommended by a civic and social organization or consumer organization related to the protection of personal information;

(e) A person who has served or currently serves as an executive in an enterprisers' organization comprised of personal information managers

4. The chairperson shall be appointed by the Minister of Public Administration and Security among non-public official members.

5. The term of office of each member shall be three years and he/she may be consecutively re-appointed only once.

6. Where it is deemed necessary to efficiently meditate disputes, the Dispute Mediation Committee may establish a mediation division comprised of not more than five members in each sector of mediation cases, as prescribed by Presidential Decree. In such cases, a resolution adopted by any mediation division upon entrustment of the Dispute Mediation Committee shall be deemed a resolution adopted by the Dispute Mediation Committee.

7. The resolution passed at a meeting of the Dispute Mediation Committee or a mediation division shall require the attendance of a majority of all incumbent members and the consent of a majority of those present.

8. The Minister of Public Administration and Security may designate a specialized institution, as prescribed by Presidential Decree, to assist the Dispute Mediation Committee in performing its affairs, such as the operation, etc. of a secretariat,

9. In addition to the matters provided for in this Act, necessary matters for the operation of the Dispute Mediation Committee shall be prescribed by Presidential Decree.

Article 41 (Status Guarantee of Members)

No member may be dismissed or de-commissioned against his/her will unless he/she is sentenced to the suspension of any qualifications, or heavier punishment, or unless he/she becomes unable to perform his/her duties due to a mental or physical disability.

Article 42 (Abstention, Recusal and Withdrawal of Members)

1. A member of the Dispute Mediation Committee shall abstain from deliberation and decision-making on a case filed for mediation of a dispute (hereinafter referred to as "case" in this Article) pursuant to Article 43.1 in any of the following cases:

(a) If the member or his/her spouse or ex-spouse is a party to the case or is related to the case as a joint right holder or a joint obligor;

(b) If the member is or was a relative of a party to the case;

(c) If the member has testified or given an expert opinion or legal advice with respect to the case;

(d) If the member is or was involved in the case as an agent of a party to the case.

2. If a party to a case finds it difficult to expect a fair deliberation or resolution from a Committee member, he/she may file a recusal with the chairperson against the Committee member. In such cases, the chairperson shall decide upon the recusal without any resolution of the Dispute Mediation Committee.

3. If a Committee member falls under any of the cases under paragraph 1 or 2, he/she may voluntarily withdraw from deliberation and resolution on a case.

Article 43 (Application, etc. for Mediation)

1. Any person who wants a dispute over personal information to be mediated, may file an application with the Dispute Mediation Committee to conduct a mediation.

2. Upon receiving an application for mediation of a dispute from a party to a case, the Dispute Mediation Committee shall inform the other party of the details of such application.

3. When a public institution is informed of mediation of a dispute under paragraph 2, it shall respond to mediation of the dispute unless extenuating circumstances exist.

Article 44 (Handling Period)

1. The Dispute Mediation Committee shall examine a case and prepare a proposed mediation

within 60 days from the date it has received an application for mediation of a dispute under Article 43.1: Provided, That the handling period may be extended by the resolution of the Dispute Mediation Committee, if any unavoidable cause exists.

2. When the Dispute Mediation Committee extends the handling period pursuant to the proviso to paragraph 2, it shall inform the applicant of the reasons for the extension of the period and other matters concerning the extension of the period.

Article 45 (Requests, etc. for Data)

1. The Dispute Mediation Committee may request parties to a dispute to furnish it with data necessary for mediating the dispute. In such cases, the parties to the dispute shall comply with the request, unless any justifiable ground exists otherwise.

2. The Dispute Mediation Committee may, if deemed necessary, require parties to a dispute and witnesses to make an appearance at the Dispute Mediation Committee to hear their opinions.

Article 46 (Recommendation on Agreement Prior to Mediation)

When the Dispute Mediation Committee receives an application for mediation of a dispute pursuant to Article 43.1, it may present the details thereof to the parties to a case and recommend them to reach agreement prior to mediation.

Article 47 (Mediation of Disputes)

1. The Dispute Mediation Committee may prepare a proposed mediation including any of the following matters:

(a) Suspension of an infringement subject to investigation;

(b) Reinstatement, compensation for loss, and other necessary remedies;

(c) Necessary measures to prevent the recurrence of the same or a similar infringement

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

3. When each party to a dispute in receipt of a proposed mediation under paragraph 1 fails to inform the Dispute Mediation Committee of whether he/she accepts the proposed mediation within 15 days from the date on which he/she received such proposed mediation, he/she is deemed to reject mediation.

4. If the parties to a dispute accept a proposed mediation, the Dispute Mediation Committee shall prepare a letter of mediation, and the chairperson of the Dispute Mediation Committee and parties to the dispute shall print their names and affix their seals on the letter of mediation.

5. Details of mediation under paragraph (4) are as effective as judicial compromise.

Article 48 (Rejection and Suspension of Mediation)

1. If the Dispute Mediation Committee deems that it is inappropriate to settle a dispute by mediation of the Dispute Mediation Committee in light of the nature of the dispute or an application for mediation has been filed for any unjust purpose, it may reject the application for mediation. In such cases, it shall notify the applicant of the grounds for rejection of the application for mediation and other related matters.

2. If a party to a dispute files a lawsuit while proceedings of a case filed for mediation are in progress, the Dispute Mediation Committee shall suspend the mediation proceedings and notify the parties thereof.

Article 49 (Mediation of Collective Dispute)

1. In connection with cases prescribed by Presidential Decree in which many subjects of information suffer the same or similar types of loss or infringement of their rights, the State, a local government, a personal information protection organization or institution, a subject of information or a personal information manager may request or apply for mediation of a dispute collectively (hereinafter referred to as "mediation of a collective dispute") to the Dispute Mediation Committee.

2. The Dispute Mediation Committee in receipt of a request or application for mediation of a collective dispute under paragraph 1 may start, by resolution, proceedings for mediation of the collective dispute pursuant to paragraphs 3 through 7. In such cases, the Dispute Mediation Committee shall announce that it started such proceedings for a period prescribed by Presidential Decree.

3. The Dispute Mediation Committee may receive from a subject of information or a personal information manager other than a party to mediation of a collective dispute an application requesting to be an additional party to the mediation of the said dispute.

4. The Dispute Mediation Committee may pass a resolution to appoint one person or several persons who are most appropriate for representing common interests as a representative party among parties to the mediation of a collective dispute under paragraphs 1 and 3.

5. When a personal information manager accepts the mediation of a collective dispute done by

the Dispute Mediation Committee, the Dispute Mediation Committee may recommend that the personal information manager prepare a compensation plan for a subject of information who is not a party to the mediation of the collective dispute and suffers loss and submit it to the Committee.

6. Notwithstanding Article 48.2, if some subjects of information among many subjects of information who are parties to the mediation of a collective dispute institute a suit in a court, the Dispute Mediation Committee shall exclude some subjects of information who institute the suit from proceedings without suspending the proceedings.

7. No period for the mediation of a collective dispute shall exceed 60 days from the date following that on which an announcement under paragraph 2 ends: Provided, That the period can be extended by the resolution of the Dispute Mediation Committee if any unavoidable reason exists.

8. Necessary matters concerning the proceedings for mediation of a collective dispute and other related matters shall be prescribed by Presidential Decree.

Article 50 (Mediation Procedure, etc.)

1. Except as provided for in Articles 43 through 49, necessary matters concerning the method and procedure for mediation of disputes, the handling of mediation affairs, and other related matters shall be prescribed by Presidential Decree.

2. The Judicial Conciliation of Civil Disputes Act, Judicial Conciliation of Civil Disputes Act shall apply mutatis mutandis to matters concerning the operation of the Dispute Mediation Committee and the procedure for meditation of disputes which are not provided for in this Act.

CHAPTER VII CLASS ACTIONS ON PERSONAL INFORMATION

Article 51 (Those, etc. Eligible for Class Actions)

Any of the following organizations may institute an action requesting for the prohibition or suspension of an infringement on rights (hereinafter referred to as "class action") in a court if a personal information manager rejects the mediation of a collective dispute under Article 49 or does not accept the mediation results of the collective dispute:

1. Consumer organizations registered with the Fair Trade Commission pursuant to Framework Act on Consumers Article 29 of the Framework Act on Consumers that meet all of the following requirements:

(a) Their ordinary and primary objective shall be to promote the rights and interests of subjects of information pursuant to articles of association;

(b) The number of their regular members shall be at least one thousand;

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

2. Non-profit, non-governmental organizations referred to in Assistance for Non-Profit, Non-Governmental Organizations Act Article 2 of the Assistance for Non-Profit, Non-Governmental Organizations Act that meet all of the following requirements:

(a) They shall be requested to institute a class action from at least 100 subjects of information which suffer a legal or factual same infringement;

(b) They shall have been working for the protection of personal information for the preceding three years or more after stipulating the protection of personal information as their objective in the articles of association;

(c) The number of their regular members shall be at least five thousand;

(d) They shall have to be registered with any central administrative agency.

Article 52 (Exclusive Jurisdiction)

1. A class action shall be exclusively governed by the collegiate division of the district court having jurisdiction over the location in which a defendant's principal office or place of business is located, or the domicile of the person principally in charge of the defendant's business exists if such office or place of business does not exist.

2. When applying paragraph 1 to a foreign enterpriser, the exclusive jurisdiction shall be determined based on the address of the principal office of place of business in the Republic of Korea or the address of the person principally in charge of his/her business.

Article 53 (Appointment of Litigation Representative)

The plaintiff of a class action shall appoint an attorney as a litigation representative.

Article 54 (Application for Permission to File Action)

1. An organization instituting a class action shall file with the court a petition and an application for approval for such an action which states the following matters:

(a) A plaintiff and his/her litigation representative;

(b) A dependent;

(c) Details of the infringed right.

2. An application for action permission under paragraph (1) shall be accompanied by the following data:

(a) Explanatory materials proving that an organization instituting an action meets any requirement referred in each subparagraph of Article 51;

(b) Materials evidencing that a personal information manager rejects mediation or does not accept the result of mediation.

Article 55 (Requirements, etc. for Permission of Actions)

1. The court shall rule to permit a class action only if all of the following requirements are met:

(a) A personal information manager rejects mediation by the Dispute Mediation Committee or does not accept the result of mediation;

(b) Information recorded in an application for permission of actions under Article 54 is incomplete.

2. An immediate appeal can be filed in connection with a decision to permit or not to permit a class action.

Article 56 (Validity of Final and Conclusive Rulings)

When a ruling dismissing a plaintiff's request becomes final and conclusive, other organizations under Article 51 may not institute a class action against the same case: Provided, That this shall not apply to any of the following cases:

1. When the State, a local government or an institution established by the State or a local government discovers new evidence of the case after the ruling becomes final and conclusive;

2. It is verified that an dismissal ruling is due to plaintiff's intention.

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

1. Unless otherwise specifically provided for in this Act, the Civil Procedure Act
Civil Procedure Act shall apply to class actions.

2. When a decision to permit a class action is made under Article 55, preservative measures under PART IV of the Civil Execution Act, Civil Execution Act can be taken.

3. Necessary matters concerning class action procedures shall be determined by the Supreme Court Regulations.

CHAPTER VIII SUPPLEMENTARY PROVISIONS

Article 58 (Partial Exclusion from Application)

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

(a) Personal information collected pursuant to the Statistics Act, Statistics Act, among personal information managed by public institutions;

(b) Personal information collected or requested to provide for the purpose of analyzing information related to national security;

(c) Personal information managed temporarily as it is urgently necessary for ensuring the public safety and security, including public health, etc.;

(d) Personal information collected or used by the press, a religious organization or a political party to achieve its intended purpose, such as collecting or reporting news, missionary work, recommendation of electoral candidates, etc.

2. Articles 15, 22, 27.1 and 2, 34 and 37 shall not apply to the personal information managed by installing and operating the image data processing equipment at a public space pursuant to each subparagraph of Article 25.1.

3. Articles 15, 30 and 31 shall not apply where a personal information manager manages personal information to operate a group for promoting friendship, such as an alumni association, club, etc.

4. Although a personal information manager manages personal information pursuant to each subparagraph of paragraph 1, he/she shall manage personal information to the minimum extent necessary for achieving the purposes for a minimum period. The personal information manager shall prepare technical, administrative and physical protection measures necessary for safely administering personal information, and necessary measures for handling complaints concerning the management of personal information and appropriately managing personal information.

Article 59 (Prohibited Acts)

No person who has ever managed or manages personal information shall perform any of the following acts:

1. Acquiring personal information or obtaining consent to the management thereof by false or other unlawful means;

2. Revealing personal information that comes to his/her knowledge in the course of business or providing any third person with such information for his/her use without due authority;

3. Corrupting, destroying, altering, fabricating or leaking any third person's personal information without due authority or beyond granted authority.

Article 60 (Keeping Confidentiality, etc.)

No one who was or is engaged in the following affairs shall reveal any confidential information which comes to his/her knowledge in the course of performing his/her duties to any third person or use such information for any purpose other than for his/her duties: Provided, That this shall not apply if otherwise provided for in other Acts:

1. Affairs of the Protection Committee under Article 8;

2. Impact assessment affairs under Article 33;

3. Dispute mediation affairs of the Dispute Mediation Committee under Article 40.

Article 61 (Presentation of Opinions and Recommendation of Improvements)

1. If it is deemed necessary with regard to Acts and subordinate statutes or municipal ordinances that contain details affecting the protection of personal information, the Minister of Public Administration and Security may present his/her opinion to any relevant agency following deliberation and resolution thereon by the Protection Committee.

2. If it is deemed necessary for protecting personal information, the Minister of Public Administration and Security may recommend a personal information manager to improve the management of personal information. In such cases, the personal information manager in receipt of a recommendation shall sincerely endeavor to carry out the recommendation, and inform the Minister of Public Administration and Security of the result of measures taken.

3. If it is deemed necessary for protecting personal information, the head of a central administrative agency concerned may recommend a personal information manager to improve

the managing status of personal information in accordance with governing Acts. In such cases, the personal information manager in receipt of a recommendation shall sincerely endeavor to carry out the recommendation, and inform the head of the central administrative agency concerned of the result of measures taken.

4. A central administrative agency, a local government, the National Assembly, a court, the Constitutional Court, and the National Election Commission may present its opinion on the protection of personal information to, or instruct or inspect agencies and public institutions under its control or jurisdiction.

Article 62 (Reporting, etc. Facts of Infringements)

1. A person whose rights and interests in personal information are infringed on when a personal information manager manages his/her personal information may report the infringement to the Minister of Public Administration and Security.

2. The Minister of Public Administration and Security may designate a specialized institution, as prescribed by Presidential Decree, in order to efficiently carry out the affairs concerning receipt, handling, etc. of reporting under paragraph 1. In such cases, the specialized institution shall establish and operate a reporting center for infringements on personal information (hereinafter referred to as "Reporting Center"):

3. The Reporting Center shall carry out the following affairs:

(a) Receipt of and consultation on reporting concerning the management of personal information;

(b) Investigation and verification of facts, and hear related persons' opinions;

(c) Affairs incidental to those under subparagraphs (a) and (b).

4. The Minister of Public Administration and Security may second a public official under his/her control to the specialized institution under paragraph 2 pursuant to State Public Officials Act, Article 32-4 of the State Public Officials Act, if necessary for efficiently carrying out affairs such as investigation, verification, etc. of facts referred to in paragraph 3 (b).

Article 63 (Requests for Submission of Data and Inspection)

1. The Minister of Public Administration and Security may require a personal information manager to submit data, such as relevant articles, documents, etc. in any of the following cases:

(a) Where he/she discovers a violation of this Act or suspects a violation of this Act;

(b) Where he/she receives reporting or a civil petition concerning a violation of this Act;

(c) Other cases prescribed by Presidential Decree which are necessary for protecting the personal information of a subject of information.

2. Where a personal information manager fails to submit data pursuant to paragraph 1 or is deemed to have violated this Act, the Minister of Public Administration and Security may require a public official under his/her jurisdiction to inspect business status, books, documents, etc. by entering the personal information manager's office or place of business. In such cases, the public official who conducts an inspection shall carry a certificate indicating his/her authority and produce it to related persons.

3. The head of a central administrative agency concerned may require a personal information manager to submit data under paragraph 1 or conduct an inspection under paragraph 2 pursuant to governing Acts.

4. The Minister of Public Administration and Security and the head of a central administrative agency concerned shall not provide any third person with documents, data, etc. received or collected from a personal information manager or disclose the same to the general public unless otherwise provided for in this Act.

5. Where the Minister of Public Administration and Security and the head of a central administrative agency concerned receives data via an information and communications network or computerizes the collected data, etc., he/she shall take institutional and technical supplementary measures in order to prevent personal information, confidential business information, etc. from being leaked.

Article 64 (Corrective Measures, etc.)

1. Were the Minister of Public Administration and Security believes that there exist reasonable grounds to determine that personal information has been infringed on and negligence over such infringement could inflict damage that is difficult to recover, he/she may order any of the following measures to a violator of this Act (excluding a central administrative agency, a local government, the National Assembly, the courts, the Constitutional Court, the National Election Commission):

(a) Suspension of infringement on personal information;

(b) Temporary suspension of managing personal information;

(c) Other necessary measures for protecting personal information and preventing

infringement on personal information.

2. Where the head of a central administrative agency concerned believes that there exist reasonable grounds to determine that personal information has been infringed on and negligence over such infringement could inflict damage that is difficult to rectify, he/she may order a personal information manager to take any of the measures referred to in the subparagraphs of paragraph 1 pursuant to the governing Acts.

3. A local government, the National Assembly, a court, the Constitutional Court, or the National Election Commission may order agencies and public institutions under its control or jurisdiction to take any of the measures referred to in the subparagraphs of paragraph 1 if they violate this Act.

4. When a central administrative agency, a local government, the National Assembly, a court, the Constitutional Court and the National Election Commission violates this Act, the Protection Committee may recommend that the head of each relevant agency take measures referred to in each subparagraph of paragraph 1. In such cases, an agency in receipt of a recommendation shall obey it unless extenuating circumstances exist.

Article 65 (Accusation and Recommendation of Disciplinary Measures)

1. If the Minister of Public Administration and Security finds reasonable grounds to suspect that a personal information manager has violated any Act or subordinate statute related to the protection of personal information, including this Act, he/she may file an accusation with the competent investigation agency.

2. If the Minister of Public Administration and Security finds reasonable grounds to believe that a person has violated any Act or subordinate statute related to the protection of personal information, including this Act, he/she may advise the head of an agency, organization, etc. to which the responsible person belongs to take disciplinary action. In such cases, a person in receipt of such advice shall respect it and update the Minister of Public Administration and Security on the outcome.

3. The head of a central administrative agency concerned may file an accusation against a personal information manager pursuant to paragraph 1 or advise the head of an agency, organization, etc. to which a responsible person belongs to take disciplinary action pursuant to paragraph 2, as provided for by governing Acts. In such cases, a person in receipt of advice pursuant to paragraph 2 shall respect it and update the Minister of Public Administration and Security on the outcome.

Article 66 (Publication of Outcome)

1. The Minister of Public Administration and Security may publish the details and the outcome of recommendations for improvement under Article 61, orders for corrective measures under Article 64, accusation and advice for disciplinary action under Article 65, and imposition of fines for negligence under Article 75, following deliberation and resolution thereon by the Protection Committee.

2. The head of a central administrative agency concerned may publish matters referred to in paragraph 1 pursuant to governing Acts.

3. Methods, standards and procedures of publication under paragraphs 1 and 2 and other related matters shall be prescribed by Presidential Decree.

Article 67 (Annual Reports)

1. The Protection Committee shall annually prepare a report on the establishment and implementation of the personal information protection policies after receiving necessary data from related agencies, etc., and shall submit (including submission via an information and communications network) it to the National Assembly before the regular session opens.

2. A report under paragraph 1 shall contain the following matters:

(a) Infringements on the rights of a subject of information and remedy status;

(b) Findings from investigating the actual state of the management of personal information;

(c) Current status and records of implementing personal information protection policies;

(d) Foreign legislation and policy trends on personal information;

(e) Other matters to be disclosed or reported about the personal information protection policies.

Article 68 (Delegation and Entrustment of Authority)

1. The Minister of Public Administration and Security or the head of a central administrative agency concerned may delegate or entrust part of his/her authority under this Act to the Special Metropolitan City Mayor, a Metropolitan City Mayor, Do Governor, the Governor of a Special Self-Governing Province or a specialized institution determined by Presidential Decree, as prescribed by Presidential Decree.

2. Agencies delegated or entrusted with the authority of the Minister of Public Administration and Security or the head of a central administrative agency concerned pursuant to paragraph 1

shall notify the Minister of Public Administration and Security or the head of central administrative agency concerned of the results of handling the delegated or entrusted affairs.

3. Where the Minister of Public Administration and Security delegates or entrusts part of his/her authority pursuant to paragraph 1, he/she may contribute expenses incurred in performing the affairs to the relevant specialized institution.

Article 69 (Legal Fiction as Public Official in Application of Penal Provisions)

An executive or employee of a relevant agency engaged in affairs to which the authority of the Minister of Public Administration and Security or the head of a central administrative agency concerned is entrusted shall be deemed a public official in the application of provisions under Criminal Act, Articles 129 through 132 of the Criminal Act.

CHAPTER IX PENAL PROVISIONS

Article 70 (Penal Provisions)

A person who seriously hinders, interrupts or paralyzes a public institution in performing its business by altering or erasing personal information managed by the public institution with the intention of interfering with the management affairs of personal information shall be punished by imprisonment for not more than ten years, or by a fine not exceeding 100 million won

Article 71 (Penal Provisions)

A person who falls under any of the following cases shall be punished by imprisonment for not more than five years or by a fine not exceeding 50 million won:

1. Any person who provides a third person with personal information without obtaining the consent of a subject of information in violation of Article 17.1 (a) although he/she is not applicable under subparagraph (b) of the same paragraph, and a person who knowingly receives such personal information;

2. A person who uses personal information or provides a third person with personal information, in violation of Articles 18.1 and 2, 19, 26.5 or 27.3, and a person who knowingly receives personal information for profit or an unjust purpose;

3. A person who manages sensitive information, in violation of Article 23;

4. A person who manages unique identifying information, in violation of Article 24.1;

5. A person who reveals personal information that comes to his/her knowledge in the course of business or provides any third person with such information without due authority, in violation of subparagraph 2 of Article 59, and a person who knowingly receives personal information for profit or unjust purposes;

6. A person who corrupts, destroys, alters, fabricates or leaks any third person's personal information, in violation of subparagraph 3 of Article 59.

Article 72 (Penal Provisions)

Any person who falls under any of the following cases shall be punished by imprisonment for not more than three years or by a fine not exceeding 30 million won:

1. A person who arbitrarily handles image data processing equipment for any purpose other than the intended purpose of installation, films other locations, or uses a recording function, in violation of Article 25.5;

2. A person who acquires personal information or obtains consent to the management of personal information by false or other unlawful means, in violation of subparagraph 1 of Article 59, and a person who knowingly receives personal information for profit or an unjust purpose;

3. A person who reveals confidential information that comes to his/her knowledge in the course of his/her business or uses such information for any purpose other than for his/her duties, in violation of Article 60.

Article 73 (Penal Provisions)

A person who falls under any of the following cases shall be punished by imprisonment for not more than two years or by a fine not exceeding ten million won:

1. A person whose personal information is lost, thieved, leaked, altered or corrupted due to his/her failure to take necessary measures for securing safety, in violation of Article 24.3, 25.6 or 29;

2. A person who keeps using personal information without taking necessary measures, such as correction, deletion, etc., in violation of Article 36.2, or provides a third person with such information;

3. A person who keeps using personal information without suspending the management thereof, in violation of Article 37.2, or provides a third person with such information.

Article 74 (Joint Penal Provisions)

1. Where a representative of a corporation, or an agent, employee or other servant of a corporation or individual commits a violation under Article 70 in connection with the business of the corporation or individual, not only shall such violator be punished, but the corporation or individual also shall be punished by a fine for negligence not exceeding 70 million won: Provided, That where such corporation or individual has not been negligent in giving due attention and supervision concerning the relevant duties to prevent such violation, this shall not apply.

2. Where a representative of a corporation, or an agent, employee or other servant of a corporation or individual commits a violation under Articles 71 through 73 in connection with the business of the corporation or individual, not only shall such violator be punished, but the corporation or individual also shall be punished by a fine under the relevant provisions: Provided, That where such corporation or individual has not been negligent in giving due attention and supervision concerning the relevant duties to prevent such violation, this shall not apply.

Article 75 (Fines for Negligence)

1. A person who falls under any of the following cases shall be punished by a fine for negligence not exceeding 50 million won:

(a) A person who collects personal information, in violation of Article 15.1;

(b) A person who fails to obtain the consent of a legal representative, in violation of Article 22.5;

(c) A person who installs and operates the image data processing equipment, in violation of Article 25.2.

2. A person who falls under any of the following cases shall be punished by a fine for negligence not exceeding 30 million won:

(a) A person who fails to notify a subject of information of the matters to be notified, in violation of Article 15.2, 17.2, 18.3 or 26.3;

(b) A person who refuses to provide goods or services, in violation of Article 16.2 or 22.4;

(c) A person who fails to notify a subject of information of the matters referred to in any of the subparagraphs of Article 20.1, in violation of Article 20.1;

(d) A person who fails to destroy personal information, in violation of Article 21.1;

(e) A person who fails to provide a subject of information with a way to register as a member without providing his/her resident registration number, in violation of Article 24.2;

(f) A person who fails to take necessary measures for securing safety, in violation of Article 24.3, 25.6 or 29;

(g) A person who installs and operates the image data processing equipment, in violation of Article 25.1;

(h) A person who fails to notify a subject of information of the facts referred to in each subparagraph of Article 34.1, in violation of Article 34.1;

(i) A person who fails to report the results of measures taken, in violation of Article 34.3;

(j) A person who restricts or rejects an inspection, in violation of Article 35.5;

(k) A person who fails to take necessary measures, such as correction, deletion, etc., in violation of Article 36.2;

(l) A person who fails to take necessary measures, such as destruction, etc. in connection with the personal information suspended from management, in violation of Article 37.4;

(m) A person who fails to comply with a corrective order issued under Article 64.1.

3. A person who falls under any of the following cases shall be punished by a fine for negligence not exceeding ten million won:

(a) A person who fails to separately save and administer personal information, in violation of Article 21.3;

(b) A person who obtains consent, in violation of provisions referred to in Article 22.1 through 3;

(c) A person who fails to take necessary measures, such as installation of a signboard, etc., in violation of Article 25.4;

(d) A person who fails to entrust his/her affairs in writing stating the matters referred to in each subparagraph of Article 26.1, in violation of Article 26.1;

(e) A person who fails to disclose the details of entrusted affairs and the identity of a trustee,

in violation of Article 26.2;

(f) A person who fails to notify a subject of information of the fact that his/her personal information has been transferred, in violation of Article 27.1 or 2;

(g) A person who fails to establish or disclose personal information management policies, in violation of Article 30.1 or 2;

(h) A person who fails to designate a personal information protection manager, in violation of Article 31.1;

(i) A person who fails to notify a subject of information of the matters to be notified, in violation of Article 35.3 and 4, 36.2 and 4, or 37.3;

(j) A person who fails to submit data such as relevant articles, documents, etc. under Article 63.1 or submits false data;

(k) A person who refuses, interferes with or evades access and inspection under Article 63.2.

4. Fines for negligence under paragraphs 1 through 3 shall be imposed and collected by the Minister of Public Administration and Security and the head of a central administrative agency concerned, as prescribed by Presidential Decree. In such cases, the head of a central administrative agency concerned shall impose and collect fines for negligence on/from a personal information manager under his/her jurisdiction.

ADDENDUM

Article 1 (Enforcement Date)

This Act shall enter into force six months after the date of its promulgation: Provided, That Articles 24.2 and 75.2 (e) shall enter into force one year after the date of its promulgation.

Article 2 (Repeal of other Acts)

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

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

An act performed by or against the Personal Information Dispute Mediation Committee under the former Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

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

Article 4 (Transitional Measures concerning Personal Information being Managed)

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

Article 5 (Transitional Measures concerning Application of Penal Provisions)

1. The application of the penal provisions to a violation of the former Act on the Protection of Personal Information Maintained by Public Institutions, Act on the Protection of Personal Information Maintained by Public Institutions before this Act enters into force shall be governed by the former Act on the Protection of Personal Information Maintained by Public Institutions, Act on the Protection of Personal Information Maintained by Public Institutions.

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

Article 6 Omitted.

Article 7 (Relationship with other Acts)

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